# *A Course on Quantum Information & Error Correction*

*Lecture Notes from EE5750 Quantum Error Correction (2026)*

Lakshmi Prasad Natarajan
Department of Electrical Engineering
IIT Hyderabad

# *Preface and Acknowledgments*

This document is a compilation of my lecture notes from the course EE5750 *Quantum Error Correction* offered at IIT Hyderabad in 2026. The course was a self-contained introduction to the fundamentals of quantum error correction. The only prerequisite for this course was an undergraduate treatment of linear algebra. No familiarity with quantum information or classical coding theory was assumed.

The main goal of the course was to provide a primary treatment of the Knill–Laflamme error correction conditions and the stabilizer codes framework, which are the core of the contents of Chapters 2 and 3 of Daniel Gottesman's book *Surviving as a Quantum Computer in a Classical World*. The first half of the course builds the material towards this by introducing the basics of quantum information (which includes some aspects from open quantum systems which are not usually covered in a quantum computing course).

I thank Vedant Prakash Shenoy, Chiruvella Gagan Chandra Sai Ram, Pathri Vidya Praveen, H Anantha Krishnan, G Ashritha and Jaideep Nirmal A J. Their inputs and interactions during the lectures improved the course material.

The lectures were physically conducted using a blackboard. The lecture material was then transcribed into LaTeX with assistance from Claude (AI).

# *Contents*


***Preface and Acknowledgments*** . . . . . i

***Lecture 1*** . . . . . 1
About the course
Linear algebra in Dirac notation
Matrix multiplication in Dirac notation
Linear algebra formulation of classical computing

***Lecture 2*** . . . . . 6
Recap
Mixed states and ensembles
Classical functions as maps on density matrices
Kraus representation of classical operations

***Homework 1*** . . . . . 11

***Lecture 3*** . . . . . 14
Recap
Kraus representation of classical functions
Remarks on Kraus maps
Invertible functions

***Lecture 4*** . . . . . 18
Kronecker (tensor) products
Properties of the Kronecker product
Bipartite systems

***Homework 2*** . . . . . 22

***Lecture 5*** . . . . . 25
Recap: Kronecker products
Partial trace
Product states
Local operations

***Lecture 6*** . . . . . 31
Classical measurement of classical states
Classical measurement in terms of projections
Generalizing classical measurement of classical states

***Homework 3*** . . . . . 37

***Lecture 7*** . . . . . 40
Quantum systems and pure states
An example of a qubit: the Mach–Zehnder interferometer
Mixed states and ensembles

*Lecture 8* . . . . . 46
Characterization of states
Unitary freedom in state preparation
Composite quantum systems

*Homework 4* . . . . . 51

*Lecture 9* . . . . . 54
Recap
Schmidt decomposition
Preparations of a mixed state

*Lecture 10* . . . . . 60
Purification
Closed quantum systems
Additional material not covered during lecture

*Homework 5* . . . . . 66

*Lecture 11* . . . . . 69
Projective measurements
Examples
Additional material not covered during lecture

*Lecture 12* . . . . . 77
Measurement
Kraus form of operations on a quantum register
Appendix: proof of the no-cloning theorem

*Homework 6* . . . . . 83

*Lecture 13* . . . . . 87
Kraus forms: operational significance
Quantum channels and CPTP maps
Appendix: a concise definition of CPTP maps

*Lecture 14* . . . . . 94
Closing the gap: characterization of quantum channels
Choi's theorem
Unitary freedom in Kraus representations
Appendix: proof of the vectorization remark

*Homework 7* . . . . . 102

*Lecture 15* . . . . . 106
Stinespring dilation
Reversible quantum channels
Appendix: Stinespring dilation for any $d_1, d_2$

***Lecture 16*** . . . . . 113
A note on terminology
Quantum noise
Dephasing (phase-damping) channel
Amplitude-damping channel
Appendix

***Homework 8*** . . . . . 121

***Lecture 17*** . . . . . 125
Quantum channel examples
An example of quantum error correction

***Lecture 18*** . . . . . 130
Prerequisites
The three-qubit phase-flip code revisited
The Steane code

***Lecture 19*** . . . . . 138
The Steane code
Remarks on stabilizer codes
The Shor code

***Homework 9*** . . . . . 144

***Lecture 20*** . . . . . 148
Quantum error correcting codes
Correcting a channel
Correcting a collection of errors
Correcting linear combinations of errors
Summary

***Lecture 21*** . . . . . 156
Recap
Using the Stinespring dilation
Corollaries
The Knill–Laflamme conditions

***Lecture 22*** . . . . . 162
Recap
The Knill–Laflamme conditions
$t$-qubit error correction
Appendix

***Homework 10*** . . . . . 170

***Lecture 23*** . . . . . 175
$t$-error correction
Applying the Knill–Laflamme conditions to $t$-error correction
Appendix

*Lecture 24* . . . . . 182
Stabilizer codes
The Pauli group
Stabilizer groups
The size of a stabilizer

*Lecture 25* . . . . . 189
Recap and generating sets
Dimension of a stabilizer code
How to enlarge a stabilizer?

*Lecture 26* . . . . . 196
Recap: enlarging a stabilizer
The normalizer of a stabilizer
Knill–Laflamme conditions and the distance of stabilizer codes
Appendix

*Homework 11* . . . . . 205

*Lecture 27* . . . . . 209
Vectors over the binary field
Linear algebra over the binary field
The orthogonal dual

*Lecture 28* . . . . . 214
Binary symplectic representation of Paulis
Characterizing stabilizers
Binary characterization of error correction conditions

*Lecture 29* . . . . . 223
Recap
Classical codes
CSS codes

*Homework 12* . . . . . 231

# *Lecture 1*

## §1.1. About the course

This is a first-level course on quantum information and quantum error correction. The only prerequisite for this course is linear algebra or matrix theory. We do not assume any other background. The purpose of the course is to provide a thorough mathematical treatment of the basics of quantum information processing, to explain why noise appears in quantum systems, and to introduce the fundamentals of quantum error correction.

The course material relies heavily on the following references:

1. John Preskill, **lecture notes** for *Ph 219/CS 219: Quantum Information and Computation*, California Institute of Technology.
2. Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (10th Anniversary Edition, Cambridge University Press, 2010).
3. Daniel Gottesman, *Surviving as a Quantum Computer in a Classical World* (book).

Other references include

4. Jaikumar Radhakrishnan's lecture notes on quantum computing (private communication).
5. Mark M. Wilde, *Quantum Information Theory* (2nd Edition, Cambridge University Press, 2017).
6. Phillip Kaye, Raymond Laflamme, and Michele Mosca, *An Introduction to Quantum Computing* (Oxford University Press, 2007).
7. John Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

The goal of the first part of this course (the first six lectures) is to review linear algebra and classical computing in "quantum language". In later lectures we generalize the treatment to quantum computing itself.

## §1.2. Linear algebra in Dirac notation

We will use the *Dirac notation*[1] for linear algebra. Throughout:

- we use matrices and vectors over the complex numbers $\mathbb{C}$;
- we restrict ourselves to finite-dimensional vector spaces;
- all vectors are column vectors.

[1] Named after the physicist Paul Dirac, who introduced it.

**Kets and bras.** Vectors are labeled by small letters $a, b, c, \ldots$ or by Greek letters $\phi, \psi, \epsilon, \nu, \ldots$. A vector $|\phi\rangle \in \mathbb{C}^d$, read "ket $\phi$", is a column vector

$$|\phi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{d-1} \end{bmatrix}, \qquad a_i \in \mathbb{C}.$$

Its conjugate transpose $\langle\phi|$, read "bra $\phi$", is the corresponding row vector:

$$\langle\phi| := |\phi\rangle^\dagger = \begin{bmatrix} a_0 \\ \vdots \\ a_{d-1} \end{bmatrix}^\dagger = \begin{bmatrix} a_0^* & a_1^* & \cdots & a_{d-1}^* \end{bmatrix},$$

where $(\cdot)^\dagger$ denotes the conjugate transpose operation.

**Inner product and norm.** Let

$$|\phi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{d-1} \end{bmatrix}, \qquad |\psi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_{d-1} \end{bmatrix}.$$

The *inner product* of $|\phi\rangle$ and $|\psi\rangle$ is the product of the row vector $\langle\phi|$ with the column vector $|\psi\rangle$:

$$\langle\phi \,|\, \psi\rangle := \langle\phi|\,|\psi\rangle = \begin{bmatrix} a_0^* & \cdots & a_{d-1}^* \end{bmatrix} \begin{bmatrix} b_0 \\ \vdots \\ b_{d-1} \end{bmatrix} = a_0^* b_0 + \cdots + a_{d-1}^* b_{d-1}.$$

Swapping the two vectors conjugates the inner product, since

$$\langle\psi \,|\, \phi\rangle = b_0^* a_0 + \cdots + b_{d-1}^* a_{d-1} = \left(a_0^* b_0 + \cdots + a_{d-1}^* b_{d-1}\right)^*, \qquad \text{i.e.,} \qquad \langle\phi \,|\, \psi\rangle = \langle\psi \,|\, \phi\rangle^*.$$

In particular $\langle\phi \,|\, \phi\rangle = |a_0|^2 + \cdots + |a_{d-1}|^2$ is a non-negative real number, and the *norm* of $|\phi\rangle$ is

$$\|\phi\| = \||\phi\rangle\| := \sqrt{\langle\phi \,|\, \phi\rangle} = \left(|a_0|^2 + \cdots + |a_{d-1}|^2\right)^{1/2}.$$

**The standard basis.** In $\mathbb{C}^d$ we write the standard basis vectors as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad |d-1\rangle = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

This basis is orthonormal: $\langle i|$ has a single 1, in position $i$, so $\langle i \,|\, j\rangle$ is the $i$th entry of $|j\rangle$, which is 1 if $i = j$ and 0 otherwise. Every vector is a linear combination of these basis vectors with its entries as coefficients:

$$|\phi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_{d-1} \end{bmatrix} = a_0|0\rangle + a_1|1\rangle + \cdots + a_{d-1}|d-1\rangle.$$

Note that $|0\rangle \neq 0$: the ket $|0\rangle$ is the first standard basis vector, a vector of norm 1, not the zero vector.

**Matrices and outer products.** Matrices are denoted by capital letters $A, B, K, M, \ldots$ or by Greek letters $\rho, \sigma, \ldots$. Consider the vector spaces $\mathbb{C}^m$ and $\mathbb{C}^n$, with standard bases $|\psi_0\rangle, \ldots, |\psi_{m-1}\rangle$ and $|\phi_0\rangle, \ldots, |\phi_{n-1}\rangle$, respectively. The *outer product* of a column vector of length $m$ and a row vector of length $n$ is an $m \times n$ matrix; for example,

$$|\psi_0\rangle\langle\phi_0| = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}_{m\times 1} \begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix}_{1\times n} = \begin{bmatrix}1 & 0 & \cdots & 0\\0 & 0 & \cdots & 0\\\vdots & & \ddots & \vdots\\0 & 0 & \cdots & 0\end{bmatrix}_{m\times n}.$$

More generally, for any $i = 0, \ldots, m-1$ and any $j = 0, \ldots, n-1$, the matrix $|\psi_i\rangle\langle\phi_j|$ has a 1 in position $(i, j)$ and 0 everywhere else:

$$|\psi_i\rangle\langle\phi_j| = \begin{bmatrix}0\\\vdots\\1\\\vdots\\0\end{bmatrix} \begin{bmatrix}0 & \cdots & 1 & \cdots & 0\end{bmatrix} = \begin{bmatrix}0 & \cdots & 0 & \cdots & 0\\\vdots & & \vdots & & \vdots\\0 & \cdots & 1 & \cdots & 0\\\vdots & & \vdots & & \vdots\\0 & \cdots & 0 & \cdots & 0\end{bmatrix} \leftarrow i$$

$$\uparrow$$

$$j$$

where the 1 of $|\psi_i\rangle$ sits in row $i$, the 1 of $\langle\phi_j|$ in column $j$, and the product matrix has its single 1 in row $i$, column $j$. Consequently, if $A$ is an $m \times n$ matrix with entries $a_{i,j}$, then

$$A = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} \, |\psi_i\rangle\langle\phi_j|,$$

since the right-hand side places the entry $a_{i,j}$ in position $(i, j)$, for every $i$ and $j$.

## §1.3. Matrix multiplication in Dirac notation

The multiplication of two matrices $A$ and $B$ can be interpreted in terms of rows of $A$ interacting with columns of $B$, or columns of $A$ interacting with rows of $B$. We will now review both these viewpoints using Dirac notation.

**Columns times rows.** Let $A$ be an $m \times n$ matrix and $B$ an $n \times p$ matrix. Write the columns of $A$ as $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle \in \mathbb{C}^m$, and the rows of $B$ as $\langle\phi_0|, \langle\phi_1|, \ldots, \langle\phi_{n-1}|$, where $|\phi_i\rangle \in \mathbb{C}^p$. (Here the $|\psi_i\rangle$ and $|\phi_i\rangle$ are arbitrary vectors, not standard basis vectors.) Then

$$AB = \begin{bmatrix}|\psi_0\rangle & \cdots & |\psi_{n-1}\rangle\end{bmatrix} \begin{bmatrix}\langle\phi_0|\\\vdots\\\langle\phi_{n-1}|\end{bmatrix} = \sum_{i=0}^{n-1} |\psi_i\rangle\langle\phi_i|.$$

This is the outer-product form of matrix-matrix multiplication.

Note that the matrix whose columns are $|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{n-1}\rangle$ is $B^\dagger$: conjugate-transposing $B$ turns its rows $\langle\phi_i|$ into the columns $\langle\phi_i|^\dagger = |\phi_i\rangle$.

**Example: resolution of the identity.** Take $m = n = p$, and let $|\psi_0\rangle, \ldots, |\psi_{n-1}\rangle$ be any orthonormal basis of $\mathbb{C}^n$:

$$\langle\psi_i \,|\, \psi_j\rangle = \delta_{i,j} = \begin{cases}1 & \text{if } i = j,\\0 & \text{otherwise.}\end{cases}$$

The matrix $U$ whose columns are $|\psi_0\rangle, \ldots, |\psi_{n-1}\rangle$ is unitary (a square matrix is unitary if and only if its columns form an orthonormal basis). Thus, we have $U^{-1} = U^\dagger$. In particular,

we have $UU^\dagger = I$. Note that the rows of $U^\dagger$ are precisely $\langle\psi_0|, \ldots, \langle\psi_{n-1}|$. Then we have

$$I = UU^\dagger = \sum_{i=0}^{n-1} |\psi_i\rangle\langle\psi_i|.$$

So any orthonormal basis resolves the identity matrix into a sum of outer products.

**Rows times columns.** Now suppose instead that $A$ (of size $m \times n$) has rows $\langle\gamma_0|, \ldots, \langle\gamma_{m-1}|$ and $B$ (of size $n \times p$) has columns $|\zeta_0\rangle, \ldots, |\zeta_{p-1}\rangle$, where all $|\gamma_i\rangle, |\zeta_j\rangle \in \mathbb{C}^n$. Then

$$AB = \begin{bmatrix} \langle\gamma_0| \\ \vdots \\ \langle\gamma_{m-1}| \end{bmatrix} \begin{bmatrix} |\zeta_0\rangle & \cdots & |\zeta_{p-1}\rangle \end{bmatrix}, \qquad \text{the } (i,j) \text{ entry of } AB = \langle\gamma_i|\,|\zeta_j\rangle = \langle\gamma_i\,|\,\zeta_j\rangle.$$

This is the usual "row times column" rule for matrix multiplication, rewritten as an inner product.

## §1.4. Linear algebra formulation of classical computing

From now until Lecture 6, we will study classical computing in quantum language.

**Digital registers and density matrices.** We say that a classical system, or a classical register, is *digital* if it can take only finitely many values. Often, we will denote these values by $0, 1, 2, \ldots, d-1$. We describe the *classical state* of such a register, i.e., the probability distribution of the value it holds, using a $d \times d$ matrix called the *density matrix* associated with the register:

$$\rho = \begin{bmatrix} p_0 & & & \\ & p_1 & & \\ & & \ddots & \\ & & & p_{d-1} \end{bmatrix}_{d\times d}, \qquad p_i = \text{probability that the register holds the value } i.$$

Thus $\rho$ is diagonal, with non-negative diagonal entries that sum to 1. Rows and columns of $\rho$ are indexed by the values $0, \ldots, d-1$ of the register.

EXAMPLE. *Consider a binary register holding a Bernoulli*$(0.1)$ *random variable, with alphabet* $\{0,1\}$ *and*

$$\mathbb{P}[\textit{value} = 0] = 0.9, \qquad \mathbb{P}[\textit{value} = 1] = 0.1,$$

*so its density matrix is*

$$\rho = \begin{bmatrix} 0.9 & 0 \\ 0 & 0.1 \end{bmatrix},$$

*whose first row and column are indexed by the value* 0 *and the second by the value* 1*. Here we work in* $\mathbb{C}^2$*, with* $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *and* $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$*, so that* $\rho = 0.9\,|0\rangle\langle 0| + 0.1\,|1\rangle\langle 1|$.

EXAMPLE. *Consider a register of two bits, so its alphabet is* $\{00, 01, 10, 11\}$ *and its density matrix is* $4 \times 4$*, with rows and columns indexed by* $00, 01, 10, 11$ *in this order. Suppose the first bit is Bernoulli*$(1/2)$ *and the second bit is the negation of the first. Then the only possible values are* 01 *and* 10*, each with probability* $1/2$*, so the density matrix is*

$$\rho = \begin{bmatrix} 0 & & & \\ & 0.5 & & \\ & & 0.5 & \\ & & & 0 \end{bmatrix} \begin{matrix} \leftarrow 00 \\ \leftarrow 01 \\ \leftarrow 10 \\ \leftarrow 11 \end{matrix}$$
$$\begin{matrix} \uparrow & \uparrow & \uparrow & \uparrow \\ 00 & 01 & 10 & 11 \end{matrix}$$

**Pure and mixed classical states.** Consider the state of a *constant* register, one that holds the value $i$ with probability 1, so that every other value has zero probability. Its density matrix has a single 1, in position $(i, i)$, and zeros everywhere else:

$$\rho_{\text{pure}} = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix}_{d \times d} \leftarrow i \qquad \text{rank}(\rho_{\text{pure}}) = 1.$$

Such states are called *pure* classical states. If instead the value of the register is genuinely random, we say that the state is *mixed*:

$$\rho_{\text{mixed}} = \begin{bmatrix} p_0 & & & \\ & p_1 & & \\ & & \ddots & \\ & & & p_{d-1} \end{bmatrix}, \qquad \text{none of the } p_i \text{ equals 1.}$$

In this case $\text{rank}(\rho_{\text{mixed}}) > 1$. Indeed, the rank of a diagonal matrix is its number of non-zero diagonal entries, and since the $p_i$ sum to 1 but none of them equals 1, at least two of them must be non-zero. So, for a classical state, *pure* means rank 1 and *mixed* means rank at least 2. The rank of the density matrix can never be zero, since its diagonal entries sum to 1.

**Ket notation for pure states.** The pure state that holds the value $i$ is, by the outer-product rule of §1.2,

$$\rho_{\text{pure}} = |i\rangle\langle i|,$$

since $|i\rangle\langle i|$ is the matrix with a 1 in row $i$, column $i$, and zeros elsewhere. Because of this, we often say "the state of this register is $|i\rangle$"; this is shorthand for "this register is in the pure state $|i\rangle\langle i|$".

EXAMPLE. *Let $d = 2$. The statement "the state of the register is $|0\rangle$" means*

$$\text{"the density matrix of this register is } |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{"}.$$

**Global phase.** The ket describing a pure state is not unique. For any real $\theta$, consider

$$|\psi\rangle = e^{i\theta}|0\rangle = \begin{bmatrix} e^{i\theta} \\ 0 \end{bmatrix}.$$

Then $\langle\psi| = \begin{bmatrix} e^{-i\theta} & 0 \end{bmatrix}$, and

$$|\psi\rangle\langle\psi| = \begin{bmatrix} e^{i\theta} \\ 0 \end{bmatrix} \begin{bmatrix} e^{-i\theta} & 0 \end{bmatrix} = \begin{bmatrix} e^{i\theta}e^{-i\theta} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = |0\rangle\langle 0|.$$

So we can equally well say that the state of this register is $e^{i\theta}|0\rangle$; both kets describe the same density matrix. The factor $e^{i\theta}$ is called a *global phase*. More generally, for any vector $|\phi\rangle$,

$$\left(e^{i\theta}|\phi\rangle\right)\left(e^{i\theta}|\phi\rangle\right)^\dagger = e^{i\theta}e^{-i\theta}|\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|,$$

so a global phase never changes the density matrix.

# *Lecture 2*

The agenda for this lecture is the *Kraus representation*[1] of classical operations: we will describe the action of a classical function on the state of a register by a map of the form

$$\rho \longmapsto \mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger,$$

where $\sum_j K_j^\dagger K_j = I$.

## §2.1. Recap

**Notation.** A ket $|\phi\rangle$ is a column vector, and the corresponding bra $\langle\phi| = |\phi\rangle^\dagger$ is a row vector. The inner product of $|\psi\rangle$ and $|\phi\rangle$ is $\langle\psi\,|\,\phi\rangle = \langle\psi|\,|\phi\rangle$. In $\mathbb{C}^d$ the standard basis is $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$, and we index the rows and columns of a $d \times d$ matrix by $0, 1, \ldots, d-1$. When the alphabet is a set of strings, we index by the strings instead; for example, for the alphabet $\{00, 01, 10, 11\}$ the rows and columns of a $4 \times 4$ matrix are indexed by $00, 01, 10, 11$, in this order.

**Classical states.** The classical state of a register with alphabet $\{0, 1, \ldots, d-1\}$ is described by the $d \times d$ density matrix

$$\rho = \begin{bmatrix} p_0 & & & \\ & p_1 & & \\ & & \ddots & \\ & & & p_{d-1} \end{bmatrix}_{d\times d},$$

where $p_i$ is the probability that the register holds the value $i$.

**Pure states.** If the value of the register is $k$ (with probability 1), its density matrix has a single 1, in position $(k, k)$:

$$\rho = |k\rangle\langle k| = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix} \leftarrow k$$
$$\uparrow$$
$$k$$

which has rank 1. When dealing with pure states, we have the liberty to describe the state as a density matrix (as shown above) or through a vector $|\psi\rangle$. When we say "the state of a register is $|\psi\rangle$", what we mean is that its density operator is $\rho = |\psi\rangle\langle\psi|$. For a given pure state $\rho$, there are several choices of $|\psi\rangle$ such that $|\psi\rangle\langle\psi| = \rho$; all of them are equally valid representatives of this state, and any two of them differ by a multiplicative *global phase* $e^{i\theta}$.

[1] Named after the physicist Karl Kraus.

## §2.2. Mixed states and ensembles

A mixed state can be written as a sum of pure states weighted by their probabilities:

$$\rho = \begin{bmatrix} p_0 & & \\ & \ddots & \\ & & p_{d-1} \end{bmatrix} = p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1| + \cdots + p_{d-1}|d-1\rangle\langle d-1|.$$

That is, $\rho$ is a *probabilistic mixture of pure states*: with probability $p_i$ the register is in the pure state $|i\rangle\langle i|$. We record this as the *ensemble*

$$\{(p_i, |i\rangle)\}_{i=0}^{d-1}.$$

EXAMPLE. *Consider a register with alphabet* $\mathcal{X} = \{0, 1, 2\}$ *and*

$$\mathbb{P}[0] = \tfrac{1}{4}, \qquad \mathbb{P}[1] = \tfrac{1}{4}, \qquad \mathbb{P}[2] = \tfrac{1}{2}, \qquad \textit{so that} \qquad \rho = \begin{array}{c} \left[\begin{array}{ccc} \frac{1}{4} & & \\ & \frac{1}{4} & \\ & & \frac{1}{2} \end{array}\right] \begin{array}{l} \leftarrow 0 \\ \leftarrow 1 \\ \leftarrow 2 \end{array} \\ \begin{array}{ccc} \uparrow & \uparrow & \uparrow \\ 0 & 1 & 2 \end{array} \end{array}$$

*The corresponding ensemble is* $\{(p_i, |i\rangle)\}_{i=0}^{2} = \{(\frac{1}{4}, |0\rangle),\ (\frac{1}{4}, |1\rangle),\ (\frac{1}{2}, |2\rangle)\}$.

**Notes.**

1. The mixed state is *not* the ket $|\psi\rangle = p_0|0\rangle + \cdots + p_{d-1}|d-1\rangle$. A probabilistic mixture is not a linear combination of kets. Indeed, the density matrix of the ket $|\psi\rangle$ would be

   $$|\psi\rangle\langle\psi| = \Big(\sum_i p_i|i\rangle\Big)\Big(\sum_k p_k\langle k|\Big) = \sum_{i,k} p_i p_k\, |i\rangle\langle k|,$$

   which has rank 1 and non-zero off-diagonal entries $p_i p_k$ whenever two of the $p_i$ are non-zero, whereas $\rho$ is diagonal.

2. Mixed states are represented only by density operators or by ensembles, not by kets. Only pure states can be represented as kets.

3. If you have to take probabilistic combinations, or mixtures, always use density operators, not kets.

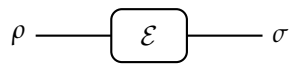
4. Think of $\rho$ as embodying a statistical distribution.

## §2.3. Classical functions as maps on density matrices

Consider two registers: register $A$, with alphabet $\mathcal{X} = \{0, 1, \ldots, d_1 - 1\}$ and state $\rho$, and register $B$, with alphabet $\mathcal{Y} = \{0, 1, \ldots, d_2 - 1\}$ and state $\sigma$. Let

$$f : \mathcal{X} \to \mathcal{Y}, \qquad j \longmapsto f(j),$$

be a function. We denote the action of $f$ by a map $\mathcal{E}$, which takes the state $\rho$ of the input register to the state $\sigma = \mathcal{E}(\rho)$ of the output register:



The map $\mathcal{E}$ is the representation of the function $f$ in quantum language. The function $f$ maps a value in $\mathcal{X}$ to a value in $\mathcal{Y}$. The map $\mathcal{E}$ maps a probability distribution over $\mathcal{X}$ to a probability distribution over $\mathcal{Y}$. When working with $\mathcal{E}$, we think in terms of distributions and how they are modified by operations.

If the input register holds the value $j$, the output register holds $f(j)$. In terms of density matrices,

$$\mathcal{E}\big(|j\rangle\langle j|\big) = |f(j)\rangle\langle f(j)|.$$

If instead the input is random, holding the value $j$ with probability $p_j$, then the output holds $f(j)$ with probability $p_j$, so

$$\mathcal{E}\Big(\sum_j p_j|j\rangle\langle j|\Big) = \sum_j p_j|f(j)\rangle\langle f(j)|.$$

Note that several inputs $j$ may have the same image $f(j)$; their probabilities then add up in the output.

EXAMPLE (NOT operation). *Here* $\mathcal{X} = \mathcal{Y} = \{0,1\}$ *and*

$$|0\rangle\langle 0| \longmapsto |1\rangle\langle 1|, \qquad |1\rangle\langle 1| \longmapsto |0\rangle\langle 0|, \qquad \textit{so} \qquad \mathcal{E}\left(\begin{bmatrix} p_0 & 0 \\ 0 & p_1 \end{bmatrix}\right) = \begin{bmatrix} p_1 & 0 \\ 0 & p_0 \end{bmatrix}.$$

EXAMPLE (OR operation). *Here* $\mathcal{X} = \{00,01,10,11\}$, $\mathcal{Y} = \{0,1\}$, *and* $f(b_1,b_2) = b_1$ *OR* $b_2$, *whose truth table is*

| *input* | *output* |
|---|---|
| 00 | 0 |
| 01 | 1 |
| 10 | 1 |
| 11 | 1 |

*i.e.,*

$$\begin{array}{rcl} |00\rangle\langle 00| & \longmapsto & |0\rangle\langle 0|, \\ |01\rangle\langle 01| & \longmapsto & |1\rangle\langle 1|, \\ |10\rangle\langle 10| & \longmapsto & |1\rangle\langle 1|, \\ |11\rangle\langle 11| & \longmapsto & |1\rangle\langle 1|. \end{array}$$

*The input register lives in* $\mathbb{C}^4$, *with standard basis*

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

*and the output register lives in* $\mathbb{C}^2$, *with* $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *and* $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. *For example,* $|11\rangle\langle 11|$ *is the* $4 \times 4$ *matrix with a single* 1, *in position* $(11,11)$. *A general input state is mapped as follows:*

$$\mathcal{E}\left(\begin{bmatrix} p_{00} & & & \\ & p_{01} & & \\ & & p_{10} & \\ & & & p_{11} \end{bmatrix}\right) = p_{00}|0\rangle\langle 0| + (p_{01}+p_{10}+p_{11})|1\rangle\langle 1|,$$

*that is,*

$$\begin{bmatrix} p_{00} & & & \\ & p_{01} & & \\ & & p_{10} & \\ & & & p_{11} \end{bmatrix}_{4\times 4} \longmapsto \begin{bmatrix} p_{00} & 0 \\ 0 & p_{01}+p_{10}+p_{11} \end{bmatrix}_{2\times 2}.$$

EXAMPLE. *Let* $f : \{0,1,2\} \to \{0,1,2,3,4\}$, $j \mapsto j^2$. *Then* $f(0) = 0$, $f(1) = 1$, $f(2) = 4$, *and*

$$\mathcal{E}\left(\begin{bmatrix} p_0 & & \\ & p_1 & \\ & & p_2 \end{bmatrix}_{3\times 3}\right) = \begin{bmatrix} p_0 & & & & \\ & p_1 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & p_2 \end{bmatrix}_{5\times 5}.$$

*The values* 2 *and* 3 *are not in the range of* $f$, *so they have zero probability at the output.*

## §2.4. Kraus representation of classical operations

Let $f : \mathcal{X} \to \mathcal{Y}$ with $|\mathcal{X}| = d_1$ and $|\mathcal{Y}| = d_2$. We seek a representation of the corresponding map

$$\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \longrightarrow \mathbb{C}^{d_2 \times d_2}$$

in the form

$$\rho \longmapsto \sum_j K_j \, \rho \, K_j^\dagger \qquad \text{with} \qquad \sum_j K_j^\dagger K_j = I_{d_1}.$$

Here $\rho$ is $d_1 \times d_1$, each $K_j$ is $d_2 \times d_1$, and each $K_j^\dagger$ is $d_1 \times d_2$, so that $K_j \rho K_j^\dagger$ is $d_2 \times d_2$ and $K_j^\dagger K_j$ is $d_1 \times d_1$. Such a representation is called a *Kraus representation*, or *operator-sum representation*, of $\mathcal{E}$, and the matrices $K_j$ are its *Kraus operators*. The second condition is called the *completeness condition*.

**What does the completeness condition guarantee?** A density matrix $\rho$ satisfies $\mathrm{Tr}(\rho) = 1$, since its diagonal entries are probabilities that sum to 1. Using linearity of the trace and its cyclic property $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ (which holds for any $M \in \mathbb{C}^{a \times b}$, $N \in \mathbb{C}^{b \times a}$),

$$\begin{aligned} \mathrm{Tr}\big(\mathcal{E}(\rho)\big) = \mathrm{Tr}\Big[\sum_j K_j \rho K_j^\dagger\Big] &= \sum_j \mathrm{Tr}\big[K_j \rho K_j^\dagger\big] = \sum_j \mathrm{Tr}\big[\rho K_j^\dagger K_j\big] \\ &= \mathrm{Tr}\Big[\rho \sum_j K_j^\dagger K_j\Big] = \mathrm{Tr}\big[\rho \, I_{d_1}\big] = \mathrm{Tr}(\rho) = 1. \end{aligned}$$

More generally, the same computation shows $\mathrm{Tr}(\mathcal{E}(M)) = \mathrm{Tr}(M)$ for every $M \in \mathbb{C}^{d_1 \times d_1}$. Thus, completeness implies that $\mathcal{E}$ is a *trace-preserving* (TP) map.

EXAMPLE (Kraus representation of the OR operation). *Take one Kraus operator for each input value,*

$$K_{b_1 b_2} = |f(b_1 b_2)\rangle\langle b_1 b_2|, \qquad b_1 b_2 \in \{00, 01, 10, 11\},$$

*each a* $2 \times 4$ *matrix:*

$$K_{00} = |f(00)\rangle\langle 00| = |0\rangle\langle 00| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}_{2\times 1} \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}_{1\times 4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$K_{01} = |f(01)\rangle\langle 01| = |1\rangle\langle 01| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$K_{10} = |f(10)\rangle\langle 10| = |1\rangle\langle 10| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$K_{11} = |f(11)\rangle\langle 11| = |1\rangle\langle 11| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

*The map is then*

$$\mathcal{E}(\rho) = K_{00} \, \rho \, K_{00}^\dagger + K_{01} \, \rho \, K_{01}^\dagger + K_{10} \, \rho \, K_{10}^\dagger + K_{11} \, \rho \, K_{11}^\dagger.$$

*Let us check that this reproduces the OR operation. Take a diagonal input*

$$\rho = \sum_{x \in \{00,01,10,11\}} p_x |x\rangle\langle x|, \qquad \textit{so that} \qquad \langle x|\rho|x\rangle = p_x.$$

*Then*

$$\begin{aligned} K_{00} \, \rho \, K_{00}^\dagger &= |0\rangle \, \langle 00|\rho|00\rangle \, \langle 0| = p_{00}|0\rangle\langle 0|, \\ K_x \, \rho \, K_x^\dagger &= |1\rangle \, \langle x|\rho|x\rangle \, \langle 1| = p_x|1\rangle\langle 1|, \qquad x = 01, 10, 11, \end{aligned}$$

*and adding these up,*

$$\mathcal{E}(\rho) = p_{00}|0\rangle\langle 0| + (p_{01} + p_{10} + p_{11})|1\rangle\langle 1|,$$

*as required. Completeness also holds: since* $\langle f(x) \,|\, f(x)\rangle = 1$*,*

$$\sum_x K_x^\dagger K_x = \sum_x |x\rangle\langle f(x) \,|\, f(x)\rangle\langle x| = \sum_x |x\rangle\langle x| = I_4.$$

# *Homework 1*

1. A collection of vectors $\{|\psi_1\rangle, \ldots, |\psi_\ell\rangle\}$ is orthonormal if $\langle \psi_i \,|\, \psi_j \rangle = 0$ for $i \neq j$ and equal to 1 when $i = j$. Verify that the following sets of vectors are orthonormal.

   (a) $\{|0\rangle, |1\rangle\}$

   (b) $\{|+\rangle, |-\rangle\}$ where

   $$|+\rangle \triangleq \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle \triangleq \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

   (c) $\{|+i\rangle, |-i\rangle\}$ where

   $$|+i\rangle \triangleq \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \text{ and } |-i\rangle \triangleq \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

2. **Properties of the inner product.** Consider vectors in the finite-dimensional vector space $\mathbb{C}^d$.

   (a) What is the relation between $\langle \psi \,|\, \phi \rangle$ and $\langle \phi \,|\, \psi \rangle$ ? When are these two inner products equal?

   (b) Are the following relations true? If not, what are the correct relation(s)? Here $\alpha_i \in \mathbb{C}$.

   $$\langle \psi | \left( \alpha_1 |\phi_1\rangle + \alpha_2 |\phi_2\rangle \right) = \sum_i \alpha_i \langle \psi \,|\, \phi_i \rangle$$
   $$\left( \alpha_1 |\phi_1\rangle + \alpha_2 |\phi_2\rangle \right)^\dagger |\psi\rangle = \sum_i \alpha_i \langle \phi_i \,|\, \psi \rangle$$

   (c) When is $\langle \psi \,|\, \psi \rangle = 0$ ?

3. A collection of vectors $\{|\psi_1\rangle, \ldots, |\psi_\ell\rangle\}$ is linearly independent if the following is true:

   $$\textstyle\sum_i \alpha_i |\psi_i\rangle = 0 \text{ only when } \alpha_1 = \cdots = \alpha_\ell = 0.$$

   Argue that any orthonormal collection of vectors is linearly independent.

   HINT. Start with $\sum_i \alpha_i |\psi_i\rangle = 0$ and apply inner product with $|\psi_j\rangle$ on both sides.

4. **Anti-commuting matrices and trace.** Assume that $A$ and $B$ anti-commute, i.e., $AB = -BA$.

   (a) Show that $\mathrm{Tr}(AB) = 0$.

   (b) Suppose $A$ is invertible, show that $\mathrm{Tr}(B) = 0$.
   HINT. In this case $B = -A^{-1}BA$.

5. **More on orthonormal bases.**

   (a) If $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ is an orthonormal set of vectors in $\mathbb{C}^n$, show that for any $|\phi\rangle \in \mathbb{C}^n$ we have

   $$|\phi\rangle = \sum_{i=1}^{n} |\psi_i\rangle \langle \psi_i \,|\, \phi \rangle,$$

   which is a linear combination of $\{|\psi_i\rangle\}$.

(b) If $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ is any orthonormal set of vectors in $\mathbb{C}^n$, i.e., $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ is any orthonormal basis of $\mathbb{C}^n$, argue that

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} \langle \psi_i | A | \psi_i \rangle.$$

6. **Properties of adjoint (conjugate transpose).** An operator (or matrix) $A$ is Hermitian if $A^\dagger = A$ and skew-Hermitian if $A^\dagger = -A$.

   (a) Verify $(A^\dagger)^\dagger = A$

   (b) Is $(AB)^\dagger = A^\dagger B^\dagger$ ?

   (c) Is $(\alpha A)^\dagger = \alpha A^\dagger$ ? Here $\alpha \in \mathbb{C}$.

   (d) Is $(A|\psi\rangle)^\dagger = \langle \psi | A^\dagger$ ?

   (e) Verify $(A + B)^\dagger = A^\dagger + B^\dagger$.

   (f) Suppose $A$ is Hermitian, what about $\alpha A$? For what choices of $\alpha$ is this Hermitian, and for what choices is it skew-Hermitian ?

   (g) Same as above, but assume that $A$ is skew-Hermitian.

   (h) If $A$ and $B$ are Hermitian and $\alpha$ and $\beta$ are real scalars is $\alpha A + \beta B$ Hermitian?

7. **Every square matrix is a linear combination of Hermitian matrices.** Assume that $A$ is square.

   (a) Show that $\frac{1}{2}\left(A + A^\dagger\right)$ and $\frac{1}{2}\left(A - A^\dagger\right)$ are Hermitian and skew-Hermitian respectively.

   (b) Show that $A$ is the sum of a Hermitian operator and a skew-Hermitian operator.

   (c) Show that $A$ is a linear combination of two Hermitian operators, that is, there exist Hermitian operators $B$ and $C$ and scalars $\beta, \gamma \in \mathbb{C}$ such that $A = \beta B + \gamma C$.

   REMARK. This shows that every operator is a linear combination of Hermitian operators.

8. **Properties of unitary operators.** A square matrix $U$ is unitary when $U^{-1} = U^\dagger$.

   Assume that $U$ and $V$ are unitary. Verify if the following statements hold; if they are false in general, under what conditions do they hold true?

   (a) $UV$ is unitary.

   (b) $U^\dagger$ is unitary.

   (c) $\alpha U$ is unitary, $\alpha \in \mathbb{C}$.

   (d) $\||U|\psi\rangle\| = \||\psi\rangle\|$ for all $|\psi\rangle \in \mathbb{C}^n$

   (e) If $|\psi_i\rangle = U|\phi_i\rangle$ for $i = 1, 2$, then $\langle \psi_1 \,|\, \psi_2 \rangle = \langle \phi_1 \,|\, \phi_2 \rangle$.

   REMARK. Unitary operators preserve norms and inner products.

9. **Positive Matrices.** We use the term *positive* to mean *positive semi-definite* matrices. An $n \times n$ operator $A$ is positive when $A$ is Hermitian and $\langle \psi | A | \psi \rangle \geq 0$ for all $|\psi\rangle \in \mathbb{C}^n$.

   Show that the density operator corresponding to any classical state (pure or mixed) is a positive operator.

10. Find the density operators for the following random variables. Show your labelling of the rows and columns of the density operators as well.

(a) A binary string of length 3 is generated at random ins such a way that the probability of the 3-bit string is directly proportional to the number of 1's in the string.

(b) A binary string of length 2, where each bit of the string is an independent Bernoulli(2/3) random variable.

(c) What is the density operator of the output when an XOR operation is applied to all the bits of the register in question (a)?

(d) Suppose we count the number of 1's in the string stored in the register in question (b), what is the state of this output?

11. Let $\mathcal{E}$ be the map

$$\mathcal{E}(A) = \sum_j K_j A K_j^\dagger,$$

where $K_j$ are arbitrary operators. Show that if $A$ is any positive operator (whether or not it is diagonal), then $\mathcal{E}(A)$ is positive too.

# *Lecture 3*

## §3.1. Recap

1. A classical register can hold one of $d$ distinct classical values, $\mathcal{X} = \{0, 1, \ldots, d-1\}$. Its state is given by the *density operator*

$$\rho = \begin{bmatrix} p_0 & & \\ & \ddots & \\ & & p_{d-1} \end{bmatrix}_{d \times d}, \qquad p_i = \mathbb{P}[\text{value} = i].$$

2. A pure state is one with $\text{rank}(\rho) = 1$, in which case $\rho = |\psi\rangle\langle\psi|$. We then say "the state is $|\psi\rangle$", or equally "the state is $e^{i\theta}|\psi\rangle$" for any real $\theta$.

3. A *Kraus map* is a map $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ of the form

$$\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger \qquad \text{with} \qquad \sum_j K_j^\dagger K_j = I.$$

## §3.2. Kraus representation of classical functions

Consider two classical registers $A$ and $B$, with alphabets $\mathcal{X} = \{0, 1, \ldots, d_1 - 1\}$ and $\mathcal{Y} = \{0, 1, \ldots, d_2 - 1\}$, respectively. The vector spaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$ are the *Hilbert spaces* associated with registers $A$ and $B$, since the pure states are kets in these vector spaces. A Hilbert space is a vector space over the complex field equipped with an inner product such that the space is complete with respect to the norm induced by this inner product. Throughout this course, we will deal with classical and quantum systems whose Hilbert spaces are finite dimensional (however, this is not the case in general in quantum mechanics). Any $d$-dimensional vector space over $\mathbb{C}$ is isomorphic to $\mathbb{C}^d$, and these spaces are complete with respect to the standard inner product. As is common in the quantum literature, we will refer to these vector spaces as Hilbert spaces.

Let

$$f : \mathcal{X} \to \mathcal{Y}, \qquad j \overset{f}{\longmapsto} f(j).$$

In quantum language, the truth table of $f$ reads

$$|j\rangle\langle j| \overset{\mathcal{E}}{\longmapsto} |f(j)\rangle\langle f(j)|, \qquad j \in \mathcal{X},$$

and, for a random input,

$$\sum_j p_j |j\rangle\langle j| \overset{\mathcal{E}}{\longmapsto} \sum_j p_j |f(j)\rangle\langle f(j)|.$$

**CLAIM.** *There exists a Kraus map corresponding to the classical function $f$ and the classical registers $A$ and $B$.*

REMARK. *This statement is true for quantum systems and quantum operations as well. However, the technique used in the following proof works for the classical case only.*

*Proof.* Given $f : \{0, \ldots, d_1 - 1\} \to \{0, 1, \ldots, d_2 - 1\}$, for each $j \in \{0, \ldots, d_1 - 1\}$ define

$$K_j = |f(j)\rangle\langle j|, \qquad |f(j)\rangle \in \mathbb{C}^{d_2},\ |j\rangle \in \mathbb{C}^{d_1},$$

a $d_2 \times d_1$ matrix. We claim that

$$\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger$$

is a valid Kraus representation of $f$. We verify three things.

*(1) Completeness.* Since $(|a\rangle\langle b|)^\dagger = |b\rangle\langle a|$ for any vectors $|a\rangle$, $|b\rangle$, we have $K_j^\dagger = |j\rangle\langle f(j)|$. Hence

$$\sum_j K_j^\dagger K_j = \sum_j |j\rangle\langle f(j)|\,|f(j)\rangle\langle j| = \sum_j |j\rangle \underbrace{\langle f(j)\,|\,f(j)\rangle}_{=1} \langle j| = \sum_j |j\rangle\langle j| = I,$$

where $\langle f(j)\,|\,f(j)\rangle = 1$ because $|f(j)\rangle$ is a standard basis vector of $\mathbb{C}^{d_2}$.

*(2) Truth table for $f$.* We need to check that $\mathcal{E}(|k\rangle\langle k|) = |f(k)\rangle\langle f(k)|$ for every $k \in \mathcal{X}$. Indeed,

$$\begin{aligned}\mathcal{E}(|k\rangle\langle k|) &= \sum_j K_j\,|k\rangle\langle k|\,K_j^\dagger = \sum_j |f(j)\rangle\langle j\,|\,k\rangle\langle k\,|\,j\rangle\langle f(j)| \\ &= \sum_j |f(j)\rangle\langle f(j)| \cdot \underbrace{\langle j\,|\,k\rangle}_{\delta_{j,k}} \cdot \underbrace{\langle k\,|\,j\rangle}_{\delta_{j,k}} = |f(k)\rangle\langle f(k)|.\end{aligned}$$

*(3) Truth table for mixed states.* This follows from (2) and the linearity of $\mathcal{E}$, proved in the observation below:

$$\mathcal{E}\Big(\sum_k p_k |k\rangle\langle k|\Big) = \sum_k p_k\,\mathcal{E}(|k\rangle\langle k|) = \sum_k p_k |f(k)\rangle\langle f(k)|. \qquad \blacksquare$$

**Observation: any Kraus map is linear.** For any matrices $A, B \in \mathbb{C}^{d_1 \times d_1}$ and scalars $\alpha, \beta \in \mathbb{C}$,

$$\mathcal{E}(\alpha A + \beta B) = \alpha\,\mathcal{E}(A) + \beta\,\mathcal{E}(B).$$

Indeed, by the distributivity of matrix multiplication,

$$\sum_j K_j(\alpha A + \beta B)K_j^\dagger = \alpha \sum_j K_j A K_j^\dagger + \beta \sum_j K_j B K_j^\dagger = \alpha\,\mathcal{E}(A) + \beta\,\mathcal{E}(B).$$

## §3.3. Remarks on Kraus maps

**Non-uniqueness.** For a given function $f$, the representative Kraus map is not unique. Even the number of Kraus operators in the Kraus map is not unique. For example, replacing each $K_j$ in the proof above by the two operators $\frac{1}{\sqrt{2}}K_j$ and $\frac{1}{\sqrt{2}}K_j$ gives $2d_1$ Kraus operators, which still satisfy completeness and define the same map, since

$$\tfrac{1}{\sqrt{2}}K_j \rho \left(\tfrac{1}{\sqrt{2}}K_j\right)^\dagger + \tfrac{1}{\sqrt{2}}K_j \rho \left(\tfrac{1}{\sqrt{2}}K_j\right)^\dagger = K_j \rho K_j^\dagger.$$

In the quantum setting there is a precise and well-known characterization of when two Kraus forms represent the same operation; we will see this in a later lecture.

**Composition of two functions.** Consider three registers $A$, $B$, $C$, with alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, and Hilbert spaces $\mathbb{C}^{d_1}$, $\mathbb{C}^{d_2}$, $\mathbb{C}^{d_3}$, and two functions

$$\mathcal{X} \xrightarrow{f} \mathcal{Y} \xrightarrow{g} \mathcal{Z}, \qquad \text{so that} \qquad \mathcal{X} \xrightarrow{g\circ f} \mathcal{Z}.$$

Suppose $f$ and $g$ are represented by the Kraus maps

$$\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger, \qquad \mathcal{F}(\sigma) = \sum_\ell M_\ell \sigma M_\ell^\dagger,$$

where $\rho$ is $d_1 \times d_1$, each $K_j$ is $d_2 \times d_1$, $\sigma$ is $d_2 \times d_2$, and each $M_\ell$ is $d_3 \times d_2$. Applying $\mathcal{F}$ to the output of $\mathcal{E}$, and using $K_j^\dagger M_\ell^\dagger = (M_\ell K_j)^\dagger$,

$$\mathcal{F}\big(\mathcal{E}(\rho)\big) = \sum_\ell M_\ell \Big( \sum_j K_j \rho\, K_j^\dagger \Big) M_\ell^\dagger = \sum_\ell \sum_j (M_\ell K_j)\, \rho\, (M_\ell K_j)^\dagger,$$

where each $M_\ell K_j$ is $d_3 \times d_1$. This is a Kraus form for $g \circ f$, with Kraus operators

$$\{M_\ell K_j : \text{all } \ell,\ \text{all } j\}.$$

As a sanity check, these operators satisfy completeness:

$$\begin{aligned}\sum_\ell \sum_j (M_\ell K_j)^\dagger (M_\ell K_j) &= \sum_\ell \sum_j K_j^\dagger M_\ell^\dagger M_\ell K_j \\ &= \sum_j K_j^\dagger \Big( \underbrace{\sum_\ell M_\ell^\dagger M_\ell}_{I} \Big) K_j = \sum_j K_j^\dagger K_j = I.\end{aligned}$$

The map also has the right truth table: $\mathcal{F}(\mathcal{E}(|j\rangle\langle j|)) = \mathcal{F}(|f(j)\rangle\langle f(j)|) = |g(f(j))\rangle\langle g(f(j))|$.

## §3.4. Invertible functions

**CLAIM.** *Suppose a classical function $f : \mathcal{X} \to \mathcal{X}$ is invertible, and say $|\mathcal{X}| = d$. Then there is a Kraus map $\mathcal{E}$ for $f$ with a single Kraus operator,*

$$\mathcal{E}(\rho) = K \rho K^\dagger, \qquad K^\dagger K = I,$$

*where $K$ is a $d \times d$ unitary matrix.*

*Proof.* Choose

$$K = \sum_{j=0}^{d-1} |f(j)\rangle\langle j|.$$

By the columns-times-rows rule of Lecture 1, this is the $d \times d$ matrix whose $j$th column is $|f(j)\rangle$:

$$K = \begin{bmatrix} |f(0)\rangle & |f(1)\rangle & \cdots & |f(d-1)\rangle \end{bmatrix},$$

i.e., column $j$ of $K$ has a single 1, in row $f(j)$, and zeros elsewhere. Since $f$ is invertible, each row of $K$ also contains exactly one 1, so $K$ is a permutation matrix.

*(1) Check $K^\dagger K = I$.* We have $K^\dagger = \sum_i |i\rangle\langle f(i)|$, so

$$K^\dagger K = \sum_i \sum_j |i\rangle\langle f(i)\,|\,f(j)\rangle\langle j| = \sum_j |j\rangle\langle j| = I,$$

since $f$ is one-to-one, so that $\langle f(i)\,|\,f(j)\rangle = \delta_{i,j}$. As $K$ is square, $K^\dagger K = I$ means $K^{-1} = K^\dagger$, i.e., $K$ is unitary.

*(2) Truth table.* For every $\ell \in \mathcal{X}$,

$$\begin{aligned}K|\ell\rangle\langle\ell|K^\dagger &= \Big( \sum_j |f(j)\rangle\langle j| \Big) |\ell\rangle\langle\ell| \Big( \sum_i |i\rangle\langle f(i)| \Big) \\ &= \sum_i \sum_j |f(j)\rangle \underbrace{\langle j\,|\,\ell\rangle}_{\delta_{j,\ell}} \underbrace{\langle \ell\,|\,i\rangle}_{\delta_{\ell,i}} \langle f(i)| = |f(\ell)\rangle\langle f(\ell)|.\end{aligned}$$

*(3) Truth table for mixed states.* This follows from (2) using the linearity of $\mathcal{E}$, exactly as in §3.2. ∎

**Remarks.**

1. Whenever we work with an invertible function $f$, we will use the Kraus map with a single term whose Kraus operator is unitary.

   In a later lecture, we will show that, in the general quantum case, any reversible quantum operation can be represented by a Kraus form with a single Kraus operator. Further, any other Kraus representation is a trivial variation of this form.

2. The map $\mathcal{E}(\rho) = K\rho K^\dagger$ maps pure states to pure states and mixed states to mixed states. Indeed, since $K$ and $K^\dagger$ are unitary, hence invertible,

   $$\text{rank}(K\rho K^\dagger) = \text{rank}(\rho),$$

   because multiplying a matrix on either side by an invertible matrix does not change its rank.

3. If $M = e^{i\theta}K$ for some real $\theta$, then

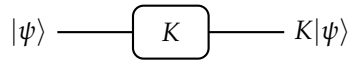
   $$M\rho M^\dagger = e^{i\theta}e^{-i\theta}K\rho K^\dagger = K\rho K^\dagger = \mathcal{E}(\rho),$$

   so $M$ and $K$ define the same map.

4. *Action on pure states.* Say $\rho = |\psi\rangle\langle\psi|$. Then

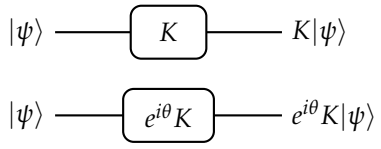
   $$\mathcal{E}(\rho) = K|\psi\rangle\langle\psi|K^\dagger = \big(K|\psi\rangle\big)\big(K|\psi\rangle\big)^\dagger.$$

   Therefore, $\mathcal{E}(\rho)$ is a pure state, specified by the ket $K|\psi\rangle$. We picture this as $|\psi\rangle$ being passed through the "gate" $K$:

   We will always refer only to unitary operators as gates.

5. For any real $\theta$, the gates $K$ and $e^{i\theta}K$ are identical in their operation:

   The two outputs differ only by the global phase $e^{i\theta}$, which can be discarded since the corresponding density operators are identical.

# *Lecture 4*

This lecture has two parts: the tensor, or Kronecker, product of matrices (§4.1–§4.2), and bipartite systems, i.e., systems made of two registers (§4.3).

## §4.1. Kronecker (tensor) products

**DEFINITION.** *Let $A$ be an $m \times n$ matrix with entries $a_{ij}$, and let $B$ be a $p \times q$ matrix. The* Kronecker product, *or* tensor product, *of $A$ and $B$ is the $mp \times nq$ matrix*

$$A \otimes B \triangleq \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}, \qquad \text{where} \qquad A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

*That is, $A \otimes B$ is an $m \times n$ array of $p \times q$ blocks, the $(i, j)$ block being $a_{ij}B$.*

Note that, in general, $A \otimes B \neq B \otimes A$; see the example with $X$ and $I_2$ below.

EXAMPLE. *Consider $|0\rangle, |1\rangle \in \mathbb{C}^2$, with $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Then*

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \in \mathbb{C}^4.$$

*This vector is also denoted*

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle.$$

*Similarly,*

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle, \qquad |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle, \qquad |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle.$$

*These four vectors are exactly the standard basis of $\mathbb{C}^4$, indexed by $00, 01, 10, 11$ as in Lecture 1. For this reason we write $\mathbb{C}^4 \cong \mathbb{C}^2 \otimes \mathbb{C}^2$.*

More generally, let $|0\rangle, \ldots, |d_1 - 1\rangle$ be the standard basis of $\mathbb{C}^{d_1}$ and $|0\rangle, \ldots, |d_2 - 1\rangle$ the standard basis of $\mathbb{C}^{d_2}$. Then

$$|i\rangle \otimes |j\rangle = |ij\rangle \in \mathbb{C}^{d_1 d_2} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}.$$

This set of vectors, as $(i, j)$ ranges over all possible pairs, is the standard basis of $\mathbb{C}^{d_1 d_2}$.

EXAMPLE. *Define*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

*Then*

$$I_2 \otimes X = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} = \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right], \qquad X \otimes I_2 = \begin{bmatrix} 0 & I_2 \\ I_2 & 0 \end{bmatrix} = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right].$$

*In particular, $I_2 \otimes X \neq X \otimes I_2$.*

EXAMPLE. *$I_{d_1} \otimes I_{d_2} = I_{d_1 d_2}$: the blocks are $1 \cdot I_{d_2}$ on the diagonal and $0 \cdot I_{d_2}$ off the diagonal.*

## §4.2. Properties of the Kronecker product

Throughout, the matrices are assumed to have sizes for which the expressions make sense. We state these properties here without proofs.

**1. Bilinearity.**

$$\begin{aligned} A \otimes (B_1 + B_2) &= A \otimes B_1 + A \otimes B_2, \\ (A_1 + A_2) \otimes B &= A_1 \otimes B + A_2 \otimes B, \\ A \otimes (\alpha B) &= (\alpha A) \otimes B = \alpha(A \otimes B), \qquad \alpha \in \mathbb{C}. \end{aligned}$$

These follow directly from the block form: for instance, the $(i, j)$ block of $A \otimes (B_1 + B_2)$ is $a_{ij}(B_1 + B_2) = a_{ij}B_1 + a_{ij}B_2$.

**2. Transpose and conjugate transpose.**

$$(A \otimes B)^T = A^T \otimes B^T, \qquad (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

In particular, note that $(A \otimes B)^\dagger$ is in general *not* $B^\dagger \otimes A^\dagger$ (unlike $(AB)^\dagger = B^\dagger A^\dagger$).

**3. Mixed-product property.**

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

Here, we assume that the number of columns of $A$ equals the number of rows of $C$, and similarly for $B$ and $D$.

**4. Rank.**

$$\operatorname{rank}(A \otimes B) = \operatorname{rank}(A) \cdot \operatorname{rank}(B).$$

**5. Inner products.** Let $|\psi_1\rangle, |\phi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle, |\phi_2\rangle \in \mathbb{C}^{d_2}$. By Property 2,

$$\big(|\psi_1\rangle \otimes |\psi_2\rangle\big)^\dagger = \langle\psi_1| \otimes \langle\psi_2|,$$

and by Property 3,

$$\big(\langle\psi_1| \otimes \langle\psi_2|\big)\big(|\phi_1\rangle \otimes |\phi_2\rangle\big) = \langle\psi_1 \,|\, \phi_1\rangle \otimes \langle\psi_2 \,|\, \phi_2\rangle = \langle\psi_1 \,|\, \phi_1\rangle \cdot \langle\psi_2 \,|\, \phi_2\rangle,$$

since the Kronecker product of two $1 \times 1$ matrices is just their product.

EXAMPLE. *Let $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$ be an orthonormal basis of $\mathbb{C}^3$, and $|\psi_1\rangle, |\psi_2\rangle$ an orthonormal basis of $\mathbb{C}^2$. Then the six vectors*

$$|\phi_1\rangle \otimes |\psi_1\rangle, \quad |\phi_1\rangle \otimes |\psi_2\rangle, \quad |\phi_2\rangle \otimes |\psi_1\rangle, \quad |\phi_2\rangle \otimes |\psi_2\rangle, \quad |\phi_3\rangle \otimes |\psi_1\rangle, \quad |\phi_3\rangle \otimes |\psi_2\rangle$$

*form an orthonormal basis of $\mathbb{C}^6 = \mathbb{C}^3 \otimes \mathbb{C}^2$. Indeed, by Property 5,*

$$\big(\langle\phi_i| \otimes \langle\psi_j|\big)\big(|\phi_k\rangle \otimes |\psi_\ell\rangle\big) = \langle\phi_i \,|\, \phi_k\rangle \cdot \langle\psi_j \,|\, \psi_\ell\rangle = \delta_{i,k}\,\delta_{j,\ell},$$

*so the six vectors are orthonormal; being six orthonormal (hence linearly independent) vectors in a 6-dimensional space, they form a basis.*

## §4.3. Bipartite systems

Consider a system $AB$ consisting of two registers $A$ and $B$:

| | $A$ | $B$ |
|---|---|---|
| alphabet | $\{0, \ldots, d_1 - 1\}$ | $\{0, \ldots, d_2 - 1\}$ |
| Hilbert space | $\mathbb{C}^{d_1}$ | $\mathbb{C}^{d_2}$ |
| standard basis | $\|0\rangle, \ldots, \|d_1 - 1\rangle$ | $\|0\rangle, \ldots, \|d_2 - 1\rangle$ |

We want to look at the composite system, a single system $AB$ that contains $A$ and $B$ as sub-registers. We also specify the order in which we list the two sub-registers: first $A$ and then $B$. Since $A$ can hold any of the $d_1$ possible values, and $B$ can hold any of the $d_2$ possible values, the alphabet of $AB$ has size $d_1 d_2$. The alphabet of the joint system $AB$ is the set of pairs

$$\big\{(0,0),(0,1),\ldots,(0,d_2-1),\ \ldots\ ,(d_1-1,0),(d_1-1,1),\ldots,(d_1-1,d_2-1)\big\},$$

listed in this order, and its Hilbert space is

$$\mathbb{C}^{d_1 d_2} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2},$$

with standard basis

$$|0,0\rangle,|0,1\rangle,\ldots,|0,d_2-1\rangle,\ \ldots\ ,|d_1-1,0\rangle,|d_1-1,1\rangle,\ldots,|d_1-1,d_2-1\rangle,$$

where

$$|i,j\rangle = |i\rangle \otimes |j\rangle.$$

**State of $AB$.** The state of $AB$ is a $d_1 d_2 \times d_1 d_2$ diagonal density matrix $\rho_{AB}$, with rows and columns indexed by the pairs $(i,j)$ in the order above. Call the entry in the $(i,j)$ diagonal position of $\rho_{AB}$

$$p_{i,j} = \mathbb{P}[\text{value in } A = i,\ \text{value in } B = j], \qquad i = 0,\ldots,d_1-1, \quad j = 0,\ldots,d_2-1.$$

Note that $\rho_{AB}$ is the joint probability distribution of two random variables, one stored in $A$ and the other in $B$. It is convenient to view $\rho_{AB}$ as a $d_1 \times d_1$ array of $d_2 \times d_2$ blocks. The off-diagonal blocks are zero, and the $i$th diagonal block collects the probabilities of the pairs $(i,0),\ldots,(i,d_2-1)$ (the diagonal blocks are boxed):

$$\rho_{AB} = \begin{bmatrix} \boxed{\begin{matrix} p_{0,0} & & \\ & \ddots & \\ & & p_{0,d_2-1} \end{matrix}} & & & \\ & \ddots & & \\ & & \boxed{\begin{matrix} p_{i,0} & & \\ & \ddots & \\ & & p_{i,d_2-1} \end{matrix}} & \\ & & & \ddots \\ & & & \boxed{\begin{matrix} p_{d_1-1,0} & & \\ & \ddots & \\ & & p_{d_1-1,d_2-1} \end{matrix}} \end{bmatrix}.$$

**What is the state of $A$?** Given $\rho_{AB}$, the probability that $A$ holds the value $i$ is obtained by summing over all values of $B$:

$$q_i = \mathbb{P}[\text{value in } A = i] = \sum_{j=0}^{d_2-1} p_{i,j}, \qquad \text{so} \qquad \rho_A = \begin{bmatrix} q_0 & & \\ & \ddots & \\ & & q_{d_1-1} \end{bmatrix}.$$

Note that $q_i$ is the sum of the entries of the $i$th diagonal block of $\rho_{AB}$.

**What is the state of $B$?** Similarly,

$$q'_j = \mathbb{P}[\text{value in } B = j] = \sum_{i=0}^{d_1-1} p_{i,j}, \qquad \text{so} \qquad \rho_B = \begin{bmatrix} q'_0 & & \\ & \ddots & \\ & & q'_{d_2-1} \end{bmatrix}.$$

Note that $q'_j$ is the sum of the $j$th diagonal entries in all the diagonal blocks.

**Partial traces.** These computations can be phrased as operations on the blocks of $\rho_{AB}$. Recall that we split $\rho_{AB}$ into $d_1^2$ blocks; each block is a submatrix of size $d_2 \times d_2$.

*Given $\rho_{AB}$, to find $\rho_A$:*

1. Split $\rho_{AB}$ into blocks (of size $d_2 \times d_2$). These blocks are arranged in a grid of size $d_1 \times d_1$ ($d_1$ row blocks and $d_1$ column blocks).
2. Replace each block with its trace.

This is denoted

$$\mathrm{Tr}_B(\rho_{AB}) = \rho_A,$$

called the *partial trace with respect to $B$*, or *tracing out $B$*. Pictorially, if the $(k,l)$ block of a $d_1d_2 \times d_1d_2$ matrix $R$ is $M_{k,l}$,

$$R = \begin{bmatrix} \boxed{M_{0,0}} & \boxed{M_{0,1}} & \cdots & \boxed{M_{0,d_1-1}} \\ \boxed{M_{1,0}} & \boxed{M_{1,1}} & \cdots & \boxed{M_{1,d_1-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{M_{d_1-1,0}} & \boxed{M_{d_1-1,1}} & \cdots & \boxed{M_{d_1-1,d_1-1}} \end{bmatrix},$$

then

$$\mathrm{Tr}_B(R) = \begin{bmatrix} \mathrm{Tr}M_{0,0} & \mathrm{Tr}M_{0,1} & \cdots & \mathrm{Tr}M_{0,d_1-1} \\ \mathrm{Tr}M_{1,0} & \mathrm{Tr}M_{1,1} & \cdots & \mathrm{Tr}M_{1,d_1-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}M_{d_1-1,0} & \mathrm{Tr}M_{d_1-1,1} & \cdots & \mathrm{Tr}M_{d_1-1,d_1-1} \end{bmatrix}.$$

Each $d_2 \times d_2$ submatrix $M_{k,l}$ collapses to the single number $\mathrm{Tr}M_{k,l}$.

*Given $\rho_{AB}$, to find $\rho_B$:*

1. As before, split $\rho_{AB}$ into blocks. There will be $d_1$ row blocks and $d_1$ column blocks.
2. Find the sum of all the diagonal blocks.

This is denoted

$$\mathrm{Tr}_A(\rho_{AB}) = \rho_B,$$

called *tracing out $A$*. Pictorially, for the same matrix $R$ with blocks $M_{k,l}$, only the boxed diagonal blocks are used:

$$R = \begin{bmatrix} \boxed{M_{0,0}} & M_{0,1} & \cdots & M_{0,d_1-1} \\ M_{1,0} & \boxed{M_{1,1}} & \cdots & M_{1,d_1-1} \\ \vdots & \vdots & \ddots & \vdots \\ M_{d_1-1,0} & M_{d_1-1,1} & \cdots & \boxed{M_{d_1-1,d_1-1}} \end{bmatrix},$$

and

$$\mathrm{Tr}_A(R) = M_{0,0} + M_{1,1} + \cdots + M_{d_1-1,d_1-1} = \sum_{k=0}^{d_1-1} M_{k,k}.$$

The off-diagonal blocks are discarded, and the $d_1$ diagonal blocks, each of size $d_2 \times d_2$, are added up to give a $d_2 \times d_2$ matrix.

# *Homework 2*

1. Suppose $\mathcal{E}(\rho) = K\rho K^\dagger$ is the Kraus form of an invertible function $f : \mathcal{X} \to \mathcal{X}$. What is the Kraus form the inverse function $f^{-1}$? Do a sanity check: what is the Kraus form of $f^{-1} \circ f$ ?

2. **Randomized functions.** Consider a randomized algorithm acting on the input alphabet $\mathcal{X} = \{0, \ldots, d_1 - 1\}$ with output alphabet $\mathcal{Y} = \{0, \ldots, d_2 - 1\}$. The algorithm generates a random output for each possible input with the following conditional probabilities:

$$\mathbb{P}\left[\text{output} = i \;\middle|\; \text{input} = j\right] = p_{i|j}$$

   Find a Kraus form for this operation. Verify the truth table (that is, check what is the output state when the input is $|j\rangle\langle j|$), and verify completeness.

3. Find the unitary matrix corresponding to the following invertible functions $f$. In each case, the function acts on a collection of classical bits, we will denote the individual bits as $b_1, b_2$, etc.

   (a) *SWAP gate:* $f(b_1, b_2) = (b_2, b_1)$
   REMARK. This is the function from Quiz 1. This is called the SWAP gate as it swaps/reorders the two physical bits $b_1, b_2$.

   (b) *NOT gate or the X gate:* this gate operates on 1 bit only, output is the logical complement of the input.
   REMARK. The corresponding unitary is denote as the $X$ operator/matrix.

   (c) *Controlled-NOT or the CNOT gate:* This function works on two bits – one of them is designated as the 'control' bit and the other is called the 'target' bit. The function flips the value (logical complement) of the target bit if the control bit value is 1, and it copies in the input to the output otherwise.
   If the control-bit is $b_1$ and the target is $b_2$, we denote this as $\text{CNOT}_{1,2}$, and we have:

$$\text{CNOT}_{1,2}(b_1, b_2) = (b_1, b_1 \oplus b_2),$$

   where $\oplus$ denotes logical XOR operation. Here the control value gets added (XOR-ed) to the target value.
   Similarly, if the control is $b_2$ and target is $b_1$, we have

$$\text{CNOT}_{2,1}(b_1, b_2) = (b_1 \oplus b_2, b_2).$$

   Find the unitaries corresponding to $\text{CNOT}_{1,2}$ and $\text{CNOT}_{2,1}$.

   (d) *Controlled-CNOT gate or CCNOT or Toffoli gate:* This acts on 3 bits $b_1, b_2, b_3$, and it applies $\text{CNOT}_{2,3}$ only when $b_1 = 1$ and acts as an identity function otherwise. So, the value of $b_1$ controls what happens on the other two bits. Here,

$$f(b_1, b_2, b_3) = (b_1, b_2, b_1 b_2 \oplus b_3),$$

   where $b_1 b_2$ is the multiplication operation denoting the logical AND of $b_1, b_2$.

4. The Toffoli gate is known to be a universal gate in classical computing, that is, any Boolean function $g(b_1, \ldots, b_m)$ can be computed using a circuits consisting of only Toffoli gates and some additional bits (whose values we are allowed to set as per our choice to 0 or 1). These additional bits (which are not inputs to the target function $g$) are called 'ancillary' bits or simply 'ancilla'.

   Can you design circuits based on Toffoli gates for the following classical operations/functions $g$? You might have to use ancillary bits in your circuits; if so, identify which bits in your circuits are the function inputs (i.e., $b_1, b_2$ etc.) and which are the ancillary bits.

   (a) NOT operation

   (b) AND operation

   (c) OR operation

5. If $A$ and $B$ are square matrices (not necessarily of the same size) and are both invertible, verify

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

   REMARK. Kronecker product of invertible operators is invertible.

6. Consider

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d_1-1} \end{bmatrix}, |b\rangle = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d_1-1} \end{bmatrix} \in \mathbb{C}^{d_1} \text{ and } |x\rangle = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d_2-1} \end{bmatrix}, |y\rangle = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{d_2-1} \end{bmatrix} \in \mathbb{C}^{d_2}.$$

   (a) Explicitly verify the formula

$$(\langle a| \otimes \langle x|)\,(|b\rangle \otimes |y\rangle) = \langle a \,|\, b\rangle \cdot \langle x \,|\, y\rangle.$$

   (b) Verify that $|a\rangle \otimes |x\rangle = 0$ if and only if $|a\rangle = 0$ or $|x\rangle = 0$.

   REMARK. You might need these results for the next problem.

7. **Kronecker products and linear independence.**

   (a) Suppose $|\psi_0\rangle, \ldots, |\psi_{m-1}\rangle \in \mathbb{C}^m$ are linearly independent. This means that if $\sum_i \alpha_i |\psi_i\rangle = 0$ then $\alpha_i = 0$ for all $i$.
   Now, let $|\phi_0\rangle, \ldots, |\phi_{m-1}\rangle \in \mathbb{C}^p$ be any set of $m$ vectors in $\mathbb{C}^p$ ($m$ need not be equal to $p$, and $|\phi_0\rangle, \ldots, |\phi_{m-1}\rangle$ need not have linear independence, these are just any collection of $m$ vectors).
   You must prove the following

$$|\phi_0\rangle \otimes |\psi_0\rangle + \cdots + |\phi_{m-1}\rangle \otimes |\psi_{m-1}\rangle = 0 \;\Rightarrow\; |\phi_i\rangle = 0 \text{ for all } i.$$

   HINT. This is one possible technique: find an invertible $mp \times mp$ matrix $A$ such that

$$A\,(|\phi\rangle \otimes |\psi_i\rangle) = |\phi\rangle \otimes |i\rangle$$

   for any $|\phi\rangle \in \mathbb{C}^p$ and for all $i = 0, \ldots, m-1$. Once you have such an $A$, apply the operator $A$ to both sides of

$$|\phi_0\rangle \otimes |\psi_0\rangle + \cdots + |\phi_{m-1}\rangle \otimes |\psi_{m-1}\rangle = 0$$

   and then make use of the fact that $|0\rangle, \ldots, |m-1\rangle$ are the standard basis for $\mathbb{C}^m$.

(b) Now, we are ready to prove the fact that if $|\psi_0\rangle, \ldots, |\psi_{m-1}\rangle$ are linearly independent in $\mathbb{C}^m$, and if $|\zeta_0\rangle, \ldots, |\zeta_{p-1}\rangle$ are linearly independent in $\mathbb{C}^p$, then the collection of $mp$ vectors $\{|\zeta_i\rangle \otimes |\psi_j\rangle \ : \ i = 0, \ldots, p-1, j = 0, \ldots, m-1\}$ is linearly independent in $\mathbb{C}^{mp}$.

Prove this using the result of part (a).

HINT. Start from $\sum_i \sum_j \alpha_{i,j} |\zeta_i\rangle \otimes |\psi_j\rangle = 0$, and reduce this to the equation considered in part (a); use the linearity of Kronecker products to do this. Finally, show that $\alpha_{i,j} = 0$ for all $i, j$.

REMARK. We saw in Lecture 4 that if $\{|\zeta_i\rangle\}$ and $\{|\psi_j\rangle\}$ are orthonormal then so are $\{|\zeta_i\rangle \otimes |\psi_j\rangle\}$. The current problem shows that a similar result holds for linear independence too. In fact, since there are precisely $mp$ vectors in $\{|\zeta_i\rangle \otimes |\psi_j\rangle\}$ we see that this collection is a basis for $\mathbb{C}^{mp}$.

This result extends to Kronecker products of matrices as well. We will see an example (applied to matrices) in the next question.

8. For simplicity and concreteness we will consider Kronecker products of $2 \times 2$ matrices only, i.e., both $A$ and $B$ in $A \otimes B$ are $2 \times 2$. Note that $A \otimes B$ is a $4 \times 4$ matrix.

   (a) Find 4 matrices $M_1, \ldots, M_4$ in $\mathbb{C}^{2\times 2}$ (the space of $2 \times 2$ complex matrices) such that every matrix in $\mathbb{C}^{2\times 2}$ can be expressed as linear combination of $M_1, \ldots, M_4$.
   HINT. Although there are many solutions, you can save a lot of work by a suitable choice of $M_1, \ldots, M_4$ that can be easily expressed in terms of the standard basis $|0\rangle$ and $|1\rangle$.

   (b) Now verify that any $4 \times 4$ matrix can be written as a linear combination of the 16 matrices:
   $$M_i \otimes M_j, \text{ where } i, j = 1, 2, 3, 4.$$

REMARK. In general if $\{M_i \ : \ i = 1, \ldots, m^2\}$ is a basis for $\mathbb{C}^{m\times m}$ and $\{N_j \ : \ j = 1, \ldots, n^2\}$ is a basis for $\mathbb{C}^{n\times n}$, then

$$\{M_i \otimes N_j : i = 1, \ldots, m^2, j = 1, \ldots, n^2\}$$

is a basis for $\mathbb{C}^{mn\times mn}$. In particular, every $mn \times mn$ matrix $A$ can be expressed as linear combination of Kronecker products

$$A = \sum_i \sum_j \alpha_{i,j} M_i \otimes N_j.$$

This is an *important observation*.

9. **When are two Kraus forms equivalent for classical operations?** In this question, we will consider invertible classical operations on classical states. Suppose

$$\mathcal{E}(\rho) = K \rho K^\dagger$$

is the Kraus form of an invertible classical function, where $\rho$ is restricted to classical states only (mixed or pure). Consider another Kraus form

$$\mathcal{F}(\rho) = \sum_{\ell=1}^{L} M_\ell \rho M_\ell^\dagger.$$

Find necessary and sufficient conditions for $\mathcal{F}(\rho) = \mathcal{E}(\rho)$ for all classical states $\rho$ (both mixed and pure). Your conditions must be explicit enough such that they can be easily used as a procedure to identify/construct the new Kraus operators $\{M_1, \ldots, M_L\}$ starting from the given Kraus operator $K$.

# *Lecture 5*

We continue to study bipartite classical systems.

## §5.1. Recap: Kronecker products

Recall from Lecture 4 that if $A$ is an $m \times n$ matrix and $B$ is a $p \times q$ matrix, then $A \otimes B$ is an $mp \times nq$ matrix. Two facts are worth keeping in mind.

(1) Not every $mp \times nq$ matrix is a Kronecker product of an $m \times n$ matrix and a $p \times q$ matrix. A Kronecker product consists of blocks (sub-matrices) of size $p \times q$, and all these blocks differ from each other by a scalar multiplication. Any $mp \times nq$ matrix where this property does not hold is not a Kronecker product.

(2) Every $mp \times nq$ matrix is a linear combination of Kronecker products of finitely many $m \times n$ and $p \times q$ matrices.

Fact (2) is a consequence of the following result, which we state without proof. We think of a matrix space $\mathbb{C}^{m\times n}$ as a vector space over the field $\mathbb{C}$. This vector space has dimension $mn$, and hence, any basis contains a list of exactly $mn$ matrices, each of size $m \times n$.

**CLAIM.** *If $\{A_i\}_{i=1}^{mn}$ is a basis of $\mathbb{C}^{m\times n}$ and $\{B_j\}_{j=1}^{pq}$ is a basis of $\mathbb{C}^{p\times q}$, then*

$$\{A_i \otimes B_j \ : \ i = 1, \ldots, mn, \ j = 1, \ldots, pq\}$$

*is a basis of $\mathbb{C}^{mp\times nq}$.*

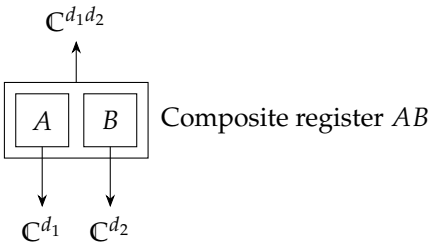
Specializing this to the case $n = 1$ and $q = 1$ yields the analogous result for vectors:

**CLAIM.** *If $\{|\psi_i\rangle\}$ is a basis for $\mathbb{C}^m$ and $\{|\phi_j\rangle\}$ is a basis for $\mathbb{C}^p$, then $\{|\psi_i\rangle \otimes |\phi_j\rangle\}$ is a basis for $\mathbb{C}^{mp} = \mathbb{C}^m \otimes \mathbb{C}^p$.*

Two exercise problems in Homework 2 deal with the proof of the second claim and a proof of a special case of the first claim.

## §5.2. Partial trace

Consider a bipartite system $AB$, where register $A$ has the Hilbert space $\mathbb{C}^{d_1}$ and register $B$ has the Hilbert space $\mathbb{C}^{d_2}$; in other words, the digital system $A$ has a $d_1$-ary alphabet and the digital system $B$ has a $d_2$-ary alphabet. Then $AB$ has the Hilbert space $\mathbb{C}^{d_1 d_2} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, and its state $\rho_{AB}$ is a $d_1 d_2 \times d_1 d_2$ matrix.



As in Lecture 4, we split $\rho_{AB}$ into blocks of size $d_2 \times d_2$, arranged in a grid of $d_1$ row blocks and $d_1$ column blocks:

$$\rho_{AB} = \begin{bmatrix} \boxed{M_{0,0}} & \boxed{M_{0,1}} & \cdots & \boxed{M_{0,d_1-1}} \\ \boxed{M_{1,0}} & \boxed{M_{1,1}} & \cdots & \boxed{M_{1,d_1-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{M_{d_1-1,0}} & \boxed{M_{d_1-1,1}} & \cdots & \boxed{M_{d_1-1,d_1-1}} \end{bmatrix}, \qquad M_{k,l} \in \mathbb{C}^{d_2 \times d_2}.$$

The states of the two registers are obtained from $\rho_{AB}$ by the two partial traces:

$$\begin{aligned} \rho_A = \mathrm{Tr}_B(\rho_{AB}): &\quad \text{replace each block with its trace,} \\ \rho_B = \mathrm{Tr}_A(\rho_{AB}): &\quad \text{sum the diagonal blocks.} \end{aligned}$$

**Linearity.** Both these operations are linear. That is, for any $d_1 d_2 \times d_1 d_2$ matrices $R_1, R_2$ and scalars $\alpha_1, \alpha_2 \in \mathbb{C}$,

$$\begin{aligned} \mathrm{Tr}_A(\alpha_1 R_1 + \alpha_2 R_2) &= \alpha_1 \mathrm{Tr}_A(R_1) + \alpha_2 \mathrm{Tr}_A(R_2), \\ \mathrm{Tr}_B(\alpha_1 R_1 + \alpha_2 R_2) &= \alpha_1 \mathrm{Tr}_B(R_1) + \alpha_2 \mathrm{Tr}_B(R_2). \end{aligned}$$

Indeed, the $(k,l)$ block of $\alpha_1 R_1 + \alpha_2 R_2$ is $\alpha_1$ times the $(k,l)$ block of $R_1$ plus $\alpha_2$ times the $(k,l)$ block of $R_2$. The partial trace $\mathrm{Tr}_A$ adds up the diagonal blocks, and $\mathrm{Tr}_B$ takes the trace of each block. Both addition and the trace are linear operations.

**Partial traces of Kronecker products.** Observe that any $\rho_{AB}$ is a linear combination of Kronecker products (with factors of sizes $d_1 \times d_1$ and $d_2 \times d_2$); this is fact (2) of §5.1 with $m = n = d_1$ and $p = q = d_2$. That is, there exist matrices $C_1, C_2, \ldots$ of size $d_1 \times d_1$ and $D_1, D_2, \ldots$ of size $d_2 \times d_2$ such that

$$\rho_{AB} = \sum_i \alpha_i \, C_i \otimes D_i$$

for some scalars $\alpha_1, \alpha_2, \ldots$. By linearity of the partial trace,

$$\rho_A = \sum_i \alpha_i \mathrm{Tr}_B(C_i \otimes D_i), \qquad \rho_B = \sum_i \alpha_i \mathrm{Tr}_A(C_i \otimes D_i).$$

So, to compute partial traces, it is enough to know the partial traces of Kronecker products.

**Claim.** *Let $C$ be a $d_1 \times d_1$ matrix and $D$ a $d_2 \times d_2$ matrix. Then*

$$\begin{aligned} \mathrm{Tr}_B(C \otimes D) &= C \cdot \mathrm{Tr}(D), \\ \mathrm{Tr}_A(C \otimes D) &= D \cdot \mathrm{Tr}(C). \end{aligned}$$

Here $C$ is the factor related to register $A$, and $D$ the factor related to register $B$. Tracing out $B$ replaces the factor $D$ by its trace, and tracing out $A$ replaces the factor $C$ by its trace.

*Proof.* Let the entries of $C$ be $c_{kl}$. By the definition of the Kronecker product,

$$C \otimes D = \begin{bmatrix} c_{11}D & c_{12}D & \cdots & c_{1d_1}D \\ c_{21}D & c_{22}D & \cdots & c_{2d_1}D \\ \vdots & \vdots & \ddots & \vdots \\ c_{d_1 1}D & c_{d_1 2}D & \cdots & c_{d_1 d_1}D \end{bmatrix},$$

so the $(k,l)$ block is $c_{kl}D$. Replacing each block with its trace gives the $d_1 \times d_1$ matrix whose $(k,l)$ entry is

$$\mathrm{Tr}(c_{kl}D) = c_{kl}\mathrm{Tr}(D).$$

This matrix is $C \cdot \mathrm{Tr}(D)$. Adding the diagonal blocks gives

$$c_{11}D + c_{22}D + \cdots + c_{d_1 d_1}D = \Big(\sum_k c_{kk}\Big)D = D \cdot \mathrm{Tr}(C). \qquad \blacksquare$$

Combining the claim with the expansion $\rho_{AB} = \sum_i \alpha_i C_i \otimes D_i$, we obtain

$$\rho_A = \sum_i \alpha_i \mathrm{Tr}(D_i)\, C_i, \qquad \rho_B = \sum_i \alpha_i \mathrm{Tr}(C_i)\, D_i.$$

Hence, it is easier to track the partial trace when we have such a Kronecker product expansion.

## §5.3. Product states

A product state is the state of a composite system $AB$ when the information contained in the registers $A$ and $B$ is independent of each other. Suppose the classical values in registers $A$ and $B$ are generated independently. Let the states of the two registers be

$$\rho_A = \begin{bmatrix} q_0 & & \\ & \ddots & \\ & & q_{d_1-1} \end{bmatrix}, \qquad \rho_B = \begin{bmatrix} q'_0 & & \\ & \ddots & \\ & & q'_{d_2-1} \end{bmatrix}.$$

Here, $(q_i, \forall i)$ and $(q'_j, \forall j)$ are the probability mass functions of the random variables stored in $A$ and $B$, respectively. What is $\rho_{AB}$?

Let $X$ be the random variable in register $A$ and $Y$ the random variable in register $B$. As in Lecture 4, the diagonal entries of $\rho_{AB}$ are

$$p_{i,j}, \qquad i = 0, \ldots, d_1 - 1, \quad j = 0, \ldots, d_2 - 1,$$

where

$$p_{i,j} = \mathbb{P}[X = i,\, Y = j].$$

Since $X$ and $Y$ are independent,

$$p_{i,j} = \mathbb{P}[X = i] \cdot \mathbb{P}[Y = j] = q_i\, q'_j.$$

So the $i$th diagonal block (of size $d_2 \times d_2$) of $\rho_{AB}$ is

$$\begin{bmatrix} q_i q'_0 & & \\ & \ddots & \\ & & q_i q'_{d_2-1} \end{bmatrix} = q_i\, \rho_B,$$

and the off-diagonal blocks are zero:

$$\rho_{AB} = \begin{bmatrix} q_0\rho_B & & & \\ & q_1\rho_B & & \\ & & \ddots & \\ & & & q_{d_1-1}\rho_B \end{bmatrix}.$$

By the definition of the Kronecker product, this is

$$\rho_{AB} = \rho_A \otimes \rho_B.$$

**DEFINITION.** *We say that the state of the bipartite system $AB$ is a* product state *if*

$$\rho_{AB} = \rho_A \otimes \rho_B.$$

For product states,

- registers $A$ and $B$ were prepared independently; or
- the information contained in $A$ and $B$ is statistically independent.

As a sanity check, let us *marginalize* this $\rho_{AB}$ to see if we retrieve the original $\rho_A$ and $\rho_B$ we started with:

$$\mathrm{Tr}_B(\rho_A \otimes \rho_B) = \rho_A \mathrm{Tr}(\rho_B) = \rho_A, \qquad \mathrm{Tr}_A(\rho_A \otimes \rho_B) = \rho_B \mathrm{Tr}(\rho_A) = \rho_B,$$

since $\rho_A$ and $\rho_B$ have unit trace.

**A special case: pure product states.** Say $\rho_{AB} = \rho_A \otimes \rho_B$ and $\mathrm{rank}(\rho_{AB}) = 1$, i.e., $AB$ is in a pure state that is also a product state. This means that the composite system holds a specific value, say $(i, j)$, with probability 1. Using the rank property of the Kronecker product (Lecture 4),

$$1 = \mathrm{rank}(\rho_{AB}) = \mathrm{rank}(\rho_A \otimes \rho_B) = \mathrm{rank}(\rho_A) \cdot \mathrm{rank}(\rho_B).$$

Since ranks are non-negative integers, this implies

$$\mathrm{rank}(\rho_A) = \mathrm{rank}(\rho_B) = 1.$$

Hence $\rho_A$ and $\rho_B$ are pure states, and we can write (Lecture 1)

$$\rho_A = |\psi\rangle\langle\psi|, \qquad \rho_B = |\phi\rangle\langle\phi|.$$

By the mixed-product property of the Kronecker product,

$$\rho_{AB} = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| = \big(|\psi\rangle \otimes |\phi\rangle\big)\big(\langle\psi| \otimes \langle\phi|\big),$$

so in ket notation the state of $AB$ is $|\psi\rangle \otimes |\phi\rangle$. Thus a pure product state is the Kronecker product of a pure state of $A$ and a pure state of $B$.

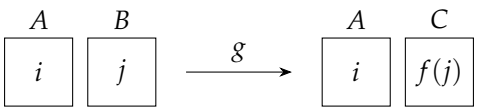
## §5.4. Local operations

Consider registers $A$, $B$ and $C$ with Hilbert spaces $\mathbb{C}^{d_1}$, $\mathbb{C}^{d_2}$ and $\mathbb{C}^{d_3}$. Let $f$ be a function that maps the values of register $B$ to the values of register $C$, and let

$$\mathcal{E}(\rho_B) = \sum_\ell K_\ell \, \rho_B \, K_\ell^\dagger$$

be a Kraus form for $f$ (Lecture 3), where each $K_\ell$ is $d_3 \times d_2$ and $\sum_\ell K_\ell^\dagger K_\ell = I$. Suppose we apply $f$ to register $B$ of the bipartite system $AB$, and leave register $A$ untouched. The resulting function on $AB$ is

$$g(i, j) = (i, f(j)),$$



which maps the values of $AB$ to the values of $AC$. Such a function, which acts on only one of the registers, is called a *local operation*. In this case register $B$ is replaced with a new register $C$.

In quantum language, the truth table for $g$ is

$$|i,j\rangle\langle i,j| \;\longmapsto\; |i,f(j)\rangle\langle i,f(j)|,$$

where

$$|i,j\rangle\langle i,j| = \big(|i\rangle \otimes |j\rangle\big)\big(\langle i| \otimes \langle j|\big) = |i\rangle\langle i| \otimes |j\rangle\langle j|$$

and

$$|i,f(j)\rangle\langle i,f(j)| = \big(|i\rangle \otimes |f(j)\rangle\big)\big(\langle i| \otimes \langle f(j)|\big) = |i\rangle\langle i| \otimes |f(j)\rangle\langle f(j)|.$$

**CLAIM.** *If $\{K_\ell\}_\ell$ is a set of Kraus operators for $f$, then $\{I_{d_1} \otimes K_\ell\}_\ell$ is a set of Kraus operators for the function $g$ (which is $f$ acting locally on register $B$).*

*Proof.* Each $I_{d_1} \otimes K_\ell$ is a $d_1 d_3 \times d_1 d_2$ matrix, as required for a map from the states of $AB$ to the states of $AC$.

*(i) Completeness.* Using the conjugate-transpose and mixed-product properties of the Kronecker product,

$$\begin{aligned}\sum_\ell (I \otimes K_\ell)^\dagger (I \otimes K_\ell) &= \sum_\ell (I \otimes K_\ell^\dagger)(I \otimes K_\ell) \\ &= \sum_\ell I \otimes K_\ell^\dagger K_\ell \\ &= I \otimes \Big(\sum_\ell K_\ell^\dagger K_\ell\Big) \\ &= I \otimes I = I.\end{aligned}$$

*(ii) Truth table.* Suppose $AB$ is in the state $|i,j\rangle\langle i,j|$. Then

$$\begin{aligned}\sum_\ell (I \otimes K_\ell)\,|i,j\rangle\langle i,j|\,(I \otimes K_\ell)^\dagger &= \sum_\ell (I \otimes K_\ell)\big(|i\rangle\langle i| \otimes |j\rangle\langle j|\big)(I \otimes K_\ell^\dagger) \\ &= \sum_\ell \big(I|i\rangle\langle i|I\big) \otimes \big(K_\ell|j\rangle\langle j|K_\ell^\dagger\big) \\ &= \sum_\ell |i\rangle\langle i| \otimes K_\ell|j\rangle\langle j|K_\ell^\dagger \\ &= |i\rangle\langle i| \otimes \Big(\sum_\ell K_\ell|j\rangle\langle j|K_\ell^\dagger\Big).\end{aligned}$$

Since $\mathcal{E}$ is a Kraus form for $f$, $\sum_\ell K_\ell|j\rangle\langle j|K_\ell^\dagger = \mathcal{E}(|j\rangle\langle j|) = |f(j)\rangle\langle f(j)|$. Hence

$$\begin{aligned}\sum_\ell (I \otimes K_\ell)\,|i,j\rangle\langle i,j|\,(I \otimes K_\ell)^\dagger &= |i\rangle\langle i| \otimes |f(j)\rangle\langle f(j)| \\ &= \big(|i\rangle \otimes |f(j)\rangle\big)\big(\langle i| \otimes \langle f(j)|\big),\end{aligned}$$

which is the truth table of $g$. As in Lecture 3, the map is linear, so it also gives the correct output when $AB$ is in a mixed state $\rho_{AB} = \sum_{i,j} p_{i,j}|i,j\rangle\langle i,j|$. ∎

**Notation.** Thus, if $\mathcal{E}(\rho_B) = \sum_\ell K_\ell \rho_B K_\ell^\dagger$ is a Kraus form for $f$, then

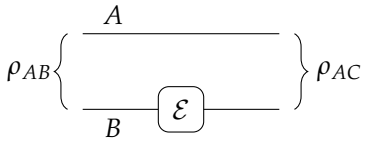
$$\mathcal{G}(\rho_{AB}) = \sum_\ell (I \otimes K_\ell)\,\rho_{AB}\,(I \otimes K_\ell)^\dagger$$

is a Kraus form for $g$. We also denote this map as

$$\mathcal{G} = \mathbb{I}_A \otimes \mathcal{E}_B = \mathbb{I} \otimes \mathcal{E},$$

where $\mathbb{I}$ is the identity map, which leaves register $A$ unchanged. Note that, just like $\mathcal{E}$, $\mathbb{I}$ is a function that maps matrices to matrices (or operators to operators), i.e., $\mathcal{E}$ and $\mathbb{I}$ are *superoperators*. Observe the difference between $\mathbb{I}$ (maps a matrix/operator to itself) and $I$ (maps a ket to itself); the former is a superoperator and the latter is an operator.

In a circuit, $\mathcal{E}$ acts on the wire of register $B$ alone, and the output is the state $\rho_{AC}$ of $AC$:



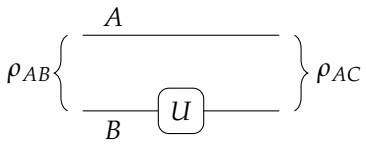

**Special case: invertible functions.** Suppose $f$ is invertible. Then, from Lecture 3, there exists a unitary operator $U$ such that

$$\mathcal{E}(\rho_B) = U\rho_B U^\dagger.$$

(Here $d_3 = d_2$, since an invertible function maps the $d_2$ values of $B$ to $d_2$ distinct values.) The Kraus form of $g$ then has the single Kraus operator $I \otimes U$:

$$\rho_{AC} = (I \otimes U)\,\rho_{AB}\,(I \otimes U)^\dagger.$$

Note that $I \otimes U$ is itself unitary, since $(I \otimes U)^\dagger(I \otimes U) = I \otimes U^\dagger U = I \otimes I = I$.



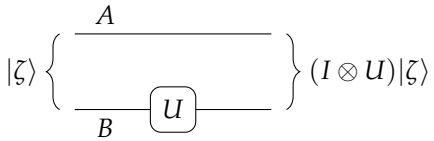

**A further special case: pure input states.** If, in addition, $\rho_{AB}$ is a pure state,

$$\rho_{AB} = |\zeta\rangle\langle\zeta|,$$

then

$$\rho_{AC} = (I \otimes U)|\zeta\rangle\langle\zeta|(I \otimes U)^\dagger = \big((I \otimes U)|\zeta\rangle\big)\big((I \otimes U)|\zeta\rangle\big)^\dagger.$$

So the state of $AC$ is the pure state $(I \otimes U)|\zeta\rangle$.




In words:

$$\begin{aligned} \text{pure state} &\longrightarrow \text{reversible operation (local or global)} \longrightarrow \text{pure state,} \\ \text{ket} &\longrightarrow \text{multiply by a unitary} \longrightarrow \text{ket.} \end{aligned}$$

This also follows from two facts about the rank of a product of matrices:

- $\text{rank}(MN) \leq \min\{\text{rank}(M), \text{rank}(N)\}$;
- if $M$ is square and invertible, then $\text{rank}(MN) = \text{rank}(NM) = \text{rank}(N)$.

Since $I \otimes U$ and $(I \otimes U)^\dagger$ are invertible,

$$\text{rank}(\rho_{AC}) = \text{rank}\big((I \otimes U)\,\rho_{AB}\,(I \otimes U)^\dagger\big) = \text{rank}(\rho_{AB}).$$

So a reversible operation maps a pure state (rank 1) to a pure state, and a mixed state to a mixed state.

# *Lecture 6*

In this lecture we describe the measurement of a classical register in the language of linear operators. The key tool is the projection operator.

## §6.1. Classical measurement of classical states

Consider a classical register, call it $A$, with alphabet

$$\mathcal{X} = \{0, 1, \ldots, d-1\}.$$

Suppose this register is in the state

$$\rho = \begin{bmatrix} q_0 & & \\ & \ddots & \\ & & q_{d-1} \end{bmatrix}, \qquad q_j = \mathbb{P}[X = j],$$

where $X$ is the classical random variable stored in $A$. One of the $d$ values $0, \ldots, d-1$ is contained in $A$; the probabilities $\{q_j\}$ are the priors which reflect our ignorance about the exact value contained in $A$. When we measure the register $A$:

- we see the outcome $X = j$ (if $j$ is indeed the value in $A$), and this event occurs with probability $q_j$;
- if the outcome is $X = j$, then the post-measurement state of $A$ is $|j\rangle\langle j|$.

Our goal is to express both of these facts in terms of linear operators acting on $\rho$.

Note that the classical measurement process does not change the actual value stored in $A$; what changes is our belief about the value contained in this register. This is reflected in the change in the state of the register:

$$\begin{bmatrix} q_0 & & \\ & \ddots & \\ & & q_{d-1} \end{bmatrix} \rightarrow |j\rangle\langle j|.$$

In case we measure the classical register and do not observe the measurement outcome, then there is no update to our beliefs, so the state of the system remains the same. This is captured by the following analysis: the measurement outcome (the 'reading' from a measurement device) is $j$ with probability $q_j$, and if the measurement outcome is $j$, then the post-measurement state (our updated belief) is $|j\rangle\langle j|$; if we do not see the measurement outcome we must average over these updated beliefs (posterior probability distributions) arriving at

$$\sum_j q_j |j\rangle\langle j| = \rho,$$

which is the pre-measurement state.

Later, we will see that in the quantum scenario a measurement can change the 'value' stored in a quantum register apart from updating our belief about the state of the system. Even if we do not observe the measurement outcome, a quantum measurement *can* change the state of a quantum system.

## §6.2. Classical measurement in terms of projections

**Review of projection operators.** We will use orthogonal projections to describe classical measurement (we will extend this to the quantum case in a later lecture). For brevity, we will refer to orthogonal projections simply as projections.

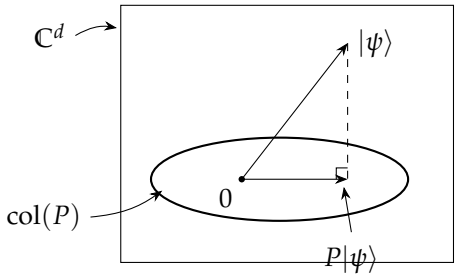
**DEFINITION.** *An operator $P$ is an* (orthogonal) projection *if*

$$P^\dagger = P \qquad \textit{and} \qquad P^2 = P.$$

Let $\mathrm{col}(P)$ denote the column space of $P$, a subspace of $\mathbb{C}^d$. For any $|\psi\rangle \in \mathbb{C}^d$,

$$P|\psi\rangle = \text{the vector in } \mathrm{col}(P) \text{ that is closest to } |\psi\rangle.$$

That is, $P|\psi\rangle$ is the foot of the perpendicular dropped from $|\psi\rangle$ onto $\mathrm{col}(P)$.




In particular, if $|\psi\rangle \in \mathrm{col}(P)$, then the closest vector is $|\psi\rangle$ itself, so

$$P|\psi\rangle = |\psi\rangle.$$

That is, if $|\psi\rangle \neq 0$, then $|\psi\rangle$ is an eigenvector of $P$ with eigenvalue $+1$.

EXAMPLE. *The $d \times d$ matrix*

$$P = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} = |0\rangle\langle 0|$$

*is a projection operator. Also, for any $|\psi\rangle \in \mathbb{C}^d$ with $\||\psi\rangle\| = 1$, the operator $|\psi\rangle\langle\psi|$ is a projection operator.*

EXAMPLE. *Every subspace $W$ of $\mathbb{C}^d$ has a unique projection operator $P$ such that $\mathrm{col}(P) = W$. One can construct $P$ as follows: for any choice of orthonormal basis $\{|\phi_j\rangle\}$ for $W$ we have*

$$P = \sum_j |\phi_j\rangle\langle\phi_j|.$$

**Linear operator language for classical measurement.** Consider again the classical register $A$ in the state

$$\rho = \begin{bmatrix} q_0 & & \\ & \ddots & \\ & & q_{d-1} \end{bmatrix}.$$

We observe the outcome $X = j$ with probability

$$q_j = \mathrm{Tr}\big(|j\rangle\langle j|\,\rho\big).$$

Indeed, $|j\rangle\langle j|$ is the matrix with a 1 in position $(j,j)$ and 0 elsewhere, so

$$|j\rangle\langle j|\,\rho = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix} \begin{bmatrix} q_0 & & & \\ & \ddots & & \\ & & & q_{d-1} \end{bmatrix}$$

is the diagonal matrix whose only non-zero entry is $q_j$, in position $(j,j)$. Its trace is $q_j$. Let us define the projection operators $P_0, P_1, \ldots, P_{d-1}$ by

$$P_j = |j\rangle\langle j|.$$

Then, since $P_j^2 = P_j$, $P_j^\dagger = P_j$ and the trace is cyclic ($\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$),

$$\begin{aligned} q_j &= \mathrm{Tr}\big(P_j\rho\big) \\ &= \mathrm{Tr}\big(P_j^2\rho\big) = \mathrm{Tr}\big(P_jP_j\rho\big) \\ &= \mathrm{Tr}\big(P_j\rho P_j\big) = \mathrm{Tr}\big(P_j\rho P_j^\dagger\big). \end{aligned}$$

Thus, we have an expression for the probabilities of the measurement outcomes:

$$\mathbb{P}[\text{outcome is } j] = \mathrm{Tr}\big(P_j\rho P_j^\dagger\big).$$

Suppose the measurement outcome is $X = j$ (assuming $q_j > 0$; otherwise we do not bother about this event). Then the post-measurement state is

$$|j\rangle\langle j| = \frac{1}{q_j}\cdot q_j|j\rangle\langle j| = \frac{1}{q_j}\begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & q_j & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix},$$

where $q_j$ sits in position $(j,j)$. The matrix on the right is exactly $P_j\rho P_j^\dagger$, so the post-measurement state is

$$|j\rangle\langle j| = \frac{1}{q_j}\,P_j\rho P_j^\dagger = \frac{P_j\rho P_j^\dagger}{\mathrm{Tr}\big(P_j\rho P_j^\dagger\big)}.$$

**Observe.** The projections $P_0, \ldots, P_{d-1}$ defined above have two important properties.

(1) For all $i, j$,

$$P_iP_j = \begin{cases} P_i, & i = j, \\ 0, & i \neq j. \end{cases}$$

Indeed, $P_iP_j = |i\rangle\langle i\,|\,j\rangle\langle j|$, and $\langle i\,|\,j\rangle$ is 1 if $i = j$ and 0 otherwise. Hence, if $i \neq j$, then $P_i$ and $P_j$ perform projections onto mutually orthogonal subspaces, namely $\mathrm{span}\{|i\rangle\}$ and $\mathrm{span}\{|j\rangle\}$.

(2) The *completeness condition*

$$\sum_{j=0}^{d-1} P_j = I.$$

This is the resolution of the identity from Lecture 1 and reflects the fact that the measurement outcomes exhaust all possibilities.

## §6.3. Generalizing classical measurement of classical states

As before, the random variable $X$ is stored in the register $A$, and a measuring device reads the register. Now, instead of reporting the value of $X$ itself, the device reports only partial information about $X$, determined as follows:

- partition the alphabet $\{0, 1, \ldots, d-1\}$ into $L$ subsets $S_1, S_2, \ldots, S_L$;
- fix real numbers $\lambda_1, \lambda_2, \ldots, \lambda_L$, all distinct;
- the device outputs $\lambda_\ell$ if $X \in S_\ell$.

The measurement of §6.1 is the special case $L = d$, where each subset $S_\ell$ contains a single symbol.

EXAMPLE. *Consider a 2-bit register $A$ with alphabet $\{00, 01, 10, 11\}$. Suppose we connect a measurement device to the first bit of this register and read its contents; say, the device outputs $-5$ volts if this bit is 0 and $+5$ volts if this bit is 1. This situation is captured by*

$$L = 2, \quad S_1 = \{00, 01\}, S_2 = \{10, 11\}, \quad \lambda_1 = -5, \lambda_2 = +5.$$

Again, we want to describe the measurement outcome probabilities and the post-measurement states using projection operators.

**Measurement outcomes.** The probability of the outcome $\lambda_\ell$ is

$$\begin{aligned} \mathbb{P}[\lambda_\ell] = \mathbb{P}[X \in S_\ell] &= \sum_{j \in S_\ell} q_j \\ &= \sum_{j \in S_\ell} \mathrm{Tr}\big(|j\rangle\langle j|\,\rho\big) \\ &= \mathrm{Tr}\Big(\sum_{j \in S_\ell} |j\rangle\langle j|\,\rho\Big), \end{aligned}$$

using the linearity of the trace. Let

$$P_\ell = \sum_{j \in S_\ell} |j\rangle\langle j|.$$

(Here $P_\ell$ is indexed by the subset $S_\ell$, unlike in the previous section where $P_j = |j\rangle\langle j|$ for $j \in \mathcal{X}$.) Then

$$\mathbb{P}[\lambda_\ell] = \mathrm{Tr}\big(P_\ell\,\rho\big).$$

Note that $P_\ell$ is a projection operator. It is Hermitian, being a sum of Hermitian matrices, and by fact (1) of §6.2,

$$P_\ell^2 = \sum_{i \in S_\ell} \sum_{j \in S_\ell} |i\rangle\langle i\,|\,j\rangle\langle j| = \sum_{j \in S_\ell} |j\rangle\langle j| = P_\ell.$$

Thus,

$$\mathbb{P}[\lambda_\ell] = \mathrm{Tr}(P_\ell \rho) = \mathrm{Tr}(P_\ell \rho P_\ell^\dagger).$$

**Post-measurement state.** Suppose the measurement outcome is $\lambda_\ell$ (assume $\mathbb{P}[\lambda_\ell] > 0$). Given this fact, i.e., given that $X \in S_\ell$, what is the probability mass function of $X$? We need

$$\mathbb{P}\big[X = j \,\big|\, X \in S_\ell\big] \qquad \text{for all } j = 0, 1, \ldots, d-1.$$

By the definition of conditional probability,

$$\mathbb{P}\big[X = j \,\big|\, X \in S_\ell\big] = \frac{\mathbb{P}[X = j,\ X \in S_\ell]}{\mathbb{P}[X \in S_\ell]} = \frac{\mathbb{P}[X = j] \cdot \mathbb{P}\big[X \in S_\ell \,\big|\, X = j\big]}{\mathbb{P}[X \in S_\ell]}.$$

There are two cases.

- If $j \notin S_\ell$, then $\mathbb{P}[X \in S_\ell \mid X = j] = 0$, and hence

$$\mathbb{P}\big[X = j \,\big|\, \lambda_\ell\big] = 0.$$

- If $j \in S_\ell$, then $\mathbb{P}[X \in S_\ell \mid X = j] = 1$, and hence

$$\begin{aligned}\mathbb{P}\big[X = j \,\big|\, \lambda_\ell\big] &= \frac{\mathbb{P}[X = j]}{\mathbb{P}[X \in S_\ell]} = \frac{\mathbb{P}[X = j]}{\operatorname{Tr}(P_\ell \rho)} \\ &= \frac{q_j}{\operatorname{Tr}\big(P_\ell \rho P_\ell^\dagger\big)} = \frac{q_j}{\mathbb{P}[\lambda_\ell]}.\end{aligned}$$

For instance, say $S_\ell = \{1, d-1\}$. Then the measurement acts on the state as follows:

$$\begin{bmatrix} q_0 & & & \\ & q_1 & & \\ & & \ddots & \\ & & & q_{d-1} \end{bmatrix} \xrightarrow[\text{outcome } \lambda_\ell]{\text{measurement}} \frac{1}{\mathbb{P}[\lambda_\ell]} \begin{bmatrix} 0 & & & \\ & q_1 & & \\ & & 0 & \\ & & & \ddots \\ & & & & q_{d-1} \end{bmatrix}.$$

In general, the post-measurement state keeps the diagonal entries $q_j$ with $j \in S_\ell$, sets all other entries to 0, and divides by $\mathbb{P}[\lambda_\ell]$. Since $P_\ell \rho P_\ell^\dagger$ is exactly the diagonal matrix with entries $q_j$ for $j \in S_\ell$ and 0 elsewhere, the post-measurement state is

$$\frac{P_\ell \rho P_\ell^\dagger}{\mathbb{P}[\lambda_\ell]} = \frac{P_\ell \rho P_\ell^\dagger}{\operatorname{Tr}\big(P_\ell \rho P_\ell^\dagger\big)}.$$

This reflects the update to our belief once we observe the measurement outcome to be $\lambda_\ell$.

**Example.** Let the alphabet be

$$\mathcal{X} = \{0, 1, 2, 3\},$$

and consider the partition

$$S_1 = \{0, 2\} \;\longrightarrow\; \lambda_1 = +1, \qquad S_2 = \{1, 3\} \;\longrightarrow\; \lambda_2 = -1.$$

This measurement device reports whether $X$ is even or odd. The corresponding projections are

$$P_1 = |0\rangle\langle 0| + |2\rangle\langle 2| = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{bmatrix}, \qquad P_2 = |1\rangle\langle 1| + |3\rangle\langle 3| = \begin{bmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 1 \end{bmatrix}.$$

As a check, $P_1 + P_2 = I$. Suppose the pre-measurement state is

$$\rho = \begin{bmatrix} 1/3 & & & \\ & 1/3 & & \\ & & 1/3 & \\ & & & 0 \end{bmatrix}.$$

*Measurement outcomes.* Since

$$P_1 \rho = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{bmatrix} \begin{bmatrix} 1/3 & & & \\ & 1/3 & & \\ & & 1/3 & \\ & & & 0 \end{bmatrix} = \begin{bmatrix} 1/3 & & & \\ & 0 & & \\ & & 1/3 & \\ & & & 0 \end{bmatrix},$$

we get

$$\mathbb{P}[\lambda_1] = \mathrm{Tr}\big(P_1\rho\big) = \frac{2}{3}.$$

Similarly,

$$\mathbb{P}[\lambda_2] = \mathrm{Tr}\big(P_2\rho\big) = \mathrm{Tr}\left(\begin{bmatrix} 0 & & \\ & 1 & \\ & & 0 \\ & & & 1 \end{bmatrix} \begin{bmatrix} 1/3 & & & \\ & 1/3 & & \\ & & 1/3 & \\ & & & 0 \end{bmatrix}\right),$$

that is,

$$\mathbb{P}[\lambda_2] = \mathrm{Tr}\begin{bmatrix} 0 & & & \\ & 1/3 & & \\ & & 0 & \\ & & & 0 \end{bmatrix} = \frac{1}{3}.$$

*Post-measurement state.* If the outcome is $\lambda_1$, the post-measurement state is

$$\frac{P_1\rho P_1^\dagger}{\mathrm{Tr}\big(P_1\rho P_1^\dagger\big)} = \frac{1}{2/3}\begin{bmatrix} 1/3 & & & \\ & 0 & & \\ & & 1/3 & \\ & & & 0 \end{bmatrix} = \begin{bmatrix} 1/2 & & & \\ & 0 & & \\ & & 1/2 & \\ & & & 0 \end{bmatrix}.$$

If the outcome is $\lambda_2$, the post-measurement state is

$$\frac{P_2\rho P_2^\dagger}{\mathrm{Tr}\big(P_2\rho P_2^\dagger\big)} = \frac{1}{1/3}\begin{bmatrix} 0 & & & \\ & 1/3 & & \\ & & 0 & \\ & & & 0 \end{bmatrix} = \begin{bmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{bmatrix}.$$

In the first case, $X$ is equally likely to be 0 or 2; in the second case, $X = 1$ with certainty.

# *Homework 3*

1. Consider the Hilbert space $\mathbb{C}^d$, and let $\{|\psi_i\rangle : i = 0, \ldots, d-1\}$ be any orthonormal basis (this need not be the standard basis). Let $P_i = |\psi_i\rangle\langle\psi_i|$.

   (a) Check if $P_i$ is a projection operator.

   (b) Find the rank and the column space of $P_i$.

   (c) Verify $P_i P_j = 0$ if $i \neq j$.

   (d) Verify completeness condition.

   REMARK. When we choose $|\psi_i\rangle = |i\rangle$, i.e., when the orthonormal basis used for measurement is the standard basis, we say that we 'perform measurement in the computational basis.'

2. Let $P$ and $Q$ be projection operators such that $PQ = 0$.

   (a) Find $QP$.

   (b) If $|\psi\rangle$ is an eigenvector of $Q$ with eigenvalue 1, then find the value of $P|\psi\rangle$.

   (c) Is $P + Q$ a projection operator?

   REMARK. In this case, one can show that $\text{rank}(P+Q) = \text{rank}(P) + \text{rank}(Q)$, and $P + Q$ projects onto the subspace obtained as the 'sum' of the column spaces of $P$ and $Q$.

3. If $P$ is a projection operator, is $I - P$ a projection operator too? Are the column spaces of $P$ and $I - P$ orthogonal to each other?

4. Consider classical measurement of classical states as done in Lecture 6, i.e., consider a partition $S_1, \ldots, S_L$ of $\{0, 1, \ldots, d-1\}$ and distinct real numbers $\lambda_1, \ldots, \lambda_L$. The measurement device outputs $\lambda_\ell$ if the classical random variable $X$ stored in the classical register belongs to $S_\ell$, i.e., $X \in S_\ell$.

   Define an operator $M = \sum_{\ell=1}^{L} \lambda_\ell P_\ell$, where $P_\ell = \sum_{j \in S_\ell} |j\rangle\langle j|$.

   (a) What does the value $\text{Tr}\,(M\rho)$ denote/signify, where $\rho$ is a classical state?

   (b) What about $\text{Tr}\left(M^2\rho\right)$ ?

   REMARK. Note that $M$ is a Hermitian operator and it contains all the information about $P_1, P_2, \ldots$ and $\lambda_1, \lambda_2, \ldots$, that is, given the matrix $M$ we can find all $P_i$ and $\lambda_i$, this is how:

   - $\lambda_1, \ldots, \lambda_L$ are the distinct eigenvalues of $M$ (that is, all eigenvalues not counting repetitions).
   - $P_\ell$ is the projection onto the eigenspace corresponding to the eigenvalue $\lambda_\ell$. In particular, if the multiplicity of the eigenvalue $\lambda_\ell$ is $m_\ell$, then there will be $m_\ell$ orthonormal eigenvectors of $M$ with eigenvalue $\lambda_\ell$, say $|\psi_{\ell,1}\rangle, \ldots, |\psi_{\ell,m_\ell}\rangle$, then

   $$P_\ell = |\psi_{\ell,1}\rangle\langle\psi_{\ell,1}| + \cdots + |\psi_{\ell,m_\ell}\rangle\langle\psi_{\ell,m_\ell}|$$

   Such a matrix $M$, in the context of measurement, is called an *observable*.

5. This question is based on the remark of the last question (about observables). The *Pauli Z operator* is defined as

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

   (a) Find all the eigenvalues and eigenvectors of $Z$.

   (b) If $Z$ is used as an observable for a measurement, find the corresponding measurement outputs $\lambda_1, \lambda_2, \ldots$ and the projection operators $P_1, P_2, \ldots$.

   (c) Do the same for the observable $Z \otimes Z$.

6. Let $C = A \otimes B$. Verify the following.

   (a) $A$ and $B$ are unitary $\Rightarrow$ $C$ is unitary.

   (b) $A$ and $B$ are Hermitian $\Rightarrow$ $C$ is Hermitian.

   (c) $A$ and $B$ are skew-Hermitian $\Rightarrow$ $C$ is Hermitian.

7. **Unitary Diagonalizability.** We say that a square matrix $A$ is *unitarily diagonalizable* if there exists a unitary matrix $U$ and a diagonal matrix $\Lambda$ such that

$$A = U\Lambda U^\dagger.$$

   The characterization of unitarily diagonalizable matrices is well known:

$$A \text{ is unitarily diagonalizable if and only if } AA^\dagger = A^\dagger A.$$

   (a) Verify if the following matrices are unitarily diagonalizable: Hermitian, skew-Hermitian, unitary.

   (b) Verify that the columns of $U$ are the eigenvectors of $A$ and the diagonal entries of $\Lambda$ are the eigenvalues.
   HINT. Use the fact $AU = U\Lambda$.

   REMARK. $A$ is unitarily diagonalizable if and only if it has a complete orthonormal set of eigenvectors, i.e., $|\psi_1\rangle, \ldots, |\psi_d\rangle$ are an orthonormal basis of $\mathbb{C}^d$ and each $|\psi_i\rangle$ is an eigenvector of $A$. These $|\psi_i\rangle$ are precisely the columns of $U$.

8. Suppose $A$ and $B$ are unitarily diagonalizable, verify if $A \otimes B$ is unitarily diagonalizable. Find the eigenvalues and eigenvectors of $A \otimes B$ based on the eigenvalues and eigenvectors of $A$ and $B$.

9. **Kraus form of partial trace.** We consider applying the partial trace operation on an arbitrary $d_1 d_2 \times d_1 d_2$ matrix $R$ (that is, $R$ need not be a density operator).

   (a) Verify the following Kraus form

$$\mathrm{Tr}_B(R) = \sum_{j=0}^{d_2-1} \left(I_{d_1} \otimes \langle j|\right) R \left(I_{d_1} \otimes |j\rangle\right).$$

   You must check the completeness condition as well.
   REMARK. This expression is sometimes written in shorthand as

$$\sum_{j=0}^{d_2-1} \langle j|_B \, R \, |j\rangle_B$$

   (b) Find the Kraus form for tracing out $A$.

10. The *Pauli operators* are defined as follows

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

(a) Verify that every $2 \times 2$ Hermitian operator is a linear combination of the Pauli operators with *real coefficients* used for the linear combination.

(b) Is *every* $2 \times 2$ operator some complex linear combination of the Pauli operators? Do these operators form a basis for $\mathbb{C}^{2\times 2}$?

HINT. You must check that every $2 \times 2$ matrix is some linear combination of $I, X, Y, Z$, and you must also show that if $\alpha_1 I + \alpha_2 X + \alpha_3 Y + \alpha_4 Z = 0$, then all $\alpha_i = 0$.

(c) The *n-qubit Paulis* are the operators

$$\{A_1 \otimes \cdots \otimes A_n : A_i \in \{I, X, Y, Z\},\ i = 1, \ldots, n\}.$$

Argue that the $n$-qubit Paulis form a basis for $\mathbb{C}^{2^n \times 2^n}$.

11. **Applying a function based on a measurement outcome.** An experiment/operation that operates on classical states is described below. You must identify the Kraus form of this operation.

*Experiment.* A computer is programmed to act on a classical register $A$ as follows. The alphabet corresponding to the register is $\mathcal{X} = \{0, 1, 2, 3\}$. The register is initialized with an arbitrary classical state $\rho$, which is the input to this procedure/operation. The program first reads the value in the register $A$. If the value is 0 or 1, it applies a classical function

$$f : \{0, 1, 2, 3\} \to \{0, 1, \ldots, d-1\}$$

and writes the output to a classical register $B$. If the value in $A$ is 2 or 3, it applies a classical function

$$g : \{0, 1, 2, 3\} \to \{0, 1, \ldots, d-1\}$$

and writes the output to the register $B$. The state of the register $B$, call it $\sigma$, is the output of this operation.

Note that as a user of this computer you do not observe the outcome of the measurement (i.e., the process of reading the contents of $A$), only the computer reads the value available in register $A$, while you do not.

*Question.* Suppose the Kraus operators for the function $f$ are $K_1, \ldots, K_n$ and the Kraus operators for the function $g$ are $M_1, \ldots, M_n$, for some integer $n \geq 1$. Find the Kraus operators for the above procedure, whose input is the state $\rho$ of $A$ and whose output is the state $\sigma$ of $B$.

# *Lecture 7*

## §7.1. Quantum systems and pure states

**State space.** Associated with every quantum system is a Hilbert space. In this course we consider only systems whose Hilbert space is *finite dimensional*. This Hilbert space is called the *state space* of the system. If its dimension is $d$, we call the system a *$d$-level quantum system*, and we take the state space to be

$$\mathbb{C}^d.$$

**Classical states.** A $d$-level system can hold exactly one of $d$ distinct classical values. The corresponding $d$ states are the *computational basis states*; we identify them with the standard basis vectors of $\mathbb{C}^d$,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad |d-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

**Pure states.** Not every vector of $\mathbb{C}^d$ is a legitimate pure state: only the unit-norm vectors are, and two that differ only by a global phase represent the same state.

**DEFINITION.** *A* pure state *of a $d$-level quantum system is a vector of unit norm in the state space $\mathbb{C}^d$. Two unit vectors that differ by a global phase, $|\psi\rangle = e^{i\theta}|\phi\rangle$ for some $\theta \in \mathbb{R}$, represent the* same *physical state.*

To a pure state $|\psi\rangle \in \mathbb{C}^d$ we associate its *density operator*

$$\rho = |\psi\rangle\langle\psi|.$$

The density operator is insensitive to the global phase: if $|\psi\rangle = e^{i\theta}|\phi\rangle$ then

$$|\psi\rangle\langle\psi| = e^{i\theta}e^{-i\theta}|\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|,$$

so equivalent state vectors have the same density operator.

**Example: the qubit.** A 2-level quantum system is called a *qubit*. Its state space is $\mathbb{C}^2$ and its classical states are $|0\rangle$ and $|1\rangle$. Besides these we will often use

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \qquad |-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix},$$

$$|+i\rangle := \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}, \qquad |-i\rangle := \frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}.$$

Each is a unit vector, hence a valid pure state. Their density operators are the rank-one operators

$$|+\rangle\langle+| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \qquad |-\rangle\langle-| = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

**Properties of a pure-state density operator.** Write $\rho = |\psi\rangle\langle\psi|$ with $\|\psi\| = 1$.

1. *Unit trace:* $\mathrm{Tr}(\rho) = \mathrm{Tr}\big(|\psi\rangle\langle\psi|\big) = \langle\psi \,|\, \psi\rangle = \|\psi\|^2 = 1$.
2. *Rank one:* $\mathrm{rank}(\rho) = 1$, since $\rho$ maps every vector into the line spanned by $|\psi\rangle$, i.e., the column space of $\rho$ is the 1-dimensional subspace $\{\alpha|\psi\rangle : \alpha \in \mathbb{C}\}$.
3. *Hermitian:* $\rho^\dagger = \big(|\psi\rangle\langle\psi|\big)^\dagger = |\psi\rangle\langle\psi| = \rho$.
4. *Positive:* for every $|\phi\rangle \in \mathbb{C}^d$,

$$\langle\phi|\rho|\phi\rangle = \langle\phi \,|\, \psi\rangle\langle\psi \,|\, \phi\rangle = \big|\langle\phi \,|\, \psi\rangle\big|^2 \geq 0,$$

which is real and non-negative.

**Notation.** For an operator (matrix) $A$ we write

$$A \geq 0$$

to mean "$A$ is *positive*" (positive semidefinite): $A$ is Hermitian and $\langle\phi|A|\phi\rangle \geq 0$ for every $|\phi\rangle$. Property 4 above says $\rho \geq 0$.

REMARK. *For matrices over the complex field (such as the operators encountered in this course), we have*

$$\langle\phi|A|\phi\rangle \text{ is real and non-negative for all } |\phi\rangle \Rightarrow A^\dagger = A.$$

*This is stated as a question in one of the homework problems. Given this fact, the definition of a positive matrix reduces to a single condition: $\langle\phi|A|\phi\rangle$ is real and non-negative for all $|\phi\rangle$; Hermiticity is then automatic.*

*For matrices over the real field, the definition of positivity must retain the condition that $A$ be symmetric: over $\mathbb{R}$, symmetry does not follow from $\langle\phi|A|\phi\rangle \geq 0$.*

REMARK. *The notation $A \geq 0$ does not mean that all the entries of $A$ are positive or real; $A$ may have complex entries. It is simply a shorthand for the statement "$\langle\phi|A|\phi\rangle$ is real and non-negative for every $|\phi\rangle$".*

REMARK. *Global phase carries no physical meaning, but* relative *phase does. The vectors*

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \textit{and} \qquad \frac{e^{i\theta}|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}} = e^{i\theta}\,\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

*differ by a global phase and are the same state. But*

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \textit{and} \qquad \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$$

*differ by a relative phase between $|0\rangle$ and $|1\rangle$, and for $\theta \not\equiv 0 \pmod{2\pi}$ they are* different *states (for instance $\theta = \pi$ gives $|+\rangle$ versus $|-\rangle$).*

## §7.2. An example of a qubit: the Mach–Zehnder interferometer

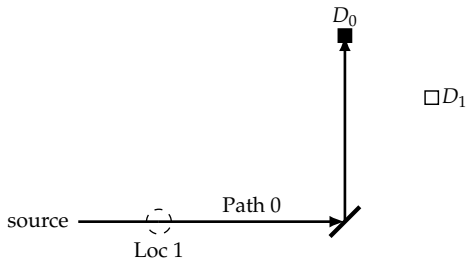
A concrete example of a qubit is the *which-path* degree of freedom of a single photon in a Mach–Zehnder interferometer; the treatment here follows Kaye, Laflamme, and Mosca, *An Introduction to Quantum Computing*, §1.6.

**The classical device.** Before any quantum behaviour enters, here is a purely classical way to use this apparatus to store one bit. The single-photon source points at a fixed spot we call Loc 1; two fixed fold mirrors then steer the light towards one of two detectors, $D_0$ and $D_1$. (Loc 1 is where the first beam splitter will later go; for now it is just a position in the setup.) A single choice fixes where the photon goes: whether or not a plain, fully reflecting mirror occupies Loc 1.

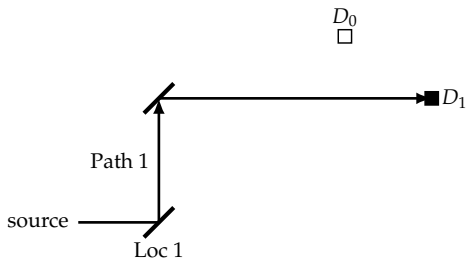
*No mirror at Loc 1* (Figure (a)): the photon passes straight through, follows Path 0, and is always registered at $D_0$. Call this configuration the classical state $|0\rangle$.

*A plain mirror at Loc 1* (Figure (b)): the photon is reflected onto Path 1 and is always registered at $D_1$. Call this configuration the classical state $|1\rangle$.

Each configuration sends the photon to a definite detector on every run, so the device has exactly two distinguishable settings — it holds one classical bit, with values $|0\rangle$ and $|1\rangle$.

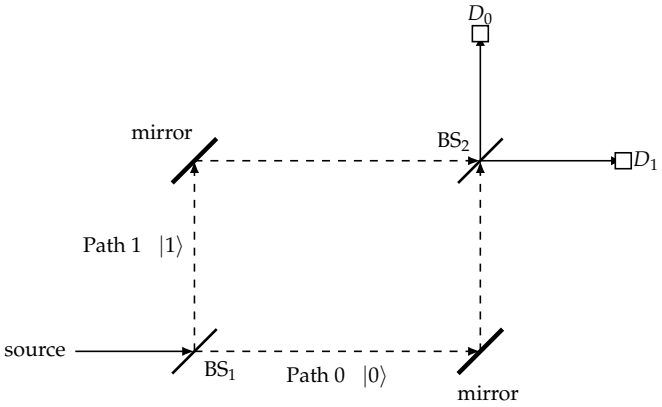



(a) no mirror at Loc 1: the photon always reaches $D_0$, giving the classical state $|0\rangle$




(b) a plain mirror at Loc 1: the photon always reaches $D_1$, giving the classical state $|1\rangle$

**Setup.** Now put a *beam splitter* $\mathrm{BS}_1$ — a quantum-mechanical device with no classical counterpart — at Loc 1, and a second, identical one, $\mathrm{BS}_2$, where the two paths recombine. In the figure below, the path segments lying between $\mathrm{BS}_1$ and $\mathrm{BS}_2$ are drawn dashed, as a reminder that the photon does not travel along a single definite path there.




**A beam splitter is a unitary.** Each beam splitter acts on the qubit as the unitary

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \qquad U^\dagger U = I.$$

In circuit language a gate $U$ takes $|\psi\rangle \mapsto U|\psi\rangle$.

**Tracking the photon.** The photon enters $BS_1$ in state $|0\rangle$. After $BS_1$,

$$U|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = |+i\rangle,$$

a superposition of the two paths. The photon travels on to $BS_2$, still in state $|+i\rangle$ — the fold mirrors redirect the beams but do not change the qubit — and after $BS_2$,

$$U|+i\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+i^2 \\ i+i \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 \\ 2i \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = e^{i\pi/2}|1\rangle \equiv |1\rangle.$$

The output is $|1\rangle$ (up to a global phase), so the photon leaves $BS_2$ on Path 1: detector $D_1$ clicks on every run, and $D_0$ never clicks.

**Superposition is not a classical mixture.** Suppose instead each beam splitter were a *classical random router*, sending the photon down Path 0 or Path 1 with probability $\frac{1}{2}$ each. Then the photon would arrive at a detector along a definite but random path, and $D_0$ and $D_1$ would each click with probability $\frac{1}{2}$. Experiment shows otherwise: only $D_1$ clicks. The state after $BS_1$ is therefore the superposition

$$|+i\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} \qquad \text{and } \textit{not} \text{ the mixture } \{\, (\tfrac{1}{2}, |0\rangle),\ (\tfrac{1}{2}, |1\rangle) \,\}.$$

REMARK. Where is the photon between $BS_1$ and $BS_2$? *There is no universally agreed answer; the question belongs to the* interpretation *of quantum mechanics. Several interpretations are in use — for example the Copenhagen (orthodox) interpretation, the many-worlds interpretation, and Bohmian mechanics — and the formalism predicts the same detector statistics under all of them.*

## §7.3. Mixed states and ensembles

**The quantum-information viewpoint.** We treat every pure state as a definite, non-random state. Randomness — a source that emits one of several states, each with some probability — is handled separately, via *ensembles* and the *mixed states* they define.

**Ensembles.** Consider a $d$-level system, and let $|\psi_1\rangle, \ldots, |\psi_n\rangle \in \mathbb{C}^d$ be pure states, where $n \geq 1$ is any integer. If the system is prepared in $|\psi_i\rangle$ with probability $p_i$, we call

$$\{\, (p_1, |\psi_1\rangle),\ (p_2, |\psi_2\rangle),\ \ldots,\ (p_n, |\psi_n\rangle) \,\}$$

an *ensemble* of pure states. The state of the system is the density operator

$$\rho = p_1 \, |\psi_1\rangle\langle\psi_1| + \cdots + p_n \, |\psi_n\rangle\langle\psi_n| = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i|, \qquad p_i \geq 0, \quad \sum_{i=1}^{n} p_i = 1.$$

A state that is not pure (that is, one for which no single $|\psi\rangle$ gives $\rho = |\psi\rangle\langle\psi|$) is called *mixed*.

**Examples ($d = 2$).**

1. $\{(\frac{1}{2}, |0\rangle),\ (\frac{1}{2}, |+\rangle)\}$:

$$\rho = \tfrac{1}{2} \, |0\rangle\langle 0| + \tfrac{1}{2} \, |+\rangle\langle +| = \tfrac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \tfrac{1}{2} \cdot \tfrac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{bmatrix}.$$

2. $\{(\frac{1}{2}, |+\rangle),\ (\frac{1}{2}, |-\rangle)\}$:

$$\rho = \tfrac{1}{2} \cdot \tfrac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \tfrac{1}{2} \cdot \tfrac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \tfrac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \tfrac{1}{2} I.$$

3. $\{(\frac{1}{2}, |0\rangle),\ (\frac{1}{2}, |1\rangle)\}$:

$$\rho = \tfrac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \tfrac{1}{2} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \tfrac{1}{2} I.$$

Examples 2 and 3 use different ensembles yet produce the *same* density operator $\frac{1}{2} I$: the preparation of a mixed state is *not unique*.

**Properties of an ensemble density operator.** Let $\rho = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i|$ with $p_i \geq 0$, $\sum_i p_i = 1$, and $\|\psi_i\| = 1$.

1. *Unit trace:*

$$\operatorname{Tr}(\rho) = \sum_{i=1}^{n} p_i \operatorname{Tr}\big(|\psi_i\rangle\langle\psi_i|\big) = \sum_{i=1}^{n} p_i = 1.$$

2. *Hermitian:* $\rho^\dagger = \sum_i p_i \big(|\psi_i\rangle\langle\psi_i|\big)^\dagger = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho$, since each $p_i$ is real.

3. *Positive:* for every $|\phi\rangle \in \mathbb{C}^d$,

$$\langle\phi|\rho|\phi\rangle = \sum_{i=1}^{n} p_i \, \langle\phi \,|\, \psi_i\rangle\langle\psi_i \,|\, \phi\rangle = \sum_{i=1}^{n} p_i \, \big|\langle\phi \,|\, \psi_i\rangle\big|^2 \geq 0,$$

   because each $p_i \geq 0$. Hence $\rho \geq 0$.

So every density operator — pure or mixed — satisfies

$$\operatorname{Tr}(\rho) = 1 \qquad \text{and} \qquad \rho \geq 0.$$

(Lecture 8 establishes the converse: any $\rho$ with these two properties is the density operator of some ensemble.)

**An ensemble is not a linear combination of kets.** An ensemble $\{(p_i, |\psi_i\rangle)\}$ is a probability distribution over pure states, not a vector. Resist the temptation to fold it into a single ket such as $\sum_i \sqrt{p_i}\,|\psi_i\rangle$ or $\sum_i p_i\,|\psi_i\rangle$: any such linear combination is one vector which represents a physically different situation.

For instance, the ensemble $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ has density operator $\frac{1}{2}I$, whereas the naive linear combination $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ has density operator $|+\rangle\langle+| = \frac{1}{2}\left[\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right]$. The nonzero off-diagonal entries are what a classical mixture lacks and a quantum superposition carries, and they have observable consequences: in §7.2 the pure state $|+i\rangle$ after $\mathrm{BS}_1$ triggers only $D_1$, whereas the mixture $\frac{1}{2}I$ would trigger each detector half the time.

From an information-theorist's viewpoint, the ensemble $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ is a random bit — a Bernoulli($\frac{1}{2}$) random variable. The ket $|+\rangle$, by contrast, involves no randomness at all: it is a single, definite pure state.

The correct representation of a mixed state is its density operator $\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$: a probability-weighted sum of the *operators* $|\psi_i\rangle\langle\psi_i|$, never a sum of vectors.

# *Lecture 8*

## §8.1. Characterization of states

**Recap.** Consider a $d$-level quantum system, with associated Hilbert space $\mathbb{C}^d$ as its *state space*. A *pure state* is a unit vector in $\mathbb{C}^d$. An *ensemble* of pure states $\{(p_i, |\psi_i\rangle)\}_{i=1}^n$ — a probability distribution $\{p_i\}$ over pure states $\{|\psi_i\rangle\}$ — generates the density operator

$$\rho = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i|.$$

Here $n$ can be any positive integer — larger than, equal to, or smaller than $d$. The pure states $|\psi_1\rangle, \ldots, |\psi_n\rangle$ can be any collection of unit vectors (linearly independent or not, orthonormal or not). For *any* such $\rho$ — whatever the distribution $\{p_i\}$ and whatever the unit vectors $|\psi_i\rangle$ — two properties hold:

$$\rho \geq 0 \qquad \text{and} \qquad \mathrm{Tr}(\rho) = 1.$$

*Positivity.* Recall that $\rho \geq 0$ means that $\rho$ is Hermitian and $\langle v|\rho|v\rangle \geq 0$ for every $|v\rangle \in \mathbb{C}^d$. Hermiticity is immediate: each $p_i$ is real and each rank-one term satisfies $\big(|\psi_i\rangle\langle\psi_i|\big)^\dagger = |\psi_i\rangle\langle\psi_i|$, so

$$\rho^\dagger = \sum_{i=1}^{n} p_i \, \big(|\psi_i\rangle\langle\psi_i|\big)^\dagger = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i| = \rho.$$

For the inequality, fix an arbitrary $|v\rangle \in \mathbb{C}^d$ and expand:

$$\langle v|\rho|v\rangle = \sum_{i=1}^{n} p_i \, \langle v \,|\, \psi_i\rangle\langle\psi_i \,|\, v\rangle = \sum_{i=1}^{n} p_i \, \big|\langle\psi_i \,|\, v\rangle\big|^2.$$

Each summand is the product of a non-negative weight $p_i$ and a non-negative number $|\langle\psi_i \,|\, v\rangle|^2$, so $\langle v|\rho|v\rangle \geq 0$. Hence $\rho \geq 0$; equivalently, all eigenvalues of $\rho$ are real and non-negative.

*Unit trace.* The trace is linear, and $\mathrm{Tr}(|\psi\rangle\langle\phi|) = \langle\phi \,|\, \psi\rangle$ for any two vectors. Taking $|\phi\rangle = |\psi\rangle = |\psi_i\rangle$ and using $\||\psi_i\rangle\| = 1$ gives $\mathrm{Tr}\big(|\psi_i\rangle\langle\psi_i|\big) = \langle\psi_i \,|\, \psi_i\rangle = 1$. Therefore

$$\mathrm{Tr}(\rho) = \sum_{i=1}^{n} p_i \, \mathrm{Tr}\big(|\psi_i\rangle\langle\psi_i|\big) = \sum_{i=1}^{n} p_i = 1,$$

since $\{p_i\}$ is a probability distribution.

Thus every quantum state satisfies both conditions:

$$\rho \text{ is a quantum state (pure or mixed)} \;\Rightarrow\; \rho \geq 0 \text{ and } \mathrm{Tr}(\rho) = 1.$$

**The converse.** The two conditions above are also *sufficient*.

**THEOREM.** *Suppose $\rho \in \mathbb{C}^{d\times d}$ satisfies*

1. $\rho \geq 0$, *and*
2. $\mathrm{Tr}(\rho) = 1$.

*Then $\rho$ can be prepared as a suitable ensemble of pure states, and hence represents a valid quantum state.*

*Proof.* Since $\rho \geq 0$, it is Hermitian, $\rho^\dagger = \rho$, and its eigenvalues are real and non-negative. By the spectral theorem, a Hermitian matrix on $\mathbb{C}^d$ has a *complete orthonormal set of eigenvectors*: there exist $d$ eigenvectors $|\psi_1\rangle, \ldots, |\psi_d\rangle$ of $\rho$ that are pairwise orthogonal and of unit norm,

$$\langle \psi_i \,|\, \psi_j \rangle = \delta_{ij}.$$

They are *complete* — they span all of $\mathbb{C}^d$, so every vector is a linear combination of them. Equivalently, $|\psi_1\rangle, \ldots, |\psi_d\rangle$ form an orthonormal basis of the state space.

Let $\lambda_i$ be the eigenvalue attached to $|\psi_i\rangle$, so $\rho|\psi_i\rangle = \lambda_i|\psi_i\rangle$, and collect the eigenvectors as the columns of

$$U = \big[\, |\psi_1\rangle \;\cdots\; |\psi_d\rangle \,\big].$$

Since the columns of $U$ are orthonormal, we have $U^\dagger U = I$, i.e. $U$ is unitary. Stacking the $d$ eigenvalue equations into a single matrix identity gives $\rho\, U = U\Lambda$ with $\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_d)$, that is,

$$\rho = U \Lambda U^\dagger.$$

Multiplying out column by column,

$$\rho = \big[\, |\psi_1\rangle \;\cdots\; |\psi_d\rangle \,\big] \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{bmatrix} \begin{bmatrix} \langle\psi_1| \\ \vdots \\ \langle\psi_d| \end{bmatrix} = \big[\, \lambda_1|\psi_1\rangle \;\cdots\; \lambda_d|\psi_d\rangle \,\big] \begin{bmatrix} \langle\psi_1| \\ \vdots \\ \langle\psi_d| \end{bmatrix}$$

$$= \sum_{i=1}^{d} \lambda_i \, |\psi_i\rangle\langle\psi_i|.$$

Now check the two hypotheses against this form: condition 1 gives $\lambda_i \geq 0$, and condition 2 gives $1 = \operatorname{Tr}(\rho) = \sum_i \lambda_i$. Hence $(\lambda_1, \ldots, \lambda_d)$ is a probability distribution, and $\sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ is precisely the density operator of the ensemble

$$\big\{\, (\lambda_i,\ |\psi_i\rangle) \,\big\}_{i=1}^{d}. \qquad \blacksquare$$

Combining the recap with the theorem, we arrive at the characterisation

$$\rho \text{ is a quantum state (pure or mixed)} \quad \Longleftrightarrow \quad \rho \geq 0 \text{ and } \operatorname{Tr}(\rho) = 1.$$

This motivates the next definition, which names the set of all valid states (pure and mixed) of a quantum system.

**Definition.** *The set of* density operators *on the Hilbert space* $\mathbb{C}^d$ *is*

$$\mathcal{D}(\mathbb{C}^d) = \big\{\, \rho \in \mathbb{C}^{d\times d} \;:\; \rho \geq 0,\ \ \operatorname{Tr}(\rho) = 1 \,\big\}.$$

## §8.2. Unitary freedom in state preparation

The main references for this section are Chapter 2 of Nielsen & Chuang, *Quantum Computation and Quantum Information*, and Chapter 2 of **John Preskill's lecture notes** for *Ph 219 / CS 219*.

For a given state $\rho$, we want to characterise all ensembles that yield it. To do so, we encode each ensemble in a matrix $B$ with $\rho = BB^\dagger$, and then invoke a matrix-theoretic fact that describes all such $B$.

**Two facts from matrix theory.**

(1) $A \geq 0$ if and only if $A = BB^\dagger$ for some matrix $B$ (which need not be square).

(2) Suppose $BB^\dagger = CC^\dagger = A$ and $B$ and $C$ have the *same number of columns*. Then $C = BU$ for some unitary matrix $U$.

**Equalising the number of columns.** When $B$ and $C$ have different numbers of columns, the mismatch is easily removed by appending all-zero columns to the smaller of the two, which changes neither $BB^\dagger$ nor $CC^\dagger$. Concretely, if $B = \big[\, |b_1\rangle \;\cdots\; |b_n\rangle \,\big]$, then

$$A = BB^\dagger = \big[\, |b_1\rangle \;\cdots\; |b_n\rangle \,\big] \begin{bmatrix} \langle b_1| \\ \vdots \\ \langle b_n| \end{bmatrix} = \sum_{i=1}^{n} |b_i\rangle\langle b_i|.$$

Appending zero columns changes nothing: with $\tilde{B} = \big[\, |b_1\rangle \;\cdots\; |b_n\rangle \;\; \mathbf{0} \,\big]$ (one or more zero columns),

$$\tilde{B}\tilde{B}^\dagger = \sum_{i=1}^{n} |b_i\rangle\langle b_i| + \mathbf{0}\,\mathbf{0}^\dagger = A.$$

So any factorisation of $A$ can be padded with zero columns to meet the equal-number-of-columns hypothesis of fact (2).

**Ensembles as factorisations.** If $\rho$ is generated by the ensemble $\{(p_i, |\psi_i\rangle)\}_{i=1}^n$, then

$$\rho = \sum_{i=1}^{n} p_i\, |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{n} \big(\sqrt{p_i}\,|\psi_i\rangle\big)\big(\sqrt{p_i}\,|\psi_i\rangle\big)^\dagger = BB^\dagger, \qquad B = \big[\, \sqrt{p_1}\,|\psi_1\rangle \;\cdots\; \sqrt{p_n}\,|\psi_n\rangle \,\big].$$

All the information in the ensemble — the probabilities $p_i$ and the pure states $|\psi_i\rangle$ — is contained in this matrix $B$, and it can be read back out as follows. Each $|\psi_i\rangle$ is a pure state and hence has unit norm, so the squared norm of the $i$-th column of $B$ is

$$\big\|\sqrt{p_i}\,|\psi_i\rangle\big\|^2 = p_i\,\||\psi_i\|^2 = p_i,$$

and dividing that column by $\sqrt{p_i}$ recovers $|\psi_i\rangle$ (assuming $p_i > 0$).

Note the difference between the information carried by $B$ and by $\rho$. The density operator $\rho$ is simply the final state of the register; it records nothing about how that state was prepared. The matrix $B$, by contrast, is a recipe for preparing a mixture: the squared norms of its columns are the ensemble probabilities, and its normalised columns are the ensemble's pure states. Moreover $\rho$ is always square, whereas $B$ may have any number of columns (one per pure state in the ensemble).

**Characterization of all ensembles for the same state.** Suppose $\rho$ is *also* generated by a second ensemble $\{(q_i, |\phi_i\rangle)\}_{i=1}^m$, and assume without loss of generality that $m \le n$. If $m < n$, extend the second ensemble by $n - m$ arbitrary pure states $|\phi_{m+1}\rangle, \ldots, |\phi_n\rangle$ carrying probability $q_{m+1} = \cdots = q_n = 0$; this does not change the state. Then

$$\rho = CC^\dagger, \qquad C = \big[\, \sqrt{q_1}\,|\phi_1\rangle \;\cdots\; \sqrt{q_n}\,|\phi_n\rangle \,\big],$$

and $B$, $C$ now have the same number of columns. By fact (2), $C = BU$ for some unitary $U$.

**THEOREM.** *Two ensembles $\{(p_i, |\psi_i\rangle)\}$ and $\{(q_i, |\phi_i\rangle)\}$, padded to the same number $n$ of pure states, generate the same density operator $\rho$ if and only if their matrices are related by a unitary transformation,*

$$\big[\, \sqrt{q_1}|\phi_1\rangle \;\cdots\; \sqrt{q_n}|\phi_n\rangle \,\big] = \big[\, \sqrt{p_1}|\psi_1\rangle \;\cdots\; \sqrt{p_n}|\psi_n\rangle \,\big]\, U, \qquad U \text{ unitary.}$$

**Example ($d = 2$).** Start from the ensemble $\big\{(\tfrac{1}{4}, |+\rangle),\ (\tfrac{3}{4}, |0\rangle)\big\}$, so

$$\rho = \tfrac{1}{4}\,|+\rangle\langle+| + \tfrac{3}{4}\,|0\rangle\langle 0| = \begin{pmatrix} \frac{7}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{1}{8} \end{pmatrix}.$$

The matrix that represents the recipe for this ensemble is

$$B = \left[\, \tfrac{1}{2}|+\rangle \quad \tfrac{\sqrt{3}}{2}|0\rangle \,\right] = \begin{pmatrix} \frac{1}{2\sqrt{2}} & \frac{\sqrt{3}}{2} \\ \frac{1}{2\sqrt{2}} & 0 \end{pmatrix}, \qquad BB^\dagger = \rho.$$

To obtain a different two-state ensemble for the same $\rho$, take $C = BU$ for any unitary $U$. For instance, with $U = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$:

$$C = BU = \begin{pmatrix} \dfrac{1+\sqrt{6}}{4} & \dfrac{1-\sqrt{6}}{4} \\ \dfrac{1}{4} & \dfrac{1}{4} \end{pmatrix}, \qquad CC^\dagger = \rho.$$

Reading $C = \left[\, \sqrt{q_1}|\phi_1\rangle \;\; \sqrt{q_2}|\phi_2\rangle \,\right]$ off column by column: $q_i$ is the squared norm of the $i$-th column of $C$ and $|\phi_i\rangle$ is that column normalised. Thus

$$q_1 = \frac{4+\sqrt{6}}{8}, \qquad q_2 = \frac{4-\sqrt{6}}{8}, \qquad q_1 + q_2 = 1,$$

$$|\phi_1\rangle = \frac{1}{\sqrt{q_1}} \begin{pmatrix} \frac{1+\sqrt{6}}{4} \\ \frac{1}{4} \end{pmatrix}, \qquad |\phi_2\rangle = \frac{1}{\sqrt{q_2}} \begin{pmatrix} \frac{1-\sqrt{6}}{4} \\ \frac{1}{4} \end{pmatrix}.$$

The ensemble $\big\{(q_1, |\phi_1\rangle),\ (q_2, |\phi_2\rangle)\big\}$ generates the same $\rho$, with a completely different pair of pure states and probabilities.

## §8.3. Composite quantum systems

Let $A$ be a system with state space $\mathbb{C}^{d_1}$ and computational basis $|0\rangle, \ldots, |d_1 - 1\rangle$, and let $B$ have state space $\mathbb{C}^{d_2}$ and computational basis $|0\rangle, \ldots, |d_2 - 1\rangle$. The composite system $AB$ has state space

$$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \;\cong\; \mathbb{C}^{d_1 d_2},$$

with computational basis the $d_1 d_2$ product vectors

$$\big\{\, |i\rangle \otimes |j\rangle \;:\; i = 0, \ldots, d_1 - 1,\;\; j = 0, \ldots, d_2 - 1 \,\big\}.$$

**States of $AB$.** A quantum state of $AB$ is a density operator $\rho \in \mathcal{D}(\mathbb{C}^{d_1 d_2})$, i.e. $\rho \in \mathbb{C}^{d_1 d_2 \times d_1 d_2}$ with $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$. A *pure* state of $AB$ is a unit vector $|\psi\rangle \in \mathbb{C}^{d_1 d_2}$; expanding it in the product basis,

$$|\psi\rangle = \sum_i \sum_j a_{ij}\, |i\rangle \otimes |j\rangle, \qquad \sum_i \sum_j |a_{ij}|^2 = 1.$$

**Product states.** If registers $A$ and $B$ are prepared independently, in states $\rho_1$ and $\rho_2$, then the joint state is

$$\rho = \rho_1 \otimes \rho_2,$$

called a *product state*. If the independent preparations are pure, $|\phi_1\rangle$ on $A$ and $|\phi_2\rangle$ on $B$, then

$$\rho = |\phi_1\rangle\langle\phi_1| \otimes |\phi_2\rangle\langle\phi_2| = \big(|\phi_1\rangle \otimes |\phi_2\rangle\big)\big(\langle\phi_1| \otimes \langle\phi_2|\big),$$

so $AB$ is in the pure state $|\phi_1\rangle \otimes |\phi_2\rangle$ — a product of two pure states.

**Not every pure state is a product.** A pure state of $AB$ need *not* be a product of a pure state on $A$ and a pure state on $B$.

Take $d_1 = d_2 = 2$, so $|\psi\rangle \in \mathbb{C}^4$ and

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \qquad \sum_{i,j} |a_{ij}|^2 = 1.$$

Preparing $A$ in $|+\rangle$ and $B$ in $|0\rangle$ independently gives the product state

$$|+\rangle \otimes |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Now instead suppose $AB$ is in the state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

called a *Bell state* or *EPR pair*, after Einstein, Podolsky, and Rosen.[1]

**Claim.** $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *is not a product state.*

*Proof.* Suppose, for contradiction, that it is a product state,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\gamma|0\rangle + \delta|1\rangle\big) = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle.$$

Comparing coefficients,

$$\alpha\gamma = \tfrac{1}{\sqrt{2}}, \qquad \alpha\delta = 0, \qquad \beta\gamma = 0, \qquad \beta\delta = \tfrac{1}{\sqrt{2}}.$$

From $\alpha\gamma \neq 0$ we get $\alpha \neq 0$, so $\alpha\delta = 0$ forces $\delta = 0$. But $\beta\delta = \frac{1}{\sqrt{2}} \neq 0$ requires $\delta \neq 0$ — a contradiction. Hence no such $\alpha, \beta, \gamma, \delta$ exist. ∎

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Phys. Rev.* **47**, 777 (1935), doi:10.1103/PhysRev.47.777. The original argument in the EPR paper was phrased for continuous position and momentum variables. See also a **popular-science video on the EPR paper**.

# *Homework 4*

1. **Positive quadratic forms and Hermitian matrices.** In the lectures, we defined an operator $A$ to be positive, i.e., $A \geq 0$ when

   - $A^\dagger = A$, and
   - $\langle\psi|A|\psi\rangle$ is real and non-negative for all $|\psi\rangle$.

   We will now show that the second condition implies the first, and hence, the first condition is superfluous. Our task now is to show the following

   $$\langle\psi|A|\psi\rangle \geq 0 \text{ for all } |\psi\rangle \Rightarrow A^\dagger = A.$$

   To do so we will use the fact $A = B + iC$ for some Hermitian operators $B, C$ (see Homework 1).

   (a) Considering $\langle\psi|A|\psi\rangle$, which is real, what can we say about $\langle\psi|B|\psi\rangle$ and $\langle\psi|iC|\psi\rangle$? Are they both real? Is one of them equal to 0?

   (b) $C$ is Hermitian and from part (a) we know that $\langle\psi|C|\psi\rangle = 0$ for every $|\psi\rangle$. Show that all eigenvalues of $C$ are zero, and using this show that $C = 0$. This implies that $A = B$ is Hermitian.
   HINT. Use the spectral decomposition of $C$, that is, $C$ is unitarily diagonalizable

   $$C = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|$$

   where $\{|\phi_k\rangle : k = 1, 2, \dots\}$ is an orthonormal basis of the associated Hilbert space.
   REMARK. If every eigenvalue of an operator is 0, it does not necessarily mean that the operator is 0, for example

   $$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

   In the question we are interested in, $C$ is diagonalizable, and this helps us prove that $C = 0$.

2. The *Hilbert-Schmidt* inner product between operators $A$ and $B$ is defined as

   $$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B).$$

   This is an inner product on the vector space of operators. Note that $\langle A, B\rangle$ and $\langle B, A\rangle$ are conjugates of each other. You must prove the following:

   (a) Show that $\langle A, A\rangle \geq 0$.
   HINT. What kind of operator is $A^\dagger A$?

   (b) (Remember the 4 Pauli matrices $I, X, Y, Z$; it is good to know them by heart.) For any two distinct Paulis, verify that the Hilbert-Schmidt inner product is zero.

   (c) Recall that any $2 \times 2$ matrix $A$ can be written as

   $$A = c_1 I + c_2 X + c_3 Y + c_4 Z$$

   for some complex scalars $c_1, \dots, c_4$. Show that $c_1 = \mathrm{Tr}(A)/2$ and $c_2 = \langle X, A\rangle/2$. What about $c_3$ and $c_4$?
   HINT. $\mathrm{Tr}(\alpha A + \beta B) = \alpha\mathrm{Tr}(A) + \beta\mathrm{Tr}(B)$.

REMARK. Under the Hilbert-Schmidt inner product the Paulis form an orthogonal (not orthonormal) basis for the space of $2 \times 2$ matrices.

3. **The Bloch ball.** The Bloch ball (which is the generalization of the Bloch sphere) is a representation of all qubit states, both pure and mixed. This is the unit ball in $\mathbb{R}^3$. The surface of this ball, which is the unit sphere, is called the Bloch sphere.

   Consider any state $\rho$ of a 2-level system (qubit). We will map this to a point in the unit ball. This will be the Bloch ball representation of $\rho$.

   (a) Given a qubit state $\rho$, show that there exist unique real numbers $s_i, s_x, s_y, s_z$ such that
   $$2\rho = s_i I + s_x X + s_y Y + s_z Z.$$
   HINT. Use the property that $\rho$ is a Hermitian operator.

   (b) Argue that $s_i = 1$.
   HINT. Use the fact $\mathrm{Tr}(\rho) = 1$.

   (c) Compute the eigenvalues of $\rho$ in terms of $s_x, s_y, s_z$. You will be able to show that the two eigenvalues (which are both real) are
   $$\frac{1 \pm s}{2}, \quad \text{where } s = \sqrt{s_x^2 + s_y^2 + s_z^2}.$$

   (d) Since $\rho$ is a density operator what is the allowable range of values for $s$?
   HINT. $\rho$ must be a positive operator. What do we know about its eigenvalues?

   (e) Argue that $\rho$ is pure when $s = 1$ and $\rho$ is mixed when $s < 1$.

   REMARK. The Bloch ball representation of $\rho$ is the real vector $(s_x, s_y, s_z)$. You have now shown that this real vector lies within the unit ball with center at $(0, 0, 0)$. The points on the surface ($s = 1$) are the pure states, and the points in the interior are all mixed states.

   The state corresponding to $s = 0$ is called the *completely mixed* or *maximally mixed* state (what is $\rho$ when $s = 0$?).

   Typically when noise affects a pure state qubit ($s = 1$) it transforms the qubit to mixed state ($s < 1$).

4. **Mixed States and Superposition.** Consider a photon where the quantum information is stored in its polarization state. The classical polarization states of the photon are $|0\rangle$ and $|1\rangle$, denoting horizontal and vertical polarization states, respectively.

   (a) Suppose a horizontally polarized photon is passed through an optical waveguide that transforms pure states as follows: $|\psi\rangle \to H|\psi\rangle$, where
   $$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ (this is known as the Hadamard gate).}$$
   What is the state of the photon after passing through the optical waveguide? Is this a pure state or a mixed state? Is the photon in a classical state after passing through the waveguide?

   (b) Suppose a randomized experiment creates a photon in horizontal polarization with probability $1/4$ and in vertical polarization with probability $3/4$. What is the ensemble representation of this photon? What is the state of this photon?

   (c) If the photon considered in part (b) is passed through the optical waveguide in part (a), what is the state of the photon after it passes through the waveguide?

5. **Cauchy–Schwarz and triangle inequalities.** The Cauchy–Schwarz inequality states that for any non-zero $|\phi\rangle, |\psi\rangle \in \mathbb{C}^d$ we have

$$|\langle\phi|\psi\rangle| \leq \||\phi\rangle\| \cdot \||\psi\rangle\|$$

and equality occurs if and only if $|\phi\rangle = \alpha|\psi\rangle$ for some $\alpha \in \mathbb{C}$. The inequality holds even if $|\phi\rangle$ or $|\psi\rangle$ is 0, but it is trivial in this case.

Use the Cauchy–Schwarz inequality to prove the triangle inequality:

$$\||\phi\rangle + |\psi\rangle\| \leq \||\phi\rangle\| + \||\psi\rangle\|.$$

HINT. Consider $\||\phi\rangle + |\psi\rangle\|^2 = (\langle\phi| + \langle\psi|)\,(|\phi\rangle + |\psi\rangle)$.

6. **Purity of a state.** Consider any $d$-level quantum system. The *purity* of a state $\rho$ is defined to be $\mathrm{Tr}(\rho^2)$. Show that the following are true for any density operator $\rho$

   (a) $\mathrm{Tr}(\rho^2) \leq 1$,

   (b) $\mathrm{Tr}(\rho^2) = 1$ if and only if $\rho$ is a pure state.

   HINT. Use the spectral decompositions of $\rho$ and $\rho^2$.

7. **Bounds on purity.** If $\rho$ is the state of a $d$-level system, you saw in the previous question that the purity $\mathrm{Tr}(\rho^2) \leq 1$. We will now derive a lower bound on purity using the Cauchy–Schwarz inequality.

   (a) Show that for any state $\rho$ of a $d$-level system we have

   $$\mathrm{Tr}(\rho^2) \geq \frac{1}{d}.$$

   HINT. You can use Cauchy–Schwarz to prove this, with $\||\phi\rangle\| = \sqrt{\mathrm{Tr}(\rho^2)}$ and $\||\psi\rangle\| = \sqrt{d}$. Identify a $|\phi\rangle$ and a $|\psi\rangle$ which will help you reduce purity lower bound to a Cauchy–Schwarz inequality.

   (b) Identify the unique state $\rho$ for which $\mathrm{Tr}(\rho^2) = 1/d$, and argue that there is only one state that satisfies this condition.

   REMARK. This is called the *maximally mixed* or the *completely mixed* state.

8. Suppose $\rho$ is any state of a $d$-level quantum system, and the rank of $\rho$ is $r$. Argue that if $\rho$ can be prepared using an ensemble of $n$ pure states then $n \geq r$. That is, to prepare a rank-$r$ state using an ensemble we need at least $r$ pure states in the ensemble.

   HINT. Use the rank-sum inequality $\mathrm{rank}(A + B) \leq \mathrm{rank}(A) + \mathrm{rank}(B)$.

# *Lecture 9*

## §9.1. Recap

A *pure state* $|\psi\rangle \in \mathbb{C}^d$ is a unit-norm vector in the state space. The *classical* (computational-basis) states are $|0\rangle, |1\rangle, \ldots, |d-1\rangle \in \mathbb{C}^d$. Any other pure state in this state space is a *superposition*

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \qquad \alpha_i \in \mathbb{C}, \quad \sum_i |\alpha_i|^2 = 1,$$

with more than one $\alpha_i$ nonzero. The condition $\sum_i |\alpha_i|^2 = 1$ is simply $\|\psi\|^2 = 1$.

For example, $\frac{1}{\sqrt{2}}\big(|0\rangle + i|1\rangle\big)$ is a superposition of $|0\rangle$ and $|1\rangle$.

Superposition states have no classical counterpart; they are a genuinely quantum phenomenon. Recall the superposition state of the photon in the Mach–Zehnder interferometer (MZI) experiment just after it passed the first beam splitter. Recall that the Copenhagen interpretation does not associate a specific path to this state of the photon (neither Path 0 nor Path 1).

**Superposition versus classical mixture.** The superposition state $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + i|1\rangle\big)$ must be carefully distinguished from the classical *ensemble* $\big\{ (\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle) \big\}$ — "the photon is on Path 0 or Path 1, each with probability $\frac{1}{2}$." In density-operator notation,

$$\rho_{\text{sup}} = |\psi\rangle\langle\psi| = \tfrac{1}{2}\big(|0\rangle + i|1\rangle\big)\big(\langle 0| - i\langle 1|\big) = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix},$$

$$\rho_{\text{mix}} = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \tfrac{1}{2} I.$$

The two have *identical diagonals*. They differ only in the *off-diagonal* entries: $\rho_{\text{sup}}$ has $(\rho_{\text{sup}})_{01} = -i/2 \neq 0$, whereas $\rho_{\text{mix}}$ is diagonal. These off-diagonal terms record the relative phase between the coefficients of $|0\rangle$ and $|1\rangle$. A classical probability distribution, such as the mixture above, has no such entries: its only nonzero entries are on the diagonal.

**MZI experiment distinguishes superposition from classical mixture.** Suppose each beam splitter merely directed an incoming photon into one of its two outgoing directions uniformly at random, rather than acting as a unitary operator. Then the photon leaving the first beam splitter would be described by $\rho_{\text{mix}}$, the second beam splitter would again split each path 50/50, and *both* detectors would click, each with probability $\frac{1}{2}$. Experimental observations show otherwise: only Detector 1 (Path 1) clicks, every time. This is possible only because the state after the first beam splitter is the superposition $\rho_{\text{sup}}$; the second beam splitter acts unitarily on this pure superposition state to yield the state $|1\rangle\langle 1|$.

**Composite systems.** If registers $A$ and $B$ are prepared independently, the joint state is a *product state*:

$$\rho_{AB} = \rho_A \otimes \rho_B, \qquad \text{or, for pure states,} \qquad |\psi\rangle_{AB} = |\psi_1\rangle \otimes |\psi_2\rangle.$$

**Marginals do not determine the joint state.** Given a joint state $\rho_{AB}$, its *marginals* (reduced states) are $\rho_A = \text{Tr}_B[\rho_{AB}]$ and $\rho_B = \text{Tr}_A[\rho_{AB}]$. The map $\rho_{AB} \mapsto (\rho_A, \rho_B)$ is many-to-one: a pair of marginals does *not* determine $\rho_{AB}$. For two qubits, each of the following composite

states has the *same* marginals $\rho_A = \rho_B = \frac{1}{2}I$ (trace out either qubit in each case).

$$\rho_{AB}^{(1)} = |\mathrm{EPR}\rangle\langle\mathrm{EPR}|, \qquad |\mathrm{EPR}\rangle = \tfrac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \quad \text{(pure state)},$$

$$\rho_{AB}^{(2)} = \tfrac{1}{2}I \otimes \tfrac{1}{2}I = \tfrac{1}{4}I_4 \quad \text{(classical, product state)},$$

$$\rho_{AB}^{(3)} = \tfrac{1}{2}|00\rangle\langle 00| + \tfrac{1}{2}|11\rangle\langle 11| \quad \text{(classical, dependent)},$$

Written out in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$,

$$\rho_{AB}^{(1)} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \qquad \rho_{AB}^{(2)} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \rho_{AB}^{(3)} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Yet the three joint states are physically very different. $\rho_{AB}^{(1)}$ is a pure state, and it exhibits a genuinely quantum feature: some of its off-diagonal entries are nonzero.

$\rho_{AB}^{(2)}$ is a classical state in which the four basis outcomes $00, 01, 10, 11$ are equally likely. There is no statistical dependence between the value of the first bit and that of the second, which is why it is a product state.

$\rho_{AB}^{(3)}$ is also a classical state, but it mixes only the outcomes 00 and 11, with equal probability. That is, the classical values in registers $A$ and $B$ are always the same (both 0 or both 1), and the two possibilities are equally likely. The states of the two registers are therefore not independent; this is an example of a classical statistical dependence between two Bernoulli random variables.

The information about the correlations between $A$ and $B$ is present in the operator $\rho_{AB}$, and we lose it when we look only at the marginals $\rho_A$ and $\rho_B$.

**Entanglement.** Entanglement is defined separately for pure and for mixed states; here we treat the pure-state case. The notion of entanglement for mixed states (which relies on the ideas of separable states and local operations and classical communication (LOCC)) will not be discussed in this course. It is useful to know, however, that the mixed-state definition of entanglement contains the pure-state definition as a special case. Thus we treat only the special case of pure states.

**DEFINITION.** *A pure state $|\psi\rangle$ on a bipartite system $AB$ is* entangled *if it is* not *a product state; that is, if*

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

*for every $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$.*

The canonical example is the EPR state

$$|\mathrm{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

**CLAIM.** *The EPR state is entangled; that is, it is not a product state.*

*Proof.* Suppose, for contradiction, that $|\mathrm{EPR}\rangle$ *is* a product state,

$$|\mathrm{EPR}\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\gamma|0\rangle + \delta|1\rangle\big) = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle,$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Comparing coefficients with $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ gives

$$\alpha\gamma = \tfrac{1}{\sqrt{2}}, \qquad \alpha\delta = 0, \qquad \beta\gamma = 0, \qquad \beta\delta = \tfrac{1}{\sqrt{2}}.$$

From $\alpha\gamma = \frac{1}{\sqrt{2}} \neq 0$ we get $\alpha \neq 0$; then $\alpha\delta = 0$ forces $\delta = 0$. But $\beta\delta = \frac{1}{\sqrt{2}} \neq 0$ requires $\delta \neq 0$ — a contradiction. Hence no such $\alpha, \beta, \gamma, \delta$ exist, and $|\mathrm{EPR}\rangle$ is not a product state. ∎

REMARK. *The only way to bring a bipartite system $AB$ into an entangled state is to let $A$ and $B$ physically interact. Independent preparation of $A$ and $B$ can only produce product states.*

## §9.2. Schmidt decomposition

The main reference for this section is Chapter 2 of Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (10th Anniversary Edition, Cambridge University Press, 2010).

**Setting.** Let $|\psi\rangle$ be a pure state on the bipartite system $AB$. The state space of register $A$ is $\mathbb{C}^{d_1}$, with computational basis

$$|0\rangle, |1\rangle, \ldots, |d_1 - 1\rangle,$$

and the state space of register $B$ is $\mathbb{C}^{d_2}$, with computational basis

$$|0\rangle, |1\rangle, \ldots, |d_2 - 1\rangle.$$

The state space of the composite system $AB$ is the tensor product

$$\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \;\cong\; \mathbb{C}^{d_1 d_2},$$

and its computational basis is the set of product vectors

$$\big\{\, |i\rangle \otimes |j\rangle \;:\; i = 0, 1, \ldots, d_1 - 1,\;\; j = 0, 1, \ldots, d_2 - 1 \,\big\},$$

which has $d_1 d_2$ elements. Expanding $|\psi\rangle$ in this basis,

$$|\psi\rangle = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} a_{ij} \, |i\rangle \otimes |j\rangle, \qquad a_{ij} \in \mathbb{C}.$$

A general description of $|\psi\rangle$ involves $d_1 d_2$ scalars $a_{ij}$, the coefficients of the basis vectors $|i\rangle \otimes |j\rangle$. The Schmidt decomposition provides a more economical description of $|\psi\rangle$ (with as few as $\min(d_1, d_2)$ terms), and one with useful mathematical structure. This structure lets us carry out the partial-trace operation quickly and reveals relationships between $\rho_A$ and $\rho_B$ that are not otherwise easy to see.

**THEOREM.** *Given a pure state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ (which may or may not be entangled), there exist*

(1) *an integer $r \in \{1, 2, \ldots, \min(d_1, d_2)\}$, called the* Schmidt rank *of $|\psi\rangle$;*

(2) *orthonormal vectors $|\psi_1\rangle, \ldots, |\psi_r\rangle \in \mathbb{C}^{d_1}$;*

(3) *orthonormal vectors $|\phi_1\rangle, \ldots, |\phi_r\rangle \in \mathbb{C}^{d_2}$;*

(4) *strictly positive real numbers $\mu_1, \ldots, \mu_r$, called the* Schmidt coefficients*;*

*such that*

$$|\psi\rangle = \sum_{k=1}^{r} \mu_k \, |\psi_k\rangle \otimes |\phi_k\rangle.$$

*The orthonormal sets $\{|\psi_k\rangle\}$ and $\{|\phi_k\rangle\}$ are called the* Schmidt bases *of $|\psi\rangle$ on $A$ and $B$.*

*Proof.* Collect the coefficients into a $d_1 \times d_2$ matrix $A = [a_{ij}]$, and let $r = \operatorname{rank}(A)$. Perform a (compact or economical) singular value decomposition of $A$:

$$A = UDV,$$

where

- $U$ is $d_1 \times r$ with orthonormal columns;

- $D$ is $r \times r$, real and diagonal with strictly positive entries $\mu_1, \ldots, \mu_r$;
- $V$ is $r \times d_2$ with orthonormal rows.

Write $u_{ik}$ for the entries of $U$ and $v_{kj}$ for the entries of $V$. In terms of entries,

$$a_{ij} = \sum_{k=1}^{r} u_{ik}\, \mu_k\, v_{kj}.$$

Substituting into $|\psi\rangle$,

$$\begin{aligned} |\psi\rangle &= \sum_i \sum_j a_{ij}\, |i\rangle \otimes |j\rangle = \sum_i \sum_j \sum_k u_{ik}\, \mu_k\, v_{kj}\, |i\rangle \otimes |j\rangle \\ &= \sum_k \mu_k \left[ \sum_i \sum_j u_{ik}\, v_{kj}\, |i\rangle \otimes |j\rangle \right] = \sum_k \mu_k \left( \sum_i u_{ik}\, |i\rangle \right) \otimes \left( \sum_j v_{kj}\, |j\rangle \right). \end{aligned}$$

Define $|\psi_k\rangle := \sum_i u_{ik} |i\rangle$ (the $k$-th column of $U$) and $|\phi_k\rangle := \sum_j v_{kj} |j\rangle$ (the transpose of the $k$-th row of $V$). Since $U$ has orthonormal columns, $\{|\psi_k\rangle\}$ is orthonormal; since $V$ has orthonormal rows, $\{|\phi_k\rangle\}$ is orthonormal. Hence

$$|\psi\rangle = \sum_{k=1}^{r} \mu_k\, |\psi_k\rangle \otimes |\phi_k\rangle. \qquad \blacksquare$$

REMARK. *The two expansions of the same state $|\psi\rangle$,*

$$|\psi\rangle = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} a_{ij}\, |i\rangle \otimes |j\rangle \qquad \textit{(computational-basis expansion)},$$

$$|\psi\rangle = \sum_{k=1}^{r} \mu_k\, |\psi_k\rangle \otimes |\phi_k\rangle \qquad \textit{(Schmidt form)},$$

*differ in structure:*

- Number of terms. *The first is a* double *sum with $d_1 d_2$ terms; the second is a* single *sum with only $r \leq \min(d_1, d_2)$ terms.*
- Bases. *In the first, the bases $\{|i\rangle\}$ on $A$ and $\{|j\rangle\}$ on $B$ are fixed in advance, and every pair $|i\rangle \otimes |j\rangle$ may appear. In the second, the bases $\{|\psi_k\rangle\}$ and $\{|\phi_k\rangle\}$ depend on $|\psi\rangle$ and are* paired*: the vector $|\psi_k\rangle$ on $A$ appears only together with $|\phi_k\rangle$ on $B$, sharing the single index $k$ — there are no "cross" terms $|\psi_k\rangle \otimes |\phi_l\rangle$ with $k \neq l$.*
- Coefficients. *The $a_{ij}$ are arbitrary complex numbers; the $\mu_k$ are strictly positive real numbers.*

**Reduced states of a pure bipartite state.** Assume $AB$ is in a pure state $|\psi\rangle$, written in Schmidt form $|\psi\rangle = \sum_{k=1}^{r} \mu_k |\psi_k\rangle \otimes |\phi_k\rangle$, and let $\rho_{AB} = |\psi\rangle\langle\psi|$. Expanding the outer product,

$$\rho_{AB} = \sum_k \sum_l \mu_k \mu_l\, \big(|\psi_k\rangle\langle\psi_l|\big) \otimes \big(|\phi_k\rangle\langle\phi_l|\big).$$

Tracing out $B$ uses $\mathrm{Tr}(|\phi_k\rangle\langle\phi_l|) = \langle\phi_l\,|\,\phi_k\rangle = \delta_{kl}$, and tracing out $A$ uses $\mathrm{Tr}(|\psi_k\rangle\langle\psi_l|) = \delta_{kl}$; in both cases only the terms with $k = l$ survive:

$$\rho_A = \mathrm{Tr}_B[\rho_{AB}] = \sum_{k=1}^{r} \mu_k^2\, |\psi_k\rangle\langle\psi_k|, \qquad \rho_B = \mathrm{Tr}_A[\rho_{AB}] = \sum_{k=1}^{r} \mu_k^2\, |\phi_k\rangle\langle\phi_k|.$$

**CLAIM.** *These are the* spectral decompositions *of $\rho_A$ and $\rho_B$: the Schmidt vectors are eigenvectors, and $\mu_1^2, \ldots, \mu_r^2$ are the nonzero eigenvalues.*

*Proof.* We argue for $\rho_A$; the argument for $\rho_B$ is identical with $|\psi_k\rangle$ replaced by $|\phi_k\rangle$. The Schmidt vectors $|\psi_1\rangle, \ldots, |\psi_r\rangle \in \mathbb{C}^{d_1}$ are orthonormal, so extend them to an orthonormal basis $|\psi_1\rangle, \ldots, |\psi_{d_1}\rangle$ of $\mathbb{C}^{d_1}$. Applying $\rho_A$ to a basis vector $|\psi_m\rangle$ and using $\langle\psi_k \,|\, \psi_m\rangle = \delta_{km}$,

$$\rho_A|\psi_m\rangle = \sum_{k=1}^{r} \mu_k^2 \,|\psi_k\rangle\langle\psi_k \,|\, \psi_m\rangle = \sum_{k=1}^{r} \mu_k^2 \,\delta_{km}\,|\psi_k\rangle = \begin{cases} \mu_m^2\,|\psi_m\rangle, & 1 \le m \le r, \\ 0, & r < m \le d_1. \end{cases}$$

So every $|\psi_m\rangle$ is an eigenvector of $\rho_A$, with eigenvalue $\mu_m^2 > 0$ for $m \le r$ and eigenvalue $0$ for $m > r$. Since $\{|\psi_m\rangle\}_{m=1}^{d_1}$ is an orthonormal basis, $I = \sum_{m=1}^{d_1} |\psi_m\rangle\langle\psi_m|$, and therefore

$$\rho_A = \rho_A\, I = \sum_{m=1}^{d_1} \big(\rho_A|\psi_m\rangle\big)\langle\psi_m| = \sum_{m=1}^{r} \mu_m^2\,|\psi_m\rangle\langle\psi_m|,$$

the zero-eigenvalue terms dropping out. This exhibits $\rho_A$ through a complete orthonormal set of eigenvectors with real eigenvalues — that is, its spectral decomposition. In particular the nonzero eigenvalues of $\rho_A$ are exactly $\mu_1^2, \ldots, \mu_r^2$, and $\operatorname{rank}\rho_A = r$. Finally, the Schmidt form gives $\langle\psi \,|\, \psi\rangle = \sum_{k,l} \mu_k\mu_l \,\langle\psi_k \,|\, \psi_l\rangle\langle\phi_k \,|\, \phi_l\rangle = \sum_{k=1}^{r} \mu_k^2$; hence $\operatorname{Tr}\rho_A = \sum_{k=1}^{r} \mu_k^2 = \langle\psi \,|\, \psi\rangle = 1$, and $\{\mu_k^2\}$ is a probability distribution. ∎

In matrix form,

$$\rho_A = \big[\,|\psi_1\rangle \;\cdots\; |\psi_r\rangle\,\big]_{d_1\times r} \begin{bmatrix} \mu_1^2 & & \\ & \ddots & \\ & & \mu_r^2 \end{bmatrix}_{r\times r} \begin{bmatrix} \langle\psi_1| \\ \vdots \\ \langle\psi_r| \end{bmatrix}_{r\times d_1}.$$

This is the compact (or economical) form of the eigendecomposition of $\rho_A$, which discards the eigenvectors corresponding to the zero eigenvalues.

**COROLLARY.** *$\rho_A$ and $\rho_B$ have identical nonzero eigenvalues, namely $\mu_1^2, \ldots, \mu_r^2$.*

The nonzero eigenvalues of these two operators are identical, including the multiplicities of any repeated eigenvalues. The number of zero eigenvalues, however, may differ between $\rho_A$ and $\rho_B$ (their dimensions $d_1$ and $d_2$ need not be equal). Since the rank equals the number of nonzero eigenvalues, we still have

$$\operatorname{rank}(\rho_A) = \operatorname{rank}(\rho_B).$$

**COROLLARY.** *Let $r$ be the Schmidt rank of the pure state $|\psi\rangle$ on $AB$. Then*

$$r = 1 \iff |\psi\rangle \text{ is a product state} \iff \rho_A,\ \rho_B \text{ are pure.}$$

*Proof.* By the spectral decompositions above, $\operatorname{rank}\rho_A = \operatorname{rank}\rho_B = r$, since $\mu_1^2, \ldots, \mu_r^2$ are strictly positive.

*($r = 1 \iff \rho_A, \rho_B$ are pure states).* A density operator is *pure* exactly when it has rank 1; hence

$$\rho_A \text{ is pure} \iff r = 1 \iff \rho_B \text{ is pure,}$$

which is the second equivalence. For the first:

*($r = 1 \Rightarrow$ product state).* If $r = 1$ the Schmidt decomposition has a single term, $|\psi\rangle = \mu_1\,|\psi_1\rangle \otimes |\phi_1\rangle$. Normalisation forces $\mu_1^2 = \langle\psi \,|\, \psi\rangle = 1$, so $\mu_1 = 1$ and $|\psi\rangle = |\psi_1\rangle \otimes |\phi_1\rangle$, a product state.

*(product state $\Rightarrow r = 1$).* If $|\psi\rangle = |a\rangle \otimes |b\rangle$ for unit vectors $|a\rangle \in \mathbb{C}^{d_1}$, $|b\rangle \in \mathbb{C}^{d_2}$, then

$$\rho_A = \operatorname{Tr}_B\big[|a\rangle\langle a| \otimes |b\rangle\langle b|\big] = |a\rangle\langle a|$$

is pure, and by the equivalence above $r = 1$. ∎

**COROLLARY.** *For a pure state $|\psi\rangle$ on $AB$ with Schmidt rank $r$,*

$$r > 1 \iff |\psi\rangle \text{ is entangled} \iff \rho_A,\ \rho_B \text{ are mixed.}$$

*Proof.* Since $r \geq 1$ always, "$r > 1$" is the negation of "$r = 1$"; "entangled" is by definition "not a product state"; and a density operator is mixed exactly when it is not pure. Negating each of the three statements in the previous corollary therefore gives this one. ■

## §9.3. Preparations of a mixed state

**Many preparations of the same state.** In general, a mixed state can be prepared in many ways: many different ensembles average to the same $\rho$, and many different pure states of a larger system reduce to it on tracing out the extra part (purifications; see Lecture 10).

The maximally mixed qubit state $\frac{1}{2}I$ is a case in point. Take the EPR state, whose density operator is

$$|\mathrm{EPR}\rangle\langle\mathrm{EPR}| = \tfrac{1}{2}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\big);$$

tracing out $B$ gives

$$\rho_A = \mathrm{Tr}_B\big[|\mathrm{EPR}\rangle\langle\mathrm{EPR}|\big] = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{1}{2}I,$$

and likewise $\rho_B = \frac{1}{2}I$. The same state is the average of the ensemble $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$, and also of $\{(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\}$:

$$\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| \;=\; \tfrac{1}{2}|+\rangle\langle +| + \tfrac{1}{2}|-\rangle\langle -| \;=\; \tfrac{1}{2}I.$$

In general a mixed state has *many* preparations.

**Indistinguishability of preparations.** The density operator $\rho$ is the *complete* description of a quantum system for the purpose of prediction: every measurement-outcome probability, every expectation value, and the result of every subsequent operation depends on the preparation *only through* $\rho$. Two preparation procedures that produce the same $\rho$ are therefore physically *indistinguishable*: no measurement, and no sequence of measurements and operations, can tell them apart. Watch Artur Ekert's **5 min video lecture** on quantum information science, where he explains this clearly.

*Classical analogue.* The phenomenon is not peculiar to quantum theory. "I flipped a fair coin" and "I secretly picked, with equal probability, a coin that always shows 0 or a coin that always shows 1, then reported its face" both produce the outcome distribution Bernoulli$(\frac{1}{2})$, and no experiment on the reported value distinguishes them. A third classical preparation yields the same distribution: "I secretly picked, with equal probability, a biased coin that shows 0 with probability 0.9 or a biased coin that shows 1 with probability 0.9, then reported its face." Here the two conditional distributions are Bernoulli$(0.1)$ and Bernoulli$(0.9)$, and their equal-weight average is again Bernoulli$(\frac{1}{2})$.

**Exploiting indistinguishability of preparations.** No quantum operation or measurement can distinguish two different preparations of the same state. We may therefore assume that a given state was prepared in whichever way is most convenient: the choice does not affect any prediction quantum theory makes about the outcomes of subsequent operations or measurements on that state. Depending on the problem, it can be helpful to assume that the state was prepared as an ensemble — possibly a particular ensemble, such as the eigenvectors of $\rho$ weighted by its eigenvalues — or as the reduction of a pure state on a larger composite system (a purification). Such an assumption can make a problem easier to solve.

# *Lecture 10*

## §10.1. Purification

Suppose a quantum system $A$ is in a mixed state $\rho_A$. We can associate with it a fictitious (purely mathematical) system $R$ — a *reference* system — and a *pure* state $|\psi\rangle$ on the composite system $AR$, so that the reduced state on $A$ is exactly $\rho_A$:

$$\rho_A = \mathrm{Tr}_R\big[|\psi\rangle\langle\psi|\big].$$

The bookkeeping is summarised below.

| | **Actual** | **Purification** |
|---|---|---|
| **System** | $A$ | $AR$ |
| **State** | $\rho_A$ on $A$ | $\|\psi\rangle$ on $AR$ |
| **Relation** | $\rho_A = \mathrm{Tr}_R\big[\|\psi\rangle\langle\psi|\big]$ | |

The pure state $|\psi\rangle$ is called a *purification* of $\rho_A$.

This mathematical convenience lets us work with *vectors* $\big(|\psi\rangle\big)$ instead of density operators $\big(\rho_A\big)$, and with *unitary operators* $\big(U\big)$ instead of Kraus operators and Kraus forms. It is a proof-and-analysis technique: the reference system $R$ need not exist physically.

REMARK. *Purification allows us to work with vectors instead of density operators by mapping our scenario to a larger Hilbert space (state space of $AR$ instead of state space of $A$). A logical counterpart of this tool, called the Stinespring dilation, allows us to view arbitrary quantum operations as unitary operators on a larger Hilbert space instead of working with the operator-sum representation or the Kraus form.*

*Later we will rely on Stinespring dilation, to show that if a quantum error correcting code can correct the errors $E_1$ and $E_2$, then it can also correct every linear combination $\alpha_1 E_1 + \alpha_2 E_2$, where $\alpha_1, \alpha_2 \in \mathbb{C}$.*

**The construction.**

**THEOREM.** *Given any state $\rho_A$ of register $A$, there exists a system $R$ and a pure state $|\psi\rangle$ on $AR$ such that* $\mathrm{Tr}_R(|\psi\rangle\langle\psi|) = \rho_A$.

*Proof.* Concretely, a purification can always be built as follows. Let $\rho_A$ have spectral decomposition

$$\rho_A = \sum_{k=1}^{r} \lambda_k \, |\phi_k\rangle\langle\phi_k|,$$

where $r = \mathrm{rank}(\rho_A)$ and $\{|\phi_1\rangle, \ldots, |\phi_r\rangle\}$ is a set of orthonormal vectors in the state space of the system $A$. Consider any fictitious system $R$ whose state-space dimension is at least $\mathrm{rank}(\rho_A) = r$, and let $|\zeta_1\rangle, \ldots, |\zeta_r\rangle$ be any $r$ orthonormal vectors in the state space of $R$. We are able to choose $r$ such orthonormal vectors only because the dimension of the state space of $R$ is at least $r$.

Note that it would even suffice to take $R$ with the same state space as $A$.

Define

$$|\psi\rangle_{AR} := \sum_{k=1}^{r} \sqrt{\lambda_k} \, |\phi_k\rangle \otimes |\zeta_k\rangle.$$

We now claim that with this choice of $|\psi\rangle$, we have

$$\mathrm{Tr}_R\big[|\psi\rangle_{AR}\langle\psi|_{AR}\big] = \sum_{k=1}^{r} \lambda_k\, |\phi_k\rangle\langle\phi_k| = \rho_A,$$

so $|\psi\rangle_{AR}$ is a purification of $\rho_A$.

One can immediately see that this is true by noticing that the expression used to construct $|\psi\rangle$ is precisely a Schmidt decomposition. From the discussion in Lecture 9, we can immediately gather that

$$\mathrm{Tr}_R\big[|\psi\rangle_{AR}\langle\psi|_{AR}\big] = \sum_{k=1}^{r} \lambda_k\, |\phi_k\rangle\langle\phi_k| = \rho_A.$$

Alternatively, we can expand the outer product $|\psi\rangle\langle\psi|$, and then trace out $R$ as follows

$$|\psi\rangle_{AR}\langle\psi|_{AR} = \sum_{k,l} \sqrt{\lambda_k\lambda_l}\, \big(|\phi_k\rangle\langle\phi_l|\big) \otimes \big(|\zeta_k\rangle\langle\zeta_l|\big).$$

By the partial-trace identity for Kronecker products from Lecture 5, $\mathrm{Tr}_R[C \otimes D] = \mathrm{Tr}(D)\, C$, so

$$\mathrm{Tr}_R\big[(|\phi_k\rangle\langle\phi_l|) \otimes (|\zeta_k\rangle\langle\zeta_l|)\big] = \mathrm{Tr}\big(|\zeta_k\rangle\langle\zeta_l|\big)\, |\phi_k\rangle\langle\phi_l| = \langle\zeta_l \,|\, \zeta_k\rangle\, |\phi_k\rangle\langle\phi_l| = \delta_{kl}\, |\phi_k\rangle\langle\phi_l|,$$

using orthonormality of the $|\zeta_k\rangle$. Hence only the diagonal terms survive:

$$\mathrm{Tr}_R\big[|\psi\rangle_{AR}\langle\psi|_{AR}\big] = \sum_{k} \lambda_k\, |\phi_k\rangle\langle\phi_k| = \rho_A. \qquad \blacksquare$$

REMARK. *It is common to say that "$|\psi\rangle_{AR}$ is a purification of the state $\rho_A$."*

**Freedom in the construction.** The vectors $|\zeta_1\rangle, \ldots, |\zeta_r\rangle$ may be *any* orthonormal set in $R$; different choices give different purifications of the same $\rho_A$. For instance, $|\zeta_1\rangle, |\zeta_2\rangle, \ldots$ can be chosen as $|0\rangle, |1\rangle, \ldots$ from the state space of $R$.

## §10.2. Closed quantum systems

**DEFINITION.** *A quantum system is* closed *if it does not interact with any external system — it exchanges no heat, energy, or information with other systems. A system that is not closed is called* open.

Closed quantum systems evolve unitarily across time. This is the *second postulate* of quantum mechanics: if $|\psi_i\rangle$ is the state of a closed system at time $t_i$, $i = 1, 2$, then

$$|\psi_2\rangle = U\,|\psi_1\rangle$$

for some unitary $U$. In density-matrix language, if the states at $t_1$ and $t_2$ are $\rho_1$ and $\rho_2$, then

$$\rho_2 = U\rho_1 U^\dagger.$$

**Properties of gates.** Such unitary evolution operators are called *gates*. We record the following facts.

1. The gates $e^{i\theta}U$ and $U$ act identically, since $(e^{i\theta}U)\rho(e^{i\theta}U)^\dagger = U\rho U^\dagger$; a global phase is an unobservable and computationally irrelevant quantity, so these two unitaries are considered *equivalent* gates.

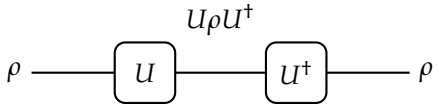
2. $U$ depends on the times $t_1$ and $t_2$ and on the *Hamiltonian* of the system, through Schrödinger's equation. In principle, by choosing the appropriate Hamiltonian and the duration $t_2 - t_1$, any unitary $U$ can be realised.

REMARK. *You can think of the Hamiltonian as a 'knob' or a parameter of the closed system that dictates how the system evolves with time. Changing the Hamiltonian changes the unitary gate arising from the time evolution.*

*For example, in the case of superconducting qubits (as used by Google and IBM), the qubits are realized as circuits containing capacitors and elements known as Josephson junctions, and the Hamiltonian is modified by applying an external field via microwave pulses.*

REMARK. *Although quantum theory allows any unitary to be realized this way, practical design of unitary gate operations is difficult. Typically, quantum hardware is built to implement a small set of unitary gates, and any other required unitary operation is realized (either exactly or approximately) as a product of gates from this small set.*

3. Unitary gates are *reversible*: $\rho \mapsto U\rho U^\dagger$ is undone by $\sigma \mapsto U^\dagger(\sigma)U$.




   In fact, unitaries are the only reversible operations in quantum mechanics.

4. Gates *preserve purity*: $\rho$ is pure if and only if $U\rho U^\dagger$ is pure, since $\text{rank}(\rho) = \text{rank}(U\rho U^\dagger)$.

5. A unitary $U$ is completely determined by its action on the computational basis $|0\rangle$, $|1\rangle$, $\ldots$, since $U|0\rangle$, $U|1\rangle$, $\ldots$ are the columns of $U$.

6. If a system $A$ does interact with its "environment" or "bath" $E$, we consider the composite system $AE$. This composite system is closed since it does not interact with any other system external to it. By the second postulate of quantum mechanics, $AE$ evolves unitarily over time. If $|\psi_1\rangle_{AE}$ and $|\psi_2\rangle_{AE}$ are the states at times $t_1$ and $t_2$, then

$$|\psi_2\rangle_{AE} = U\,|\psi_1\rangle_{AE}.$$

   Similarly, for mixed states, we have

$$\rho_2 = U\,\rho_1\,U^\dagger.$$

   REMARK. *This observation shows that unitaries play a fundamental role in quantum mechanics. Apart from measurement (which we will see in Lecture 11), these are the only physical operations that bring about a change in the state of a system:*

   - *if a system is closed, then it evolves unitarily according to the second postulate of quantum mechanics;*
   - *if a system is open, then it interacts with the environment — yielding a larger composite system that is closed — and this composite system evolves unitarily.*

   *Thus, apart from measurements, any change in the state of a system (open or closed) is brought about by unitary operations only.*

**The Pauli gates.** We now specialise to two-level systems (qubits). The Pauli gates are

$$I, \qquad X, \qquad Z, \qquad Y = iXZ.$$

In the computational basis $\{|0\rangle, |1\rangle\}$ their matrix forms are

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$X$ **(bit flip).** $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, so on a general state

$$X\big(\alpha|0\rangle + \beta|1\rangle\big) = \beta|0\rangle + \alpha|1\rangle.$$

It exchanges the two computational basis states, i.e. it interchanges the bit values 0 and 1. This is the quantum counterpart of the classical NOT gate, which is why $X$ is called the *bit-flip* gate. Recalling $|\pm\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \pm |1\rangle\big)$, its action on the four standard states is

$$\begin{aligned} X|0\rangle &= |1\rangle, & X|1\rangle &= |0\rangle, \\ X|+\rangle &= \tfrac{1}{\sqrt{2}}\big(X|0\rangle + X|1\rangle\big) = \tfrac{1}{\sqrt{2}}\big(|1\rangle + |0\rangle\big) = |+\rangle, \\ X|-\rangle &= \tfrac{1}{\sqrt{2}}\big(X|0\rangle - X|1\rangle\big) = \tfrac{1}{\sqrt{2}}\big(|1\rangle - |0\rangle\big) = -|-\rangle. \end{aligned}$$

So $X$ swaps $|0\rangle \leftrightarrow |1\rangle$ and fixes $|\pm\rangle$ (up to a sign).

*Eigenvalues and eigenvectors.* The last two lines say precisely that $|+\rangle$ and $|-\rangle$ are eigenvectors of $X$, with eigenvalues $+1$ and $-1$:

$$X|+\rangle = (+1)\,|+\rangle, \qquad X|-\rangle = (-1)\,|-\rangle.$$

*Spectral decomposition.* A Hermitian matrix $M$ on a $d$-dimensional state space is unitarily diagonalizable: it possesses a *complete orthonormal set of eigenvectors* $|v_1\rangle, \ldots, |v_d\rangle$ — eigenvectors that form an orthonormal basis of the state space — with real eigenvalues $\mu_1, \ldots, \mu_d$. Collecting them as the columns of the unitary $U = \big(|v_1\rangle \ \cdots \ |v_d\rangle\big)$, this reads $M = U\Lambda U^\dagger$ with $\Lambda = \mathrm{diag}(\mu_1, \ldots, \mu_d)$; multiplying out column by column gives the *spectral decomposition* of $M$,

$$M = \sum_{j=1}^{d} \mu_j\, |v_j\rangle\langle v_j|.$$

The rank-one terms $|v_j\rangle\langle v_j|$ are mutually orthogonal projectors that sum to $I$ (this is just $UU^\dagger = I$). For $X$, which is Hermitian, one such orthonormal eigenbasis of the qubit space is $\{|+\rangle, |-\rangle\}$, with eigenvalues $+1$ and $-1$; hence

$$X = (+1)\,|+\rangle\langle+| + (-1)\,|-\rangle\langle-| = |+\rangle\langle+| - |-\rangle\langle-|.$$

Expanding, $|+\rangle\langle+| - |-\rangle\langle-| = \frac{1}{2}\big[(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) - (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\big] = |0\rangle\langle 1| + |1\rangle\langle 0|$, which is indeed the matrix of $X$.

$Z$ **(phase flip).** $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$, so

$$Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle.$$

Note that the $Z$ gate does not affect the classical states $|0\rangle$ and $|1\rangle$. Its only effect is to negate the amplitude of $|1\rangle$, i.e. to insert a relative phase of $e^{i\pi} = -1$ between the two basis states (the relative phase is shifted by 180°). Because it flips the sign of this relative phase while leaving the bit unchanged, $Z$ is called the *phase-flip* gate. Its action on the four standard states is

$$\begin{aligned} Z|0\rangle &= |0\rangle, & Z|1\rangle &= -|1\rangle, \\ Z|+\rangle &= \tfrac{1}{\sqrt{2}}\big(Z|0\rangle + Z|1\rangle\big) = \tfrac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = |-\rangle, \\ Z|-\rangle &= \tfrac{1}{\sqrt{2}}\big(Z|0\rangle - Z|1\rangle\big) = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = |+\rangle. \end{aligned}$$

So $Z$ fixes $|0\rangle, |1\rangle$ and swaps $|+\rangle \leftrightarrow |-\rangle$: in the $\{|+\rangle, |-\rangle\}$ basis it acts exactly as $X$ does in the computational basis. Thus $X$ and $Z$ are the same operation viewed in two complementary bases.

*Eigenvalues and eigenvectors.* $|0\rangle$ and $|1\rangle$ are eigenvectors of $Z$, with eigenvalues $+1$ and $-1$:

$$Z|0\rangle = (+1)\,|0\rangle, \qquad Z|1\rangle = (-1)\,|1\rangle.$$

*Spectral decomposition.* Here the orthonormal eigenbasis is the computational basis $\{|0\rangle, |1\rangle\}$ itself (the diagonalizing unitary is $U = I$), so

$$Z = (+1)\,|0\rangle\langle 0| + (-1)\,|1\rangle\langle 1| = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

$Y = iXZ$**.** Applies both a bit flip and a phase flip.

REMARK. $X, Y, Z$ *pairwise* anticommute*:*

$$XY + YX = 0, \qquad YZ + ZY = 0, \qquad ZX + XZ = 0,$$

*equivalently* $XY = -YX,\ YZ = -ZY,\ ZX = -XZ$*. Their products are*

$$XY = iZ, \qquad YZ = iX, \qquad ZX = iY$$

*(and* $YX = -iZ$*,* $ZY = -iX$*,* $XZ = -iY$*). Each of* $X, Y, Z$ *is unitary, Hermitian, and traceless (i.e., trace is zero). Each has one* $+1$ *and one* $-1$ *eigenvalue, with eigenvectors*

$$X:\ |+\rangle,\ |-\rangle; \qquad Z:\ |0\rangle,\ |1\rangle; \qquad Y:\ |+i\rangle,\ |-i\rangle.$$

*Also, for each Pauli* $P$ *we have* $P^2 = I$*, hence* $P = P^\dagger = P^{-1}$*.*

## §10.3. Additional material not covered during lecture

**The Hadamard gate.** This single-qubit gate is

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \qquad H^\dagger = H^{-1} = H.$$

In Dirac notation,

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}}\Big[\big(|0\rangle + |1\rangle\big)\langle 0| + \big(|0\rangle - |1\rangle\big)\langle 1|\Big].$$

This follows from the general fact that a linear operator is fixed by its action on a basis: inserting the resolution of identity $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ gives $H = HI = \big(H|0\rangle\big)\langle 0| + \big(H|1\rangle\big)\langle 1|$, and substituting $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$ yields the expression above. (Equivalently, $H|0\rangle$ and $H|1\rangle$ are the columns of $H$.) Note this is *not* a spectral decomposition: $|0\rangle, |1\rangle$ are not eigenvectors of $H$, and the ket and bra in each term differ.

On the $\{|+\rangle, |-\rangle\}$ basis,

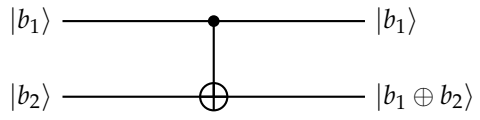
$$H|+\rangle = |0\rangle, \qquad H|-\rangle = |1\rangle.$$

This is immediate from $H = H^{-1}$: since $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, applying $H$ once more gives $H|+\rangle = H^2|0\rangle = |0\rangle$ and $H|-\rangle = H^2|1\rangle = |1\rangle$.

**The CNOT gate.** This is a 2-qubit gate, that is, it acts on a composite system of 2 qubits. Hence, it acts on $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$, and is thus a $4 \times 4$ matrix. The controlled-NOT gate acts on the computational basis by

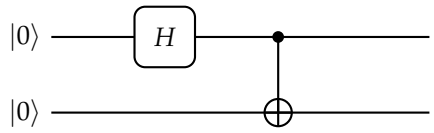
$$\mathrm{CNOT}_{1,2}\big(|b_1\rangle \otimes |b_2\rangle\big) = |b_1\rangle \otimes |b_1 \oplus b_2\rangle,$$

i.e. qubit 1 is the control and qubit 2 is the target. The circuit notation for the CNOT gate is shown below; a dot is placed on the control qubit, and $\oplus$ on the target qubit.



**Example: creating an EPR pair.** We will look at a circuit that creates entanglement starting from a product state. Typically, the initial state of each qubit is set to $|0\rangle$ (unless a qubit is an input to the circuit from an external source). We want to create an EPR pair, so we need two qubits. We assume that the two qubits are prepared independently in the state $|0\rangle$, yielding the product state $|00\rangle$.

Apply $H$ to qubit 1 and then $\text{CNOT}_{1,2}$, starting from $|00\rangle$.




*Step 1.*

$$(H \otimes I)|00\rangle = |+\rangle \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Note that $H$ acts locally on the first qubit; hence it acts as $H \otimes I$ on the composite system. Since this action of $H$ is local to a single qubit, it does not create entanglement; entanglement can be created only through a joint operation. The output of this step is still a product state.

*Step 2.*

$$\text{CNOT}_{1,2}\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left[\,|00\rangle + |11\rangle\,\right].$$

The CNOT gate is a genuine 2-qubit gate: a joint unitary operator acting on both qubits. The output state is the EPR pair, which is entangled.

# *Homework 5*

1. **Computing Schmidt decompositions.** For each state below, find a Schmidt decomposition, state the Schmidt rank $r$ and the Schmidt coefficients $\mu_k$, and say whether the state is entangled. You can use a computer program to find the SVD if you have to.

   (a) $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$

   (b) $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |21\rangle)$ on $\mathbb{C}^3 \otimes \mathbb{C}^2$

2. **Superposition versus Mixture.** We saw in Lecture 10 that unitary gates are reversible quantum operations. We do not expect a reversible operation to introduce randomness into a system, and similarly, if there is randomness pre-existing in a system we do not expect a reversible operation to eradicate this randomness. This is true in the quantum case as well: a unitary operator does not introduce new randomness or eradicate existing randomness in a system.

   (a) Consider the computational basis states $|0\rangle$ and $|1\rangle$ in $\mathbb{C}^2$. Would you consider these states as random or definite/non-random?

   (b) Consider the qubit state $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$. Is there a unitary operation that maps the state $|0\rangle$ to $|\psi\rangle$? Identify one such unitary operator. Is there a unitary that maps $|\psi\rangle$ to $|0\rangle$?

   (c) $|\psi\rangle$ and $|0\rangle$ can be transformed into each other through reversible operations. Would you consider $|\psi\rangle$ to be random or non-random?

   (d) Let $\rho$ be a qubit mixed state (not pure). What is the rank of this operator? Is there a unitary gate that transforms this state into a classical state (diagonal density operator) $\rho_{\text{classical}}$? Is $\rho_{\text{classical}}$ a constant state or a classical random variable? Since $\rho$ and $\rho_{\text{classical}}$ are related through a reversible operation, would you consider $\rho$ to be random or non-random?

3. **A secure communications scenario: classical versus quantum.** Alice would like to send Bob two classical bits of information. There is an eavesdropper (Eve) who can access one of the two systems Alice sends to Bob: if Alice sends Bob two classical bits, Eve can access one of these two bits; if Alice sends Bob two qubits, Eve can access one of the two qubits. We will look at a quantum encoding strategy in which no information leaks to Eve.

   *Quantum encoding by Alice.* Alice starts with two physical qubits $A$ and $B$ and prepares them in the EPR state $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. She has two classical bits of information $b_1, b_2$, which she encodes into the qubits as follows:

   $$|\psi\rangle_{AB} = (X^{b_1} \otimes I)(Z^{b_2} \otimes I)|\text{EPR}\rangle.$$

   That is, Alice applies $Z$ to qubit $A$ if $b_2 = 1$, and then applies $X$ to qubit $A$ if $b_1 = 1$. She then sends the registers $A$ and $B$ to Bob. Eve might get access to exactly one of these registers. We now analyze two things: decoding by Bob (assuming Eve does not tamper) and security against Eve (in case Eve tampers to extract information about $b_1, b_2$).

(a) What are the four possible values of the encoded state $|\psi\rangle_{AB}$ corresponding to the four possibilities for $(b_1, b_2)$?

(b) Verify that these four encoded states are orthonormal in $\mathbb{C}^2 \otimes \mathbb{C}^2$.

(c) Identify a unitary gate $U \in \mathbb{C}^{4\times 4}$ that maps these four states to the computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (in some order).

REMARK. Observe that, when Eve does not tamper with $A$ or $B$, Bob can retrieve the information $(b_1, b_2)$ from $|\psi\rangle_{AB}$ using $U$ and a classical measurement. Bob applies the gate $U$ to $|\psi\rangle_{AB}$; he then holds one of the four computational basis states, and a classical measurement tells him which one occurred.

Now let us consider the situation where Eve gets access to one of the two qubits $A$ or $B$.

(d) For each of the four possible values of the encoded state $|\psi\rangle_{AB}$ and each of the two possible interceptions (Eve accesses $A$, or Eve accesses $B$), find the state of the qubit that Eve intercepts (eight cases in all). Is there any variation in the state of the intercepted qubit across these eight cases?

(e) How can you argue that Eve can gather absolutely no information about $(b_1, b_2)$? Does *indistinguishability of preparations* help?

Now consider the classical case. Suppose Alice uses two classical bits, stored in registers $A$ and $B$ (the names $A, B$ are reused here for this separate classical scenario), to encode the information about $(b_1, b_2)$, and Eve can intercept one of the two classical bits $A$ or $B$. Assume Alice's classical encoding is a deterministic function $(b_1, b_2) \mapsto (A, B)$.

(f) For successful decoding by Bob (in case Eve does not tamper), show that the four possible values of $(A, B)$ must be distinct.

(g) Now argue that no matter which classical bit Eve intercepts, she can gather *some* information about $(b_1, b_2)$.

4. **Quantum circuits for entangled states.** You must design quantum circuits to prepare desired pure states (on a composite system of multiple qubits). In each case sketch the circuit and argue that the circuit functions as desired. The initial states of all the qubits must be $|0\rangle$. You are allowed to use only the following gates: Paulis, Hadamard, CNOT, Toffoli (see Question 3 of Homework 2).

(a) $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

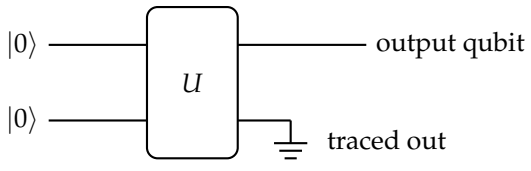
(b) $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$

(c) $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

(d) $\frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$

5. **Quantum preparation of classical randomness.** In this question, you must use pure states, unitary operations and tracing out to generate classical randomness. In each case you can use a composite system consisting of one or more qubits. All qubits must be initialized to $|0\rangle$.

In a quantum circuit, tracing out (discarding) a qubit is drawn as a wire that ends in the "ground" symbol shown below; the state of the remaining qubits is the partial trace of the circuit output over every wire that ends this way.



In each case, you must draw the quantum circuit for your preparation — using the trace-out notation above — and analytically show that the circuit output holds the desired classical state.

You are allowed to use only the following gates: Paulis, Hadamard, CNOT, Toffoli.

(a) A classical random variable that can take two possible values 0 and 1 with probabilities $1/4$ and $3/4$, respectively.

(b) Two classical bits $A$ and $B$ that are each uniformly random but always equal: the pair $(A, B)$ takes the value $(0, 0)$ with probability $1/2$ and the value $(1, 1)$ with probability $1/2$, and never takes the values $(0, 1)$ or $(1, 0)$.

6. Suppose the composite register $AB$ is in the entangled state $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$ where the state space of both $A$ and $B$ is $\mathbb{C}^d$. A unitary $U \in \mathbb{C}^{d \times d}$ is applied locally on register $A$, and let $|\phi\rangle$ denote the resulting state of $AB$.

   Show that there is a unitary $V \in \mathbb{C}^{d \times d}$ (of course, the choice of $V$ will depend on $U$) that when applied locally on $B$ transforms $|\psi\rangle$ to $|\phi\rangle$. That is, the application of $V$ on $B$ has the same effect on $|\psi\rangle$ as the application of $U$ on $A$.

7. Identify every pure state $|\psi\rangle$ on $AB$ that satisfies the property in the previous question, that is, the effect of any local unitary on register $A$ can be equivalently attained by applying a suitable local unitary on register $B$.

# *Lecture 11*

## §11.1. Projective measurements

The main references for this lecture are: Chapter 2 of Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (10th Anniversary Edition, Cambridge University Press, 2010); Chapter 3 of Phillip Kaye, Raymond Laflamme, and Michele Mosca, *An Introduction to Quantum Computing* (Oxford University Press, 2007).

Measurement is the only process through which information can be retrieved from a quantum system. Unlike the classical case, there is no way to 'read off' an arbitrary pure state $|\psi\rangle$ stored in a quantum register. That is, given a single qubit in a pure state $\alpha|0\rangle + \beta|1\rangle$, quantum mechanics does not provide us any tool to obtain the values of $\alpha$ and $\beta$ (however, if we are given *many* qubits, all of them prepared in the same state $|\psi\rangle$, then one can reliably estimate the values of $\alpha$ and $\beta$; this process is called quantum tomography). Quantum measurement has one input (a quantum state) and two outputs (a classical output that carries information about the state on which measurement was performed, and a post-measurement quantum state — this is the state of the system after the measurement). Measurements are quantized and random:

- the classical outcome can take one of only finitely many values, and
- these measurement outcomes are random, even if the input state itself is non-random (pure).

In general, the measurement process affects the state of the system in an irreversible way — this is called 'wavefunction collapse' or 'state collapse'. Unitary gates and measurements are the only physical processes through which the state of a quantum system can be altered.

Here we highlight some differences with classical measurement or classical states:

1. Classically, there is essentially only one way to measure: we read off the value stored in the classical register either partially or completely. Quantum mechanically, there are several inequivalent ways to measure the same system — there are several inequivalent aspects of a quantum system, and one can choose to measure any one of these aspects or properties.
2. Classically, the outcome of a measurement is random only when the underlying state itself is random (i.e., the register holds a genuine random variable). Quantum mechanically, the outcome can be random even when the state being measured is *pure* (i.e., not random at all, in the sense of Lecture 7).
3. Classically, measurement does not disturb the value stored in the register – reading it does not change it. Quantum mechanically, measurement can (and generally does) change/modify the state of the system. Hence, in general, if you 'read' a quantum register you risk modifying its state irreversibly.

**Measurement frameworks.** There are several mathematical descriptions or frameworks for quantum measurements:

1. General measurement.
2. POVM – positive-operator-valued measure.
3. Projective (or orthogonal) measurement.

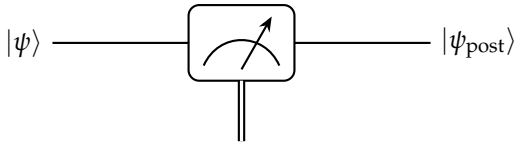
We will look at projective measurements in this course. General measurements and POVMs can be described through projective measurements. For example, any general measurement or POVM can be obtained by appending an ancillary register to a given system (so as to form a composite system), and performing a projective measurement on this composite system.

**The formal definition.** A *projective measurement* on a $d$-dimensional state space $\mathbb{C}^d$ is specified by

1. an integer $L \leq d$,
2. distinct real numbers $\lambda_1, \ldots, \lambda_L$, and
3. projections $P_1, \ldots, P_L \in \mathbb{C}^{d \times d}$ (i.e. $P_\ell^2 = P_\ell^\dagger = P_\ell$, $P_\ell \neq 0$) satisfying

$$\sum_{\ell=1}^{L} P_\ell = I \text{ (completeness)}, \qquad P_i P_j = 0 \text{ for } i \neq j \text{ (orthogonality)}.$$

Connecting a quantum register to this measurement device produces one of the $L$ possible *classical outcomes* $\lambda_1, \ldots, \lambda_L$, together with a (generally different) *post-measurement quantum state* on the quantum register:




REMARK. *This generalizes the classical measurement device of Lecture 6 (recalled in Homework 3): there, the device was specified by a partition $S_1, \ldots, S_L$ of the classical alphabet and distinct outcomes $\lambda_1, \ldots, \lambda_L$, which is exactly the special case where each $P_\ell$ is the* diagonal $0/1$ *matrix $P_\ell = \sum_{i \in S_\ell} |i\rangle\langle i|$. A general quantum projective measurement allows* any *$P_1, \ldots, P_L$ satisfying the conditions above, not just diagonal ones.*

**The geometric picture.** For $\ell = 1, \ldots, L$, let

$$S_\ell := \text{column space of } P_\ell = \text{the subspace onto which } P_\ell \text{ projects.}$$

Since $P_\ell$ is a projection operator, its eigenvalues are $0, 1$, and $S_\ell$ can be equivalently defined as the space of all $+1$-eigenvectors of $P_\ell$, that is,

$$S_\ell = \left\{ |\zeta\rangle \in \mathbb{C}^d : P_\ell |\zeta\rangle = |\zeta\rangle \right\}.$$

The subspaces $S_1, \ldots, S_L$ are pairwise orthogonal, and together they span all of $\mathbb{C}^d$.

**CLAIM.** *For $i \neq j$, every vector in $S_i$ is orthogonal to every vector in $S_j$.*

*Proof.* Let $|u\rangle \in S_i$ and $|v\rangle \in S_j$, so that $P_i|u\rangle = |u\rangle$ and $P_j|v\rangle = |v\rangle$. Then

$$\langle u \,|\, v \rangle = \langle u | P_i | v \rangle = \langle u | P_i P_j | v \rangle = 0,$$

using $|u\rangle = P_i|u\rangle$ together with $P_i^\dagger = P_i$ (first equality), then $|v\rangle = P_j|v\rangle$ (second equality), and finally $P_i P_j = 0$. ∎

**CLAIM.** *$S_1 + \cdots + S_L = \mathbb{C}^d$, i.e. the $S_\ell$ together span $\mathbb{C}^d$. What this means is that every vector in $\mathbb{C}^d$ can be written as a sum of $L$ vectors, one from each of $S_1, \ldots, S_L$. (In fact, this is a direct-sum decomposition, that is, this expansion as a sum is unique.)*

*Proof.* Let $|\phi\rangle \in \mathbb{C}^d$ be arbitrary. By completeness of the $P_\ell$,

$$|\phi\rangle = I|\phi\rangle = \Big(\sum_{\ell=1}^{L} P_\ell\Big)|\phi\rangle = P_1|\phi\rangle + \cdots + P_L|\phi\rangle.$$

Each term $P_\ell|\phi\rangle$ lies in $S_\ell$, since $P_\ell(P_\ell|\phi\rangle) = P_\ell^2|\phi\rangle = P_\ell|\phi\rangle$ shows it is a $+1$-eigenvector of $P_\ell$. Hence $|\phi\rangle \in S_1 + \cdots + S_L$; as $|\phi\rangle$ was arbitrary, $S_1 + \cdots + S_L = \mathbb{C}^d$. ∎

Together, the two claims say that $\mathbb{C}^d$ is the *orthogonal direct sum* of $S_1, \ldots, S_L$, so in particular the dimensions add up:

$$\sum_{\ell=1}^{L} \dim(S_\ell) = \dim(\mathbb{C}^d) = d.$$

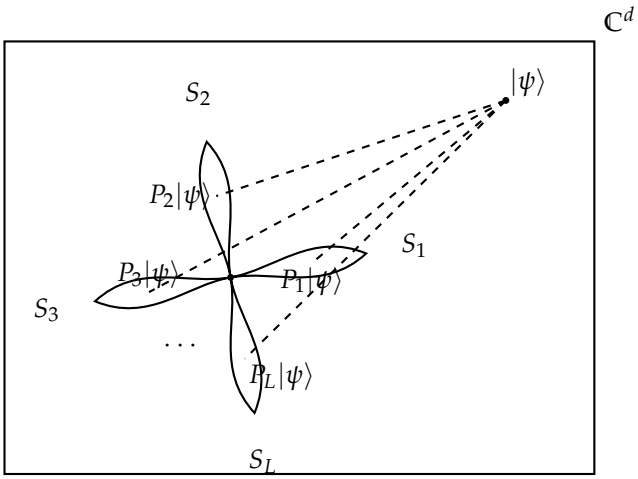
Consider a register holding a pure state $|\psi\rangle \in \mathbb{C}^d$, $\||\psi\rangle\|^2 = 1$. Using completeness of the $\{P_\ell\}$,

$$|\psi\rangle = I|\psi\rangle = \Big(\sum_{\ell=1}^{L} P_\ell\Big)|\psi\rangle = P_1|\psi\rangle + \cdots + P_L|\psi\rangle,$$

and since the $P_\ell|\psi\rangle$ lie in the pairwise-orthogonal subspaces $S_\ell$, Pythagoras' theorem gives

$$1 = \||\psi\rangle\|^2 = \|P_1|\psi\rangle\|^2 + \cdots + \|P_L|\psi\rangle\|^2.$$

The $L$ nonnegative numbers on the right, which sum to 1, will play the role of probabilities in a projective measurement, with $\|P_\ell|\psi\rangle\|^2$ being the probability of the $\ell^{\text{th}}$ classical outcome $\lambda_\ell$.




**Outcome probabilities and the post-measurement state.** We will now consider the measurement on a pure state $|\psi\rangle$. We will later generalize to mixed states. The outcome of the measurement is random. The probability of observing classical output $\lambda_\ell$ is

$$P[\lambda_\ell] = \|P_\ell|\psi\rangle\|^2 = \langle\psi|P_\ell^\dagger P_\ell|\psi\rangle = \mathrm{Tr}\big[P_\ell|\psi\rangle\langle\psi|P_\ell^\dagger\big].$$

Given that the classical output $\lambda_\ell$ is observed, the post-measurement quantum state $|\psi_{\text{post}}\rangle$ is the normalized version of $P_\ell|\psi\rangle$:

$$|\psi_{\text{post}}\rangle = \frac{P_\ell|\psi\rangle}{\|P_\ell|\psi\rangle\|} = \frac{P_\ell|\psi\rangle}{\sqrt{P[\lambda_\ell]}}.$$

This is wavefunction collapse: the state of the register is modified as part of measurement to a vector $|\psi_{\text{post}}\rangle$ lying in one of the subspaces $S_1, \ldots, S_L$ even if $|\psi\rangle$ itself does not belong to any of these $L$ subspaces.

*Description in terms of density operators.* Suppose the measurement acts on a pure state $\rho = |\psi\rangle\langle\psi|$. Then

$$P[\lambda_\ell] = \text{Tr}\big[P_\ell|\psi\rangle\langle\psi|P_\ell^\dagger\big] = \text{Tr}\big[P_\ell\rho P_\ell^\dagger\big],$$

and, if the classical outcome is $\lambda_\ell$,

$$\rho_{\text{post}} = \frac{P_\ell|\psi\rangle\langle\psi|P_\ell^\dagger}{P[\lambda_\ell]} = \frac{P_\ell\rho P_\ell^\dagger}{\text{Tr}[P_\ell\rho P_\ell^\dagger]}.$$

(This is easily checked to equal $|\psi_{\text{post}}\rangle\langle\psi_{\text{post}}|$.) Written this way, the formula makes sense for a mixed input state $\rho$ as well, and is in fact how a projective measurement acts on an arbitrary (not necessarily pure) state.

**Observables.** The data of a projective measurement device can be packaged succinctly into a single Hermitian operator, called an *observable*:

$$M := \sum_{\ell=1}^{L} \lambda_\ell P_\ell.$$

Note that $M^\dagger = M$. Conversely, $M$ determines $L$, the $\{\lambda_\ell\}$, and the $\{P_\ell\}$ (this is exactly the spectral decomposition of $M$):

1. $L$ is the number of distinct eigenvalues of $M$.
2. $\lambda_1, \ldots, \lambda_L$ are the $L$ distinct eigenvalues of $M$.
3. $S_\ell = \{|\varphi\rangle \in \mathbb{C}^d : M|\varphi\rangle = \lambda_\ell|\varphi\rangle\}$ is the eigenspace of $M$ corresponding to $\lambda_\ell$.
4. $P_\ell$ is the projection onto $S_\ell$.

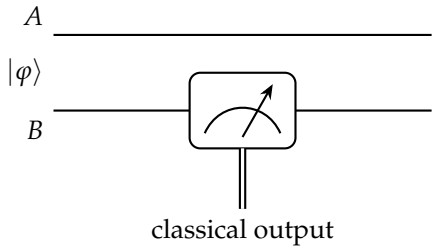
So specifying a projective measurement is the same thing as specifying an observable $M$.

**What if you don't witness the measurement outcome.** If the experimenter does not observe the classical outcome of the measurement, then the post-measurement state must *be averaged over* the statistics of the measurement outcome to reflect the knowledge of the experimenter. This is simply done using the law of total probability. Suppose $\sigma$ is the final state after measurement. Then

$$\begin{aligned}\sigma &= \sum_{\ell=1}^{L} P[\lambda_\ell]\,\rho_{\text{post}|\lambda_\ell} \\ &= \sum_{\ell=1}^{L} P[\lambda_\ell]\,\frac{P_\ell|\psi\rangle\langle\psi|P_\ell^\dagger}{P[\lambda_\ell]} \\ &= \sum_{\ell=1}^{L} P_\ell|\psi\rangle\langle\psi|P_\ell^\dagger\end{aligned}$$

**Choice of measurement.** We have the freedom to use $L$, real and distinct $\lambda_1, \ldots, \lambda_L$ and projections $P_1, \ldots, P_L$ for a projective measurement as long as they satisfy completeness and orthogonality. In the language of using observables to describe a projective measurement, quantum theory allows us to use any Hermitian operator $M$ as an observable. This is a far richer class of measurements than can be performed classically.

**Local measurement on a composite system.** Suppose a bipartite pure state $|\varphi\rangle$ (whether entangled or not) lives on registers $A$ (dimension $d_1$) and $B$ (dimension $d_2$), and we measure only register $B$, using an observable $M \in \mathbb{C}^{d_2 \times d_2}$, leaving $A$ untouched:




This *local measurement on $B$* is equivalent to a *global measurement on $AB$* using the observable $I_{d_1} \otimes M \in \mathbb{C}^{d_1 d_2 \times d_1 d_2}$: if $M = \sum_\ell \lambda_\ell P_\ell$, then

$$I \otimes M = \sum_\ell \lambda_\ell \, (I \otimes P_\ell).$$

**CLAIM.** *$\lambda_1, \ldots, \lambda_L$ together with $I \otimes P_1, \ldots, I \otimes P_L$ specify a valid projective measurement on $\mathbb{C}^{d_1 d_2}$.*

*Proof.* We check the three defining conditions, using the mixed-product property $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ and $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

*Each $I \otimes P_\ell$ is a projection.* We have

$$(I \otimes P_\ell)^2 = (I \cdot I) \otimes (P_\ell P_\ell) = I \otimes P_\ell, \qquad (I \otimes P_\ell)^\dagger = I^\dagger \otimes P_\ell^\dagger = I \otimes P_\ell,$$

using $I^2 = I$, $P_\ell^2 = P_\ell$, and $I^\dagger = I$, $P_\ell^\dagger = P_\ell$. Also $I \otimes P_\ell \neq 0$, since $P_\ell \neq 0$.

*Completeness.* By linearity of the Kronecker product in its second argument,

$$\sum_{\ell=1}^{L} (I \otimes P_\ell) = I \otimes \Big( \sum_{\ell=1}^{L} P_\ell \Big) = I \otimes I_{d_2} = I_{d_1 d_2}.$$

*Orthogonality.* For $i \neq j$,

$$(I \otimes P_i)(I \otimes P_j) = (I \cdot I) \otimes (P_i P_j) = I \otimes 0 = 0.$$

Finally, $\lambda_1, \ldots, \lambda_L$ are still distinct real numbers, and $L \leq d_2 \leq d_1 d_2$. So all the conditions in the definition of a projective measurement are satisfied. ∎

REMARK. *This is a note on terminology.* ***I did not mention this during the lecture.*** *In the state space $\mathbb{C}^d$, suppose $|\phi_1\rangle, \ldots, |\phi_d\rangle$ are an orthonormal basis. A* measurement in the basis $|\phi_1\rangle, \ldots, |\phi_d\rangle$ *is any projective measurement (with $L = d$) that uses the one-dimensional projections along these basis vectors, i.e.,*

$$P_1 = |\phi_1\rangle\langle\phi_1|, \ldots, P_d = |\phi_d\rangle\langle\phi_d|.$$

*Also, measuring in the basis $|0\rangle, \ldots, |d-1\rangle$ is called* measurement in the computational basis*, i.e., $L = d$ and*

$$P_1 = |0\rangle\langle 0|, \ldots, P_d = |d-1\rangle\langle d-1|.$$

## §11.2. Examples

**Measuring a qubit in the $\{|+\rangle, |-\rangle\}$ basis.** Take $d = 2$. The only nontrivial choice of subspaces here has $L = 2$ with $\dim(S_1) = \dim(S_2) = 1$. Let $S_1$ be spanned by $|+\rangle$ and $S_2$ by $|-\rangle$, so that

$$P_1 = |+\rangle\langle +|, \quad \lambda_1 = +1, \qquad P_2 = |-\rangle\langle -|, \quad \lambda_2 = -1;$$

the corresponding observable is $M = P_1 - P_2 = |+\rangle\langle+| - |-\rangle\langle-| = X$, the Pauli $X$ operator.

Suppose the input state is $|\psi\rangle = |0\rangle$. Since $\langle+|0\rangle = \langle-|0\rangle = \frac{1}{\sqrt{2}}$,

$$P_1|\psi\rangle = |+\rangle\langle+|0\rangle = \tfrac{1}{\sqrt{2}}|+\rangle, \qquad P_2|\psi\rangle = |-\rangle\langle-|0\rangle = \tfrac{1}{\sqrt{2}}|-\rangle,$$

so $P[\lambda_1] = \|\frac{1}{\sqrt{2}}|+\rangle\|^2 = \frac{1}{2}$ and, by symmetry, $P[\lambda_2] = \frac{1}{2}$:

| classical output | $P[\lambda_\ell]$ | $\lvert\psi_{\text{post}}\rangle$ |
|---|---|---|
| $+1$ | $1/2$ | $\lvert+\rangle$ |
| $-1$ | $1/2$ | $\lvert-\rangle$ |

So even though the input $|0\rangle$ is a pure state, measuring it in the $\{|+\rangle, |-\rangle\}$ basis produces a uniformly random classical outcome.

**Polarization glasses.** A *polarizer* is a physical realization of a projective measurement, taking a single photon as input.[1] We consider the polarization state of a photon as a realization of a qubit. This is a two-level system with classical states $|0\rangle$ and $|1\rangle$ corresponding to vertical and horizontal polarizations, respectively. In general, a photon can be in a superposition of these two states: $\alpha|0\rangle + \beta|1\rangle$.

A polarizer performs a measurement in an orthonormal basis $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^2$. That is, it uses

$$P_1 = |\phi_1\rangle\langle\phi_1| \text{ and } P_2 = |\phi_2\rangle\langle\phi_2|.$$

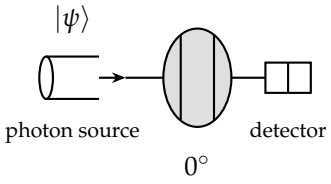
We will assume that $\lambda_1 = +1$ and $\lambda_2 = -1$. The physical action of a polarizer on a photon is a little different from the measurement process described earlier. In a polarizer, if the classical outcome of the measurement is $+1$, the photon (in its post-measurement state) appears on the other side of the polarizer. If the classical outcome is $-1$, the photon gets absorbed by the polarizer and is lost as energy or heat. The projective measurement formalism is an idealization of the action of the polarizer.

Say a photon polarized $|0\rangle$ is *vertically* polarized, and $|1\rangle$ is *horizontally* polarized, so a general polarization state is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

We now work out three scenarios, with one, two, and three polarizers in sequence.

**Scenario 1: a single vertical polarizer.** A polarizer held in the *vertical* orientation implements the measurement in the basis $|\phi_1\rangle = |0\rangle$ (pass axis), $|\phi_2\rangle = |1\rangle$ (absorb axis):



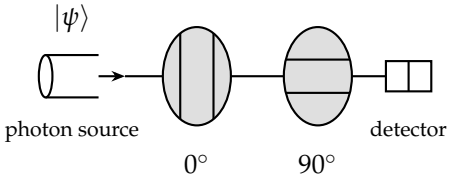

Feeding in $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$: the photon emerges on the other side (post-measurement state $|\psi_{\text{post}}\rangle = |\phi_1\rangle = |0\rangle$) only if the classical outcome is $+1$.

| classical outcome | probability | $\lvert\psi_{\text{post}}\rangle$ |
|---|---|---|
| $+1$ (pass) | $\lvert\alpha\rvert^2$ | $\lvert0\rangle$ |
| $-1$ (absorbed) | $\lvert\beta\rvert^2$ | – |

(A photon that is not seen at all, i.e. absorbed by the polarizer, corresponds to outcome $-1$; as discussed above, there is no meaningful surviving post-measurement *photon* in this branch.)

[1] You can watch the experiment on **YouTube**.

**Scenario 2: vertical followed by horizontal.** Send the photon through *two* polarizers in a row: the first held vertically (pass axis $|\phi_1\rangle = |0\rangle$), the second held *horizontally*, i.e. its pass axis is $|\phi_1'\rangle = |1\rangle$ and its absorb axis is $|\phi_2'\rangle = |0\rangle$:

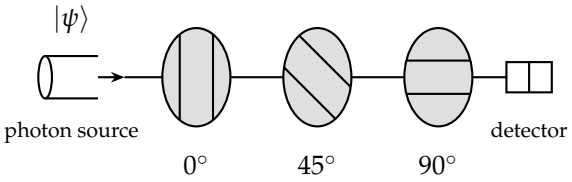



For the photon to emerge from both, it must first pass the vertical polarizer (probability $|\alpha|^2$, leaving it in the state $|0\rangle$), and then pass the horizontal polarizer starting from $|0\rangle$: this happens with probability $|\langle\phi_1'|0\rangle|^2 = |\langle 1\,|\,0\rangle|^2 = 0$. So the overall probability of the photon surviving both polarizers is

$$|\alpha|^2 \cdot 0 = 0, \qquad \textit{regardless} \text{ of } \alpha, \beta\text{:}$$

two crossed (perpendicular) polarizers block all the light.

**Scenario 3: three polarizers, 45° apart.** Now insert a *third* polarizer, held diagonally at 45°, *between* the vertical and horizontal ones of Scenario 2: its pass axis is $|\phi_1''\rangle = |+\rangle$ and its absorb axis is $|\phi_2''\rangle = |-\rangle$.




Tracking the photon step by step:

- It passes the first (0°) polarizer with probability $|\alpha|^2$, leaving it in the state $|0\rangle$.
- Starting from $|0\rangle$, it passes the second (45°) polarizer with probability $|\langle +\,|\,0\rangle|^2 = \frac{1}{2}$, leaving it in the state $|+\rangle$.
- Starting from $|+\rangle$, it passes the third (90°) polarizer with probability $|\langle 1\,|\,+\rangle|^2 = \frac{1}{2}$, leaving it in the state $|1\rangle$.

The overall probability of the photon surviving all three polarizers is

$$|\alpha|^2 \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} = \frac{|\alpha|^2}{4} > 0 \qquad (\text{whenever } \alpha \neq 0).$$

We have just witnessed a counter-intuitive fact: with two polarizers (as in Scenario 2) no photon passes through, but introducing a third polarizer in between them allows photons to pass through with non-zero probability (if $\alpha \neq 0$). The main reason is that the in-between polarizer collapses the photon's state to $|+\rangle$, which is an equal superposition of $|0\rangle$ and $|1\rangle$.

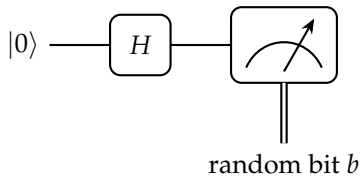
## §11.3. Additional material not covered during lecture

**Quantum random number generation.** Quantum measurements can be used as true random number generators. Classical random-number generators (RNGs), as implemented in software, are in fact *pseudorandom*: they are deterministic algorithms (typically seeded by, e.g., the system clock) that produce a sequence of numbers which merely *look* statistically random. Given the seed and the algorithm, the entire sequence is, in principle, completely predictable — classical "randomness" generated this way is not truly random.

This is fundamentally different from quantum measurement, where (recall point 2 of §11.1) the outcome of a measurement can be random even when the state being measured is pure, i.e., not random at all. This randomness is not a stand-in for some hidden or missing information about the state; it is intrinsic to nature. *Quantum random number generators* (QRNGs) exploit exactly this fact, and are used in practice (e.g. for cryptographic key generation) wherever genuine, non-deterministic randomness is required.

The simplest QRNG protocol uses a single qubit:

1. Prepare the qubit in the state $|0\rangle$.
2. Apply a Hadamard gate: $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$.
3. Measure the qubit in the computational basis, i.e., using the observable $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.




The classical outcome is 0 or 1 with probabilities

$$P[0] = |\langle 0\,|\,+\rangle|^2 = \tfrac{1}{2}, \qquad P[1] = |\langle 1\,|\,+\rangle|^2 = \tfrac{1}{2},$$

so the output bit $b$ is uniformly distributed. Crucially, the state $|+\rangle$ fed into the measurement is itself a definite, non-random pure state (prepared deterministically from $|0\rangle$ by the Hadamard gate); the randomness of $b$ comes entirely from the measurement.

# *Lecture 12*

## §12.1. Measurement

**A note on language.** We say that *"we measure an observable"*, or *"we perform a measurement on a register"* — we do *not* say "we measure a register." The reason is that a quantum system has several distinct physical aspects (e.g. position, momentum, polarization), each characterized by its own observable; measuring *an observable* of a quantum system is the same thing as measuring this or that physical property of the system. A register by itself does not pick out any one of these aspects, so "measuring a register" is not a complete description of what we want to measure — one must say *which observable* of *which register* is being measured.

REMARK. *Nevertheless, it is common to use the phrase "measure the register" (without any reference to the observable) to mean that the register is being measured in the computational basis, i.e., using the projection operators* $|0\rangle\langle 0|, |1\rangle\langle 1|, \ldots$. *Thus, if no observable is mentioned, measurement implies measurement in the computational basis.*

**Recap: projective measurements.** Recall from Lecture 11 that a projective measurement on $\mathbb{C}^d$ is succinctly described by an observable (a Hermitian operator)

$$M = \sum_{\ell=1}^{L} \lambda_\ell P_\ell,$$

with distinct eigenvalues $\lambda_1, \ldots, \lambda_L$ and $P_\ell$ the projection onto the eigenspace

$$S_\ell = \{|\varphi\rangle \in \mathbb{C}^d : M|\varphi\rangle = \lambda_\ell|\varphi\rangle\} = \{|\varphi\rangle \in \mathbb{C}^d : P_\ell|\varphi\rangle = |\varphi\rangle\}.$$

Recall the information-theoretic view that measurement is inherently random and produces one of the $L$ possible outcomes (a pair of classical output and post-measurement state) at random. The probabilities of these outcomes are dictated by both the input state $|\psi\rangle$ and the measurement observable $M$:

$$|\psi\rangle \longmapsto \left(\lambda_\ell, \frac{P_\ell|\psi\rangle}{\|P_\ell|\psi\rangle\|}\right) \quad \text{with probability } \|P_\ell|\psi\rangle\|^2, \qquad \ell = 1, \ldots, L.$$

More generally, on an arbitrary (possibly mixed) input state $\rho$,

$$\rho \longmapsto \left(\lambda_\ell, \frac{P_\ell \rho P_\ell^\dagger}{\mathrm{Tr}[P_\ell \rho P_\ell^\dagger]}\right) \quad \text{with probability } P[\lambda_\ell] := \mathrm{Tr}[P_\ell \rho P_\ell^\dagger], \qquad \ell = 1, \ldots, L.$$

**Special case: measurement on eigenvectors.** Measurement is, in general, destructive and irreversible, that is, it changes the state $|\psi\rangle$ of the system irreversibly to one of the $L$ states $\frac{P_\ell|\psi\rangle}{\|P_\ell|\psi\rangle\|}$, $\ell = 1, \ldots, L$. Thus, the task of retrieving information from a register modifies the state itself. However, in a special situation information can be retrieved without changing the state, that is, the post- and pre-measurement states are identical. This is a simple yet important observation relevant to quantum error correction (and also to several quantum computing algorithms, like Deutsch's algorithm; see Section 1.4.3 of Nielsen and Chuang).

This special case is that the state fed into the measurement device already lies in one of the eigenspaces of $M$, i.e., $|\psi\rangle$ is an eigenvector of $M$.

**CLAIM.** *Suppose the state of the register is $|\varphi\rangle \in S_i$ for some $i$, i.e. $|\varphi\rangle$ is a (unit) eigenvector of $M$ with eigenvalue $\lambda_i$. Then measuring $M$ yields the outcome $\lambda_i$ with probability 1, and the post-measurement state is $|\varphi\rangle$ itself, which is unchanged.*

*Proof.* Since $|\varphi\rangle \in S_i$, $P_i|\varphi\rangle = |\varphi\rangle$. For any $\ell \neq i$, orthogonality $P_\ell P_i = 0$ gives

$$P_\ell|\varphi\rangle = P_\ell\big(P_i|\varphi\rangle\big) = (P_\ell P_i)|\varphi\rangle = 0.$$

Hence $\|P_\ell|\varphi\rangle\|^2 = 0$ for every $\ell \neq i$; since the probabilities $\|P_\ell|\varphi\rangle\|^2$ sum to $\|\varphi\|^2 = 1$ (completeness, as in the recap above), the remaining probability $\|P_i|\varphi\rangle\|^2$ must equal 1. So the outcome is $\lambda_i$ with probability 1, and the post-measurement state is $P_i|\varphi\rangle / \|P_i|\varphi\rangle\| = |\varphi\rangle/1 = |\varphi\rangle$. ■

**Distinguishing orthogonal states.** Suppose a register is guaranteed to hold one of $N$ known, mutually orthonormal states $|\varphi_1\rangle, \ldots, |\varphi_N\rangle \in \mathbb{C}^d$ ($N \leq d$), and we want to determine, by measurement, which one it is. Use the projective measurement with

$$P_1 = |\varphi_1\rangle\langle\varphi_1|, \ \ldots, \ P_N = |\varphi_N\rangle\langle\varphi_N|,$$

together with any further projections $P_{N+1}, \ldots, P_L$ chosen freely so that completeness and orthogonality hold (e.g. any orthogonal decomposition of the subspace orthogonal to all the $|\varphi_i\rangle$). In particular, if $N = d$ then $P_1, \ldots, P_N$ already satisfy completeness and there is nothing to do; else, we can choose $N + 1$ projections with $P_{N+1} := I - P_1 - \cdots - P_N$.

**CLAIM.** *$P_1, \ldots, P_{N+1}$ are mutually orthogonal projections satisfying completeness: $P_\ell^2 = P_\ell^\dagger = P_\ell$ for each $\ell$, $P_k P_\ell = 0$ for $k \neq \ell$, and $P_1 + \cdots + P_{N+1} = I$.*

*Proof.* Write $Q := P_1 + \cdots + P_N$. Each $P_i$ ($i \leq N$) is a projection: $P_i^\dagger = P_i$ trivially, and $P_i^2 = |\varphi_i\rangle\langle\varphi_i\,|\,\varphi_i\rangle\langle\varphi_i| = P_i$, using $\langle\varphi_i\,|\,\varphi_i\rangle = 1$. For $i \neq j$ ($i, j \leq N$), orthonormality of the $|\varphi_i\rangle$ gives $P_i P_j = |\varphi_i\rangle\langle\varphi_i\,|\,\varphi_j\rangle\langle\varphi_j| = 0$; hence

$$Q^2 = \sum_{i=1}^{N}\sum_{j=1}^{N} P_i P_j = \sum_{i=1}^{N} P_i^2 = \sum_{i=1}^{N} P_i = Q, \qquad Q^\dagger = \sum_{i=1}^{N} P_i^\dagger = Q.$$

Now $P_{N+1} = I - Q$ is Hermitian ($P_{N+1}^\dagger = I - Q^\dagger = I - Q = P_{N+1}$) and idempotent ($P_{N+1}^2 = (I-Q)^2 = I - 2Q + Q^2 = I - 2Q + Q = I - Q = P_{N+1}$), so it is itself a projection. For each $i \leq N$,

$$P_{N+1}P_i = (I - Q)P_i = P_i - QP_i = P_i - \sum_{k=1}^{N} P_k P_i = P_i - P_i = 0,$$

using $P_k P_i = 0$ for $k \neq i$ and $P_i P_i = P_i$; likewise $P_i P_{N+1} = P_i - P_i Q = P_i - \sum_{k=1}^{N} P_i P_k = P_i - P_i = 0$. So $P_{N+1}$ is orthogonal to every $P_i$, $i \leq N$, and together with the pairwise orthogonality of $P_1, \ldots, P_N$ already shown, $P_1, \ldots, P_{N+1}$ are mutually orthogonal. Finally, completeness holds by construction: $P_1 + \cdots + P_N + P_{N+1} = Q + (I - Q) = I$. ■

Pick any distinct $\lambda_1, \ldots, \lambda_L \in \mathbb{R}$ and choose the observable $M = \sum_\ell \lambda_\ell P_\ell$. By construction each candidate state $|\varphi_i\rangle$ lies in the eigenspace $S_i$, so the previous Claim can be applied here: measuring $M$ on the state $|\varphi_i\rangle$ returns the outcome $\lambda_i$ with probability 1, correctly revealing which of the $N$ states was present in the register.

REMARK. *In the simplest case $N = 2$ we can simply choose $P_1 = |\varphi_1\rangle\langle\varphi_1|$ and $P_2 = I - P_1$. This satisfies completeness ($P_1 + P_2 = I$, by construction) and orthogonality ($P_1 P_2 = P_1(I - P_1) = P_1 - P_1^2 = 0$, using $P_1^2 = P_1$). Since $|\varphi_2\rangle$ is orthogonal to $|\varphi_1\rangle$ it must necessarily lie in the subspace that $I - P_1$ projects to.*

In general, it is not possible to reliably distinguish non-orthogonal states. Let's see an example.

**Example (non-orthogonal states).** Take $d = 2$ and two *non-orthogonal* candidate states $|\varphi_1\rangle = |0\rangle$, $|\varphi_2\rangle = |+\rangle$ (indeed $\langle 0|+\rangle = 1/\sqrt{2} \neq 0$, so they are not orthogonal). We are promised that a register $A$ (a qubit) is given to us that is either in state $|0\rangle$ or in state $|+\rangle$. We are tasked with finding an observable, on measuring which, we can distinguish between these two possibilities.

Reliable operation requires that observing $\lambda_1$ tells us with certainty that the register held $|0\rangle$, i.e. $P[\lambda_1] = \||P_1|0\rangle\|^2$ must equal 1 when the input state actually is $|0\rangle$:

$$\||P_1|0\rangle\|^2 = 1 \implies |0\rangle \in S_1 \implies S_1 = \text{span}\{|0\rangle\},$$

that is, $P_1 = |0\rangle\langle 0|$. By the Remark above (the case $N = 2$), this choice already fixes $P_2$: $P_2 = I - P_1 = |1\rangle\langle 1|$.

By construction, this measurement correctly identifies $|0\rangle$: feeding in $|0\rangle$ always gives outcome $\lambda_1$,

$$|0\rangle \longmapsto (\lambda_1, |0\rangle) \text{ w.p. } 1, \qquad (\lambda_2, |1\rangle) \text{ w.p. } 0.$$

But feeding in the *other* candidate state, $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, gives

$$|+\rangle \longmapsto (\lambda_1, |0\rangle) \text{ w.p. } \||P_1|+\rangle\|^2 = \tfrac{1}{2}, \qquad (\lambda_2, |1\rangle) \text{ w.p. } \||P_2|+\rangle\|^2 = \tfrac{1}{2}.$$

So the very measurement built to certify $|0\rangle$ still outputs $\lambda_1$ half the time when the true state is actually $|+\rangle$: on this outcome we cannot tell whether the register held $|0\rangle$ or $|+\rangle$, so the scheme fails to reliably distinguish the two states. This is consistent with a general fact (not proved here): no measurement can perfectly distinguish two non-orthogonal states. However, note that if the measurement outcome is $\lambda_2$, we are certain that the state is $|+\rangle$.

**Example: distinguishing using multiple preparations.** The example above asked us to distinguish between two non-orthogonal states given exactly one qubit $A$. We saw that this can not be done reliably. However, if we are given access to a large number $n$ of qubits $A_1, \ldots, A_n$ (either all in state $|0\rangle$ or all in $|+\rangle$), then we can distinguish between the states with high (still not 100 per cent) reliability. The overall state is thus,

$$|0\rangle \otimes \cdots \otimes |0\rangle \text{ or } |+\rangle \otimes \cdots \otimes |+\rangle.$$

Note that, in either case, the state is a product state (not entangled). Suppose we measure the observable $\lambda_1|0\rangle\langle 0| + \lambda_2|1\rangle\langle 1|$ on each of these $n$ qubits.

Using the measurement statistics we derived above, we deduce the following:

$$\begin{aligned}\text{State is } |0\rangle &\Rightarrow \text{ all the measurement outcomes will be } \lambda_1\\ \text{State is } |+\rangle &\Rightarrow \text{ on the average, only half the outcomes are } \lambda_1\end{aligned}$$

We can resort to the following statistical test: if all $n$ outcomes are $\lambda_1$ then decide in favor of $|0\rangle$, else declare in favor of $|+\rangle$. This test makes no error when the actual state is $|0\rangle$. However, the test makes an error when the state is $|+\rangle$ and all the measurement outcomes are $\lambda_1$. The probability of this error is

$$P[\text{error} \mid \text{state is } |+\rangle] = P[(\lambda_1, \ldots, \lambda_1) | \text{ state is } |+\rangle] = \frac{1}{2^n}.$$

This probability of error decays quickly to 0 as $n$ increases. Thus, we can distinguish with high reliability if multiple copies of the state are provided.

Note that the states $|0\rangle \otimes \cdots \otimes |0\rangle$ and $|+\rangle \otimes \cdots \otimes |+\rangle$ are almost orthogonal when $n$ is large:

$$(\langle 0| \otimes \cdots \otimes \langle 0|)\,(|+\rangle \otimes \cdots \otimes |+\rangle) = (\langle 0|+\rangle)^n = \frac{1}{2^{n/2}}.$$

Hence, it is possible to distinguish them with higher reliability.

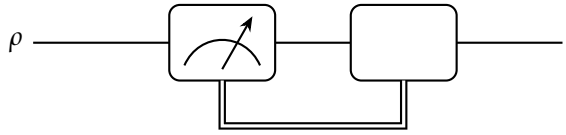
**Can't we make mulitple copies of a state ourselves?** Given a single copy of an unknown pure state $|\psi\rangle \in \mathbb{C}^d$, can we manufacture additional copies ourselves — using some fixed physical device, not depending on $|\psi\rangle$ — and then run the multiple-preparation test above? This would let us dispense with the requirement that the $n$ copies be handed to us from outside. Call such a device a *cloning machine*: a fixed quantum circuit that, given an unknown input state $|\chi\rangle \in \mathbb{C}^d$, outputs $|\chi\rangle \otimes |\chi\rangle$.

**CLAIM** (No-cloning theorem)**.** *Let $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^d$ be non-orthogonal states with $|\psi\rangle \neq |\varphi\rangle$ (up to global phase). If a quantum circuit outputs $|\psi\rangle \otimes |\psi\rangle$ on input $|\psi\rangle$, that same circuit cannot also output $|\varphi\rangle \otimes |\varphi\rangle$ on input $|\varphi\rangle$: no single, fixed cloning machine works for both states.*

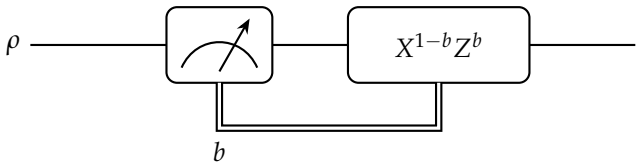
A complete proof is given in the Appendix (§12.3). This proof was not discussed during the lecture.

So a single, fixed cloning device can only ever clone one state (together with everything orthogonal to it) — never two distinct *non-orthogonal* states. In particular, our two candidate states $|0\rangle, |+\rangle$ from the example above cannot both be cloned by the same machine, since they are non-orthogonal ($\langle 0 | + \rangle = 1/\sqrt{2} \neq 0$). This answers the question posed by this subsection's title: no, we cannot manufacture our own extra copies of an unknown state and fall back on the multiple-preparation test — the $n$ copies must genuinely be supplied to us from outside, already prepared. The no-cloning theorem is one of the most consequential facts in quantum information: it underlies quantum key distribution (an eavesdropper cannot covertly copy quantum-encoded key bits), and it is also why quantum error correction cannot simply copy the state being protected, unlike its classical counterpart, and must instead work with encoded redundancy across entangled qubits.

**Classical control.** We are free to use classical logic or hardware to control a quantum circuit: the classical output of a measurement can determine which quantum gate is applied next.




For instance, if the measurement outcome is a single classical bit $b \in \{0, 1\}$, we might apply the gate $X$ if $b = 0$ or $Z$ if $b = 1$, i.e., apply the gate $X^{1-b}Z^b$:




In general, suppose we measure the observable $M = \sum_{\ell=1}^{L} \lambda_\ell P_\ell$, and apply a unitary gate $U_\ell$ whenever the classical outcome is $\lambda_\ell$. Tracking a single branch of the measurement,

$$\rho \xrightarrow{\text{measure}} \left(\lambda_\ell,\ \frac{P_\ell \rho P_\ell^\dagger}{P[\lambda_\ell]}\right) \xrightarrow{U_\ell} \frac{U_\ell P_\ell \rho P_\ell^\dagger U_\ell^\dagger}{P[\lambda_\ell]} \text{ w.p. } P[\lambda_\ell].$$

If the classical outcome is not observed, the final state is the average over branches (as in the corresponding computation of Lecture 11, now with the extra unitary gate applied in each branch):

$$\sum_{\ell=1}^{L} P[\lambda_\ell] \cdot \frac{U_\ell P_\ell \rho P_\ell^\dagger U_\ell^\dagger}{P[\lambda_\ell]} = \sum_{\ell=1}^{L} U_\ell P_\ell \rho P_\ell^\dagger U_\ell^\dagger.$$

**Example ($X^{1-b}Z^b$, continued).** Take $L = 2$ with outcomes $\lambda_1 \leftrightarrow b = 0$, $\lambda_2 \leftrightarrow b = 1$, and apply $U_1 = X$ when $b = 0$, $U_2 = Z$ when $b = 1$:

$$b = 0: \quad \frac{P_1 \rho P_1^\dagger}{P[\lambda_1]} \xrightarrow{X} \frac{X P_1 \rho P_1^\dagger X^\dagger}{P[\lambda_1]}, \qquad b = 1: \quad \frac{P_2 \rho P_2^\dagger}{P[\lambda_2]} \xrightarrow{Z} \frac{Z P_2 \rho P_2^\dagger Z^\dagger}{P[\lambda_2]}.$$

If the measurement outcome is known, say $\lambda_1$, the final state is $X P_1 \rho P_1^\dagger X^\dagger / P[\lambda_1]$ (and similarly for $\lambda_2$). If the measurement outcome is *not* known to the experimenter (such as when the entire circuit is residing within a quantum computer and you do not bother to see what is happening inside the computer), the final state is the average

$$X P_1 \rho P_1^\dagger X^\dagger + Z P_2 \rho P_2^\dagger Z^\dagger.$$

Note that $X^\dagger = X$ and $Z^\dagger = Z$ (the Pauli matrices are Hermitian — Lecture 10).

REMARK. *This pattern — measure, then apply a unitary conditioned on the classical outcome — is the way in which quantum errors are reversed/undone in the setup of quantum error correction.*

## §12.2. Kraus form of operations on a quantum register

There are essentially four kinds of operations one can perform on a quantum register: *appending* another, independently prepared register; *tracing out* (discarding) a subsystem of a composite register; applying a *unitary gate*; and *measurement*, with or without a classical-control operation as in §12.1. We will see, one at a time, that each of these has a Kraus form $\rho \mapsto \sum_k M_k \rho M_k^\dagger$, where $\sum_k M_k^\dagger M_k = I$.

**CLAIM.** *The composition of two maps in Kraus form is again in Kraus form. Precisely, if $\mathcal{E}_1(\rho) = \sum_i K_i \rho K_i^\dagger$ and $\mathcal{E}_2(\rho) = \sum_j L_j \rho L_j^\dagger$ are Kraus forms (i.e. $\sum_i K_i^\dagger K_i = I$ and $\sum_j L_j^\dagger L_j = I$), then so is $\mathcal{E}_2 \circ \mathcal{E}_1$, with Kraus operators $\{L_j K_i\}_{i,j}$.*

*Proof.* Since $\mathcal{E}_2$ is linear in its argument,

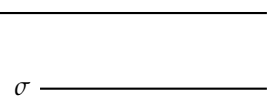
$$(\mathcal{E}_2 \circ \mathcal{E}_1)(\rho) = \mathcal{E}_2\Big(\sum_i K_i \rho K_i^\dagger\Big) = \sum_i \mathcal{E}_2\big(K_i \rho K_i^\dagger\big) = \sum_i \sum_j L_j \big(K_i \rho K_i^\dagger\big) L_j^\dagger = \sum_{i,j} (L_j K_i)\, \rho\, (L_j K_i)^\dagger.$$

Completeness of $\{L_j K_i\}_{i,j}$ follows from completeness of each Kraus form:

$$\sum_{i,j} (L_j K_i)^\dagger (L_j K_i) = \sum_i K_i^\dagger \Big(\sum_j L_j^\dagger L_j\Big) K_i = \sum_i K_i^\dagger\, I\, K_i = \sum_i K_i^\dagger K_i = I. \qquad \blacksquare$$

Consequently, since every quantum algorithm or circuit is built from a finite sequence of these four kinds of operations, and Kraus forms satisfy the above composition property, the overall input–output relationship of *any* quantum algorithm — however many gates, ancillas, and measurements it uses — can itself be written as a single Kraus form.

**Appending an independently prepared register.** Suppose a register holding state $\rho \in \mathbb{C}^{d_1 \times d_1}$ is joined by a second, independently prepared register holding a fixed state $\sigma \in \mathbb{C}^{d_2 \times d_2}$:




so that the joint state of the two (independent) registers is $\rho \otimes \sigma$, i.e. this is the map $\rho \mapsto \rho \otimes \sigma$. Can this map be written in Kraus form?

**CLAIM.** *The map $\rho \mapsto \rho \otimes \sigma$ has a Kraus form: there exist operators $K_1, \dots, K_r$ (each mapping $\mathbb{C}^{d_1} \to \mathbb{C}^{d_1 d_2}$) such that*

$$\rho \otimes \sigma = \sum_{j=1}^{r} K_j \rho K_j^\dagger \qquad \text{for every } \rho \in \mathbb{C}^{d_1 \times d_1}, \qquad \text{and} \qquad \sum_{j=1}^{r} K_j^\dagger K_j = I_{d_1}.$$

*Proof.* Since $\sigma$ is a density operator, it has a spectral decomposition

$$\sigma = \sum_{j=1}^{r} \lambda_j |\phi_j\rangle\langle\phi_j|, \qquad \lambda_1, \dots, \lambda_r > 0, \quad r = \operatorname{rank}(\sigma),$$

with $|\phi_1\rangle, \dots, |\phi_r\rangle \in \mathbb{C}^{d_2}$ orthonormal. Define

$$K_j := \sqrt{\lambda_j}\,\big(I_{d_1} \otimes |\phi_j\rangle\big), \qquad K_j^\dagger = \sqrt{\lambda_j}\,\big(I_{d_1} \otimes \langle\phi_j|\big), \qquad j = 1, \dots, r,$$

each a $d_1 d_2 \times d_1$ matrix (viewing $|\phi_j\rangle$ as a $d_2 \times 1$ column). Writing $\rho = \rho \otimes 1$ (the scalar 1 viewed as a $1 \times 1$ identity matrix) to align the Kronecker factors, the mixed-product property $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ gives

$$\begin{aligned} \sum_{j=1}^{r} K_j \rho K_j^\dagger &= \sum_{j=1}^{r} \lambda_j \big(I \otimes |\phi_j\rangle\big)(\rho \otimes 1)\big(I \otimes \langle\phi_j|\big) \\ &= \sum_{j=1}^{r} \lambda_j \big(I \rho\, I\big) \otimes \big(|\phi_j\rangle \cdot 1 \cdot \langle\phi_j|\big) \\ &= \rho \otimes \Big(\sum_{j=1}^{r} \lambda_j |\phi_j\rangle\langle\phi_j|\Big) = \rho \otimes \sigma. \end{aligned}$$

For completeness of the Kraus operators, using orthonormality $\langle\phi_j \,|\, \phi_j\rangle = 1$ and $\operatorname{Tr}(\sigma) = \sum_j \lambda_j = 1$,

$$\sum_{j=1}^{r} K_j^\dagger K_j = \sum_{j=1}^{r} \lambda_j \big(I \otimes \langle\phi_j|\big)\big(I \otimes |\phi_j\rangle\big) = \sum_{j=1}^{r} \lambda_j\, I \cdot \langle\phi_j \,|\, \phi_j\rangle = \Big(\sum_{j=1}^{r} \lambda_j\Big) I = I. \qquad \blacksquare$$

## §12.3. Appendix: proof of the no-cloning theorem

To make the statement of the no-cloning theorem (§12.1) precise enough to prove, we model a cloning machine as a fixed quantum circuit acting on the input register $A$ together with a "blank" ancilla register $B$ prepared in some fixed state $|e\rangle \in \mathbb{C}^d$: that is, a unitary $U$ on $\mathbb{C}^d \otimes \mathbb{C}^d$ with

$$U\big(|\chi\rangle \otimes |e\rangle\big) = |\chi\rangle \otimes |\chi\rangle \qquad \text{for every input state } |\chi\rangle \in \mathbb{C}^d.$$

**CLAIM** (No-cloning theorem, formal statement)**.** *Suppose $U$ is a unitary on $\mathbb{C}^d \otimes \mathbb{C}^d$ and $|e\rangle \in \mathbb{C}^d$ is fixed, with $U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle$ and $U(|\varphi\rangle \otimes |e\rangle) = |\varphi\rangle \otimes |\varphi\rangle$ for two given states $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^d$. Then $|\psi\rangle$ and $|\varphi\rangle$ must be equal or orthogonal.*

*Proof.* Since $U$ is unitary, it preserves inner products:

$$\begin{aligned} \langle\psi \,|\, \varphi\rangle = \langle\psi \,|\, \varphi\rangle \cdot \langle e \,|\, e\rangle &= \langle\psi \otimes e \,|\, \varphi \otimes e\rangle \\ &= \langle U(\psi \otimes e) \,|\, U(\varphi \otimes e)\rangle \\ &= \langle\psi \otimes \psi \,|\, \varphi \otimes \varphi\rangle = \langle\psi \,|\, \varphi\rangle^2, \end{aligned}$$

using $\langle e \,|\, e\rangle = 1$ ($|e\rangle$ normalized) and the mixed-product rule $\langle a \otimes b \,|\, c \otimes d\rangle = \langle a \,|\, c\rangle\,\langle b \,|\, d\rangle$. Writing $x := \langle\psi \,|\, \varphi\rangle$, this gives $x = x^2$, i.e. $x(x-1) = 0$, so $x = 0$ ($|\psi\rangle, |\varphi\rangle$ orthogonal) or $x = 1$ (which, since $|\psi\rangle, |\varphi\rangle$ are unit vectors, forces $|\varphi\rangle = |\psi\rangle$). $\blacksquare$

# *Homework 6*

1. **'Spooky action-at-a-distance'.**

   Recall that entanglement between two registers $A, B$ can be created only when a joint physical operation (such as a unitary gate) can be applied to $A$ and $B$. For instance, $A$ and $B$ can be brought together in a lab, a joint unitary can be applied, and afterwards $A$ and $B$ can be separated (no matter how far in space) while still maintaining their entangled state.

   Suppose *qubits* $A$ and $B$ are initially prepared in state $|0\rangle$ each.

   (a) Find a unitary gate that acts on $AB$ to create the entangled pair

   $$\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right).$$

   (b) Suppose we measure the observable $Z$ on qubit $A$ (this is a local measurement), what are the possible post-measurement states of $AB$ and with what probabilities do they occur?

   REMARK. Neither of the two post-measurement states of $AB$ is equal to the pre-measurement state. These two outcomes and their probabilities remain valid even if $A$ and $B$ are separated in space (after creating the entanglement). We observe that a physical intervention done locally at $A$ instantaneously affects the global state of $AB$, i.e., a local action creates an immediate global update even if the two qubits are located far away from each other. This is what Einstein called 'spooky action-at-a-distance'.

2. **Creating entanglement using measurement.** You showed in the previous question that entanglement can be created by doing a unitary operation on the composite system $AB$. We can also create entanglement using measurements, although we might not have control over which entangled state we end up with.

   Assume that we start with independently prepared qubits $A$ and $B$ in states $|0\rangle$ each. Design a projective measurement with 4 possible outcomes such that each of the post-measurement states of $AB$ is an entangled state.

   You must provide the following in your solutions:

   (a) an observable corresponding to your projective measurement, and steps to show that the projection operators correspond to the distinct eigenvalues of your observable.

   (b) proof that each of the 4 possible post-measurement states is actually an entangled state.

3. **Copying orthogonal states.** The no-cloning theorem (which we discussed very briefly during Lecture 12) says that we cannot build a quantum circuit that can create two independent copies (output of the circuit) of an arbitrary state (input to the circuit). In classical computing 'copy-and-paste' is of course allowed; this does not contradict the quantum no-cloning theorem — you *can* clone an input state if it is restricted to a pre-determined orthonormal set. In the classical setup this happens to be computational basis states $|0\rangle$, $|1\rangle$, etc.

   Suppose the qubit $A$ is the input to a quantum computer, and qubit $B$ is a register *present within* the computer (initialized to state $|0\rangle$). The output of the computer is $AB$.

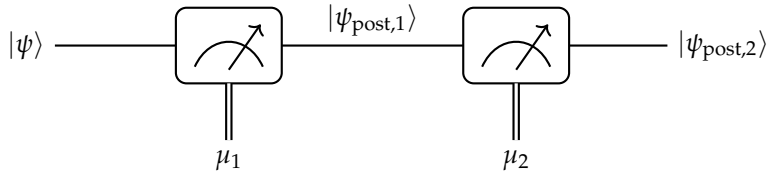
(a) Build a unitary gate for the quantum computer (to act on input $AB$) to clone the state of $A$ into the state of $B$ (so that $AB$ is in a product state) provided that the state of $A$ is restricted to $|0\rangle$ or $|1\rangle$ only.

(b) What is the output of your circuit if the input register $A$ is in state $|+\rangle$? Is $B$ a clone of $A$?

(c) Repeat part (a) for input restricted to $|+\rangle$ and $|-\rangle$.

4. **Repeated measurements.** Consider a projective measurement on $\mathbb{C}^d$ described by the observable $M = \sum_{\ell=1}^{L} \lambda_\ell P_\ell$, with distinct real numbers $\lambda_1, \ldots, \lambda_L$. The operators $P_1, \ldots, P_L$ are projections ($P_\ell^2 = P_\ell^\dagger = P_\ell$) that are complete, $\sum_{\ell=1}^{L} P_\ell = I$, and mutually orthogonal, $P_i P_j = 0$ for $i \neq j$.

   A register is prepared in a pure state $|\psi\rangle$, and the observable $M$ is measured twice in succession, as shown below. Let $\mu_1$ and $|\psi_{\text{post},1}\rangle$ be the classical outcome and post-measurement state of the first measurement, and let $\mu_2$ and $|\psi_{\text{post},2}\rangle$ be the classical outcome and post-measurement state of the second measurement (which acts on $|\psi_{\text{post},1}\rangle$).




   Assume that you (as an experimenter) can observe the classical outcomes of the measurements.

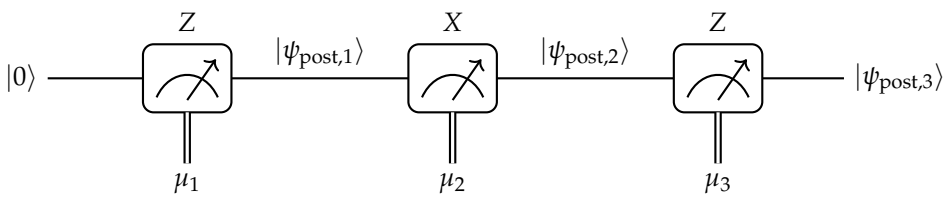
   (a) Show that $\mu_2 = \mu_1$ with probability 1, and that $|\psi_{\text{post},2}\rangle = |\psi_{\text{post},1}\rangle$. Hence a projective measurement that is immediately repeated with the same observable changes neither the classical outcome nor the state of the register.

   (b) Show that the same conclusion holds when the state fed into the first measurement is an arbitrary (possibly mixed) state $\rho$, that is, the two post-measurement states (possibly mixed states) are the same and the classical outcomes are the same.

   REMARK. This is the sense in which projective measurements are *repeatable*: the first measurement leaves the register in an eigenvector of $M$, and every subsequent measurement of $M$ reads back the same outcome without disturbing the state any further.

5. **On repeatability of measurements.** The repeatability observation holds only when the *same* observable is measured in succession. If these two measurements are interspersed with a measurement of a different observable, repeatability no longer holds.

   The figure below shows three measurements performed in succession on a qubit prepared in the state $|0\rangle$; as in the previous question, $\mu_i$ denotes the classical outcome and $|\psi_{\text{post},i}\rangle$ the post-measurement state of the $i$-th measurement. The three measurements are of the observables $Z, X, Z$, respectively.



Argue that there is a non-zero probability that $\mu_1 \neq \mu_3$ and $|\psi_{\text{post},1}\rangle \neq |\psi_{\text{post},3}\rangle$ (although the same observable is being measured).

6. **Deutsch's algorithm.** This is an introduction to the simplest quantum algorithm that shows an advantage over classical computing. You can refer to Section 1.4.3 of Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (10th Anniversary Edition, Cambridge University Press, 2010), or Chapter 6 of Phillip Kaye, Raymond Laflamme, and Michele Mosca, *An Introduction to Quantum Computing* (Oxford University Press, 2007), for a detailed treatment.

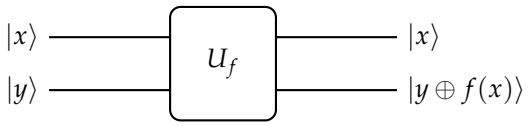
   *Querying a classical function quantumly.*

   Let $f : \{0,1\} \to \{0,1\}$ be a classical Boolean function. Think of $f$ as a sealed device — an *oracle* — whose internal workings are hidden from us: we may *query* it by supplying an input bit $x$ and reading off the output bit $f(x)$, but we cannot inspect how it computes.

   To use such a device inside a quantum circuit it must be a *unitary* gate, and hence reversible. The map $x \mapsto f(x)$ on its own is in general *not* reversible — if $f$ is constant, both inputs give the same output, so $x$ cannot be recovered from $f(x)$. The standard remedy is to use two single-qubit registers, a *query register* and a *target register*, and to define a gate $U_f$ on the computational basis by

$$U_f\big(|x\rangle \otimes |y\rangle\big) = |x\rangle \otimes |y \oplus f(x)\rangle, \qquad x, y \in \{0,1\},$$

   where $\oplus$ denotes addition modulo 2; $U_f$ is then extended linearly to superpositions of the four basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.




   Setting the target register to $|0\rangle$ gives

$$U_f\big(|x\rangle \otimes |0\rangle\big) = |x\rangle \otimes |f(x)\rangle,$$

   so a single application of $U_f$ — one *query* — writes $f(x)$ into the target register while leaving the query register unchanged.

   Thus, in the quantum scenario, querying a classical function is the same as applying the unitary $U_f$; if you quantumly query the function $n$ times in your algorithm, this means that you have applied the unitary gate $U_f$ exactly $n$ times in the circuit.

   *Query complexity.*

   In this black-box (oracle) model, an algorithm may access $f$ only through the oracle — classically by supplying $x$ and reading $f(x)$, quantumly by applying $U_f$ — and its *query complexity* is the number of oracle calls it makes, in the worst case over the possible functions $f$. Every other operation (state preparation, ordinary gates, measurements) is counted as free, so the query complexity captures how many times the algorithm must interrogate $f$ to complete its task. The question of interest is whether a quantum algorithm can decide a given property of $f$ using strictly fewer queries than any classical algorithm; Deutsch's algorithm is the simplest example where it can.

   *The problem: constant or balanced.*

   There are exactly four functions $f : \{0,1\} \to \{0,1\}$. Two are *constant* — $f(0) = f(1) = 0$ and $f(0) = f(1) = 1$ — and the other two are *balanced*, meaning $f$ takes the values 0 and 1 equally often; these are $f(x) = x$ and $f(x) = 1 \oplus x$. Thus $f$ is constant

when $f(0) = f(1)$ and balanced when $f(0) \neq f(1)$; equivalently, $f$ is constant or balanced according as the single bit $f(0) \oplus f(1)$ equals 0 or 1.

*Deutsch's problem.*

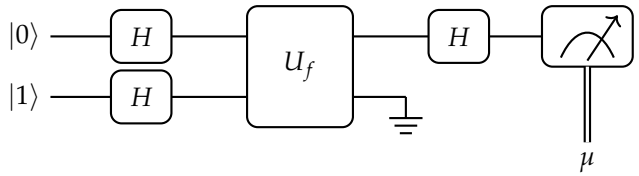
Given oracle access to an unknown $f$ — as the black box $x \mapsto f(x)$ classically, or as the gate $U_f$ quantumly — decide whether $f$ is constant or balanced (equivalently, compute the bit $f(0) \oplus f(1)$), using as few queries as possible.

*Classical query complexity.*

A classical algorithm can learn about $f$ only by evaluating it. One query returns a single value, say $f(0)$: this value is consistent both with the constant function equal to $f(0)$ everywhere and with the balanced function having $f(1) = 1 \oplus f(0)$, so a single query can never distinguish the two cases. Two queries always suffice: evaluate $f(0)$ and $f(1)$, and report "constant" if they are equal and "balanced" otherwise. Hence the classical query complexity of Deutsch's problem is exactly 2.

*Deutsch's algorithm.*

This algorithm uses exactly one quantum query to solve this problem. The circuit for this algorithm is shown, where the query register is measured in the computational basis. You must trace the state through this circuit, step by step, and show that the value $\mu$ indicates whether the function $f$ is constant or balanced.




For each of the four possible functions $f : \{0,1\} \to \{0,1\}$, find the classical outcome $\mu$ of the measurement. What is the value of $\mu$ when $f$ is balanced, and what is it when $f$ is constant?

7. Suppose $\rho$ and $\sigma$ are two different qubit states, i.e., density operators in $\mathbb{C}^{2\times 2}$ with $\rho \neq \sigma$. Argue that there exist orthonormal vectors $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^2$ such that the projective measurement with $P_1 = |\phi_1\rangle\langle\phi_1|$ and $P_2 = |\phi_2\rangle\langle\phi_2|$ has the following property: the probability of outcome $\lambda_1$ is different for states $\rho$ and $\sigma$.

   That is, there exists a projective measurement such that the probabilities of the classical outcomes (of the measurement) are different for $\rho$ and $\sigma$.

# *Lecture 13*

These notes are based on Chapter 3 of John Preskill's lecture notes for *Ph 219/CS 219* and Chapter 8 of Nielsen and Chuang, *Quantum Computation and Quantum Information* (10th Anniversary Edition, Cambridge University Press, 2010).

## §13.1. Kraus forms: operational significance

Recall from Lecture 12 (§12.2) that there are essentially four kinds of operations one can perform on a quantum register:

(1) *appending* a second, independently prepared register;

(2) *tracing out* (discarding) a subsystem of a composite register;

(3) applying a *unitary gate*;

(4) *measurement*, with or without a classically controlled follow-up gate.

Lecture 12 showed that the composition of two maps in Kraus form is again in Kraus form, and worked out the Kraus form of operation (1). In this section we exhibit the Kraus form of the remaining three. Together with the composition property this gives the operational significance of Kraus forms:

REMARK. *Any finite sequence of the four basic quantum operations — hence the input–output map of any quantum circuit or algorithm, however many gates, ancillas, and measurements it contains — can be written as a single Kraus form* $\rho \mapsto \sum_j K_j \rho K_j^\dagger$ *with* $\sum_j K_j^\dagger K_j = I$.

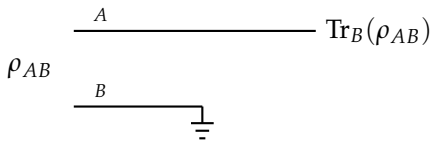
Throughout, a set of operators $\{K_j\}$ is a *Kraus form* of a map when the map is $\rho \mapsto \sum_j K_j \rho K_j^\dagger$ and the operators satisfy the completeness relation $\sum_j K_j^\dagger K_j = I$. The operators $K_j$ appearing in the Kraus form are called Kraus operators.

REMARK. *The classical information retrieved from a measurement operation can be used to decide which sequence of quantum instructions a quantum computer must execute next. This can be enforced by feeding the classical outcome of the measurement to a classical computer (say, a microcontroller) so that the microcontroller determines which unitary gate must be applied next.*

REMARK. *While we posed the classical control operation as using the measurement outcome to determine which gate to apply next, we can use the classical outcome to control* any *sequence of subsequent operations. Such as: choosing the observable of a subsequent measurement operation based on the value of the classical outcome of a previous measurement. However, this full generality of how classical outcomes can be used to steer the operations of a quantum computer is already captured in controlling the next unitary gate as described in (4) above; this follows from a result known as the Stinespring dilation theorem.*

We will now look at the Kraus forms of the remaining three basic operations that can be performed on a quantum computer.

**Tracing out.** Let $A$ and $B$ have state spaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, and let the joint register be in state $\rho_{AB}$. Discarding $B$ is the map $\rho_{AB} \mapsto \mathrm{Tr}_B(\rho_{AB})$:



From Homework 3, the partial traces can be written in the "sandwich" form

$$\mathrm{Tr}_B(\rho_{AB}) = \sum_{j=0}^{d_2-1} \big(I_{d_1} \otimes \langle j|\big)\, \rho_{AB}\, \big(I_{d_1} \otimes |j\rangle\big), \qquad \mathrm{Tr}_A(\rho_{AB}) = \sum_{j=0}^{d_1-1} \big(\langle j| \otimes I_{d_2}\big)\, \rho_{AB}\, \big(|j\rangle \otimes I_{d_2}\big),$$

where $\{|j\rangle\}$ is the computational basis of the register being discarded. Thus tracing out $B$ is a Kraus form with Kraus operators

$$K_j := I_{d_1} \otimes \langle j|, \qquad j = 0, 1, \ldots, d_2 - 1,$$

each a $d_1 \times d_1 d_2$ matrix. The completeness relation holds:

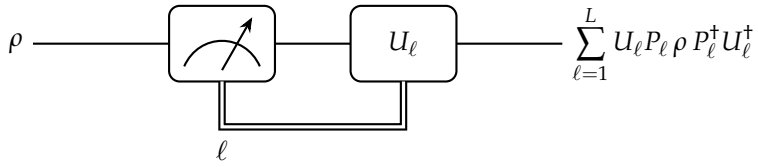
$$\sum_{j=0}^{d_2-1} K_j^\dagger K_j = \sum_{j=0}^{d_2-1} \big(I_{d_1} \otimes |j\rangle\big)\big(I_{d_1} \otimes \langle j|\big) = I_{d_1} \otimes \Big(\sum_{j=0}^{d_2-1} |j\rangle\langle j|\Big) = I_{d_1} \otimes I_{d_2} = I.$$

(One checks the sandwich formula on a product operator: $\big(I \otimes \langle j|\big)(C \otimes D)\big(I \otimes |j\rangle\big) = C \otimes (\langle j|D|j\rangle)$, and summing over $j$ gives $C\,\mathrm{Tr}(D)$, as required.) Tracing out $A$ is handled symmetrically, with $K_j = \langle j| \otimes I_{d_2}$.

**A unitary gate.** Applying a unitary $U$ is the map $\rho \mapsto U\rho U^\dagger$. This is already a Kraus form, with a single Kraus operator $K_1 = U$; the completeness relation is exactly unitarity, $K_1^\dagger K_1 = U^\dagger U = I$.

**Measurement.** Suppose we measure the observable $M = \sum_{\ell=1}^{L} \lambda_\ell P_\ell$, with $\{P_\ell\}$ the orthogonal eigenprojections ($P_k P_\ell = \delta_{k\ell} P_\ell$, $\sum_\ell P_\ell = I$).

*(a) With classical control.* Apply a unitary $U_\ell$ whenever the classical outcome is $\lambda_\ell$. When the outcome itself is not recorded, the register evolves as the average over branches (Lecture 12, §12.1):




This is a Kraus form with Kraus operators $K_\ell := U_\ell P_\ell$, $\ell = 1, \ldots, L$. Completeness follows from unitarity of the $U_\ell$ and $P_\ell^\dagger P_\ell = P_\ell^2 = P_\ell$:

$$\sum_{\ell=1}^{L} K_\ell^\dagger K_\ell = \sum_{\ell=1}^{L} P_\ell^\dagger U_\ell^\dagger U_\ell P_\ell = \sum_{\ell=1}^{L} P_\ell = I.$$

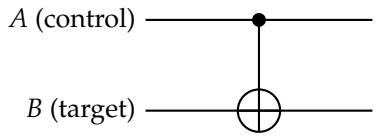
*(b) Without classical control.* This is the special case $U_\ell = I$ for every $\ell$. The map is $\rho \mapsto \sum_{\ell=1}^{L} P_\ell \rho P_\ell$, a Kraus form with Kraus operators $\{P_\ell\}$ and $\sum_\ell P_\ell^\dagger P_\ell = \sum_\ell P_\ell = I$.

The usage of the word 'control' in the above situation (measurement outcome deciding the subsequent operation) and its usage in the setting of 'one qubit controlling another qubit', as in the CNOT gate, carry different meanings. In the first scenario we extract information using measurement and decide what to do next based on this information; this is similar to what is known as 'feed forward' in control systems. In the scenario of CNOT gate, we have a unitary gate that is a quantum generalization of a classical operation. It so happens that this underlying classical operation can be described in terms of one classical bit (the control bit) determining what happens to the other classical bit (the target bit) — to flip the target bit or not. So the word 'control' in the name 'CNOT gate' refers to this underlying classical operation. When we apply CNOT to a pair of qubits we are not going to read/measure one qubit to determine what we are going to do to the other qubit.

CNOT is simply a unitary transformation applied to a composite system of two qubits. In particular, the two-qubit gate $\text{CNOT}_{1,2}$ acts on computational basis states as

$$\text{CNOT}_{1,2}\big(|a\rangle \otimes |b\rangle\big) = |a\rangle \otimes |a \oplus b\rangle, \qquad a, b \in \{0, 1\},$$

i.e. if we restrict our operation to classical states only it flips the target $B$ iff the control $A$ is $|1\rangle$:




It maps $|0\rangle \otimes |0\rangle \mapsto |0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |0\rangle \mapsto |1\rangle \otimes |1\rangle$. On a control qubit in a superposition, linearity gives

$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes |0\rangle \;\longmapsto\; \alpha\,|0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle,$$

which, for $\alpha, \beta \neq 0$, is an entangled state — in particular it is *not* the product $\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha|0\rangle + \beta|1\rangle\big)$. So CNOT copies a basis state but does not produce two copies of a superposed control qubit, in keeping with the no-cloning theorem (Lecture 12). Being unitary, its Kraus form is still the trivial single-operator one, $\{\text{CNOT}_{1,2}\}$.

## §13.2. Quantum channels and CPTP maps

**Quantum channels.** The maps above — and every finite composition of them — share a common form, which we now name.

**DEFINITION.** *A* quantum channel *is a linear map $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ that has a Kraus form: there exist finitely many operators $K_1, \ldots, K_r$ (each a $d_2 \times d_1$ matrix) such that*

$$\mathcal{E}(N) = \sum_{j=1}^{r} K_j\, N\, K_j^\dagger \quad \textit{for all } N \in \mathbb{C}^{d_1 \times d_1}, \qquad \textit{and} \qquad \sum_{j=1}^{r} K_j^\dagger K_j = I_{d_1}.$$

REMARK. *Quantum channels are called super-operators because they map operators (matrices) to operators.*

By §13.1 and the composition property of Lecture 12, any finite sequence of the four basic quantum operations is a quantum channel. We now record the properties that every quantum channel inherits from its Kraus form. Fix a quantum channel $\mathcal{E}(N) = \sum_j K_j N K_j^\dagger$.

**Basic properties.**

(1) **Linearity.** $\mathcal{E}(\alpha_1 N_1 + \alpha_2 N_2) = \alpha_1 \mathcal{E}(N_1) + \alpha_2 \mathcal{E}(N_2)$ for all $\alpha_1, \alpha_2 \in \mathbb{C}$ and $N_1, N_2 \in \mathbb{C}^{d_1 \times d_1}$. Indeed,

$$\begin{aligned}\mathcal{E}(\alpha_1 N_1 + \alpha_2 N_2) &= \sum_j K_j(\alpha_1 N_1 + \alpha_2 N_2)K_j^\dagger \\ &= \alpha_1 \sum_j K_j N_1 K_j^\dagger + \alpha_2 \sum_j K_j N_2 K_j^\dagger = \alpha_1 \mathcal{E}(N_1) + \alpha_2 \mathcal{E}(N_2).\end{aligned}$$

(2) **Hermiticity preservation.** If $N = N^\dagger$ then $\mathcal{E}(N)^\dagger = \mathcal{E}(N)$:

$$\mathcal{E}(N)^\dagger = \Big(\sum_j K_j N K_j^\dagger\Big)^\dagger = \sum_j K_j N^\dagger K_j^\dagger = \sum_j K_j N K_j^\dagger = \mathcal{E}(N).$$

(3) **Positivity preservation.** If $N \geq 0$ then $\mathcal{E}(N) \geq 0$. By (2) $\mathcal{E}(N)$ is Hermitian, and for any $|\phi\rangle$, setting $|\psi_j\rangle := K_j^\dagger|\phi\rangle$,

$$\langle\phi|\mathcal{E}(N)|\phi\rangle = \sum_j \langle\phi|K_j\, N\, K_j^\dagger|\phi\rangle = \sum_j \langle\psi_j|N|\psi_j\rangle \geq 0,$$

since $N \geq 0$ makes every term non-negative.

(4) **Trace preservation (TP).** $\mathrm{Tr}\big(\mathcal{E}(N)\big) = \mathrm{Tr}(N)$. Using linearity and cyclicity of the trace, then completeness,

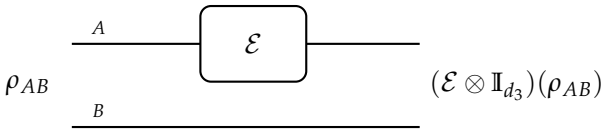
$$\begin{aligned}\mathrm{Tr}\big(\mathcal{E}(N)\big) = \mathrm{Tr}\Big[\sum_j K_j N K_j^\dagger\Big] &= \sum_j \mathrm{Tr}\big[K_j N K_j^\dagger\big] = \sum_j \mathrm{Tr}\big[N K_j^\dagger K_j\big] \\ &= \mathrm{Tr}\Big[N \sum_j K_j^\dagger K_j\Big] = \mathrm{Tr}[N].\end{aligned}$$

Properties (2)–(4) say that a quantum channel sends states to states: a density operator (Hermitian, positive, unit trace) is mapped to a density operator.

**CLAIM.** *If $\mathcal{E}$ is a quantum channel and $\rho$ is a density operator then $\mathcal{E}(\rho)$ is a density operator.*

*Proof.* Since $\rho \in \mathcal{D}(\mathbb{C}^{d_1})$, we have $\rho \geq 0$ and $\mathrm{Tr}(\rho) = 1$. Thus, $\mathcal{E}(\rho) \geq 0$ and $\mathrm{Tr}(\mathcal{E}(\rho)) = 1$, i.e., $\mathcal{E}(\rho) \in \mathcal{D}(\mathbb{C}^{d_2})$. ■

**(5) Complete positivity (CP).** There is a stronger sense in which a channel respects positivity. Imagine $\mathcal{E}$ acting on a register $A$ that may be entangled with another quantum register $B$ of dimension $d_3$. Applying $\mathcal{E}$ locally to $A$ is the map $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$, and to be physically sensible it must send every joint state $\rho_{AB}$ to a valid joint state. This must happen irrespective of the value of $d_3$ and the input state $\rho_{AB}$. In particular, $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$ must preserve positivity, i.e., map positive matrices to positive matrices.




Here $\mathbb{I}_{d_3 \times d_3}$ denotes the quantum channel or super-operator that acts trivially: it maps $N \mapsto N$ for all $N \in \mathbb{C}^{d_3 \times d_3}$.

REMARK. *The definition of $\mathcal{E} \otimes \mathbb{I}$ is as follows. Given any linear super-operator $\mathcal{E}$, we define $\mathcal{E} \otimes \mathbb{I}$ to be the linear super-operator that acts on Kronecker products as*

$$C \otimes D \mapsto \mathcal{E}(C) \otimes D.$$

*The action of $\mathcal{E} \otimes \mathbb{I}$ on any matrix in $\mathbb{C}^{d_1 d_3 \times d_1 d_3}$ then follows simply by linearity: if $A = \sum_i \alpha_i C_i \otimes D_i$ then*

$$\mathcal{E}(A) = \sum_i \alpha_i \mathcal{E}(C_i) \otimes D_i.$$

*This definition relies on the fact that every $A$ can be written as a linear combination of Kronecker products.*

REMARK. *Note that $\mathcal{E} \otimes \mathbb{I}$ is different from the physical operation that applies $\mathcal{E}$ on register $A$ and discards $B$. In the latter case the quantum device does not output register $B$; in the former case it does.*

**DEFINITION.** *A linear map $\mathcal{E}$ is* completely positive *(CP) if $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$ preserves positivity for every $d_3 \geq 1$.*

CP is a strictly stronger requirement than positivity preservation — the transpose map below is positive yet fails CP — but every quantum channel meets it.

**CLAIM.** *Every quantum channel $\mathcal{E}$ is completely positive.*

*Proof.* Let $\mathcal{E}$ have Kraus operators $\{K_j\}$ and choose any $d_3 \geq 1$. The operators $\{K_j \otimes I_{d_3}\}$ are a Kraus form for $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$: on a product operator $C \otimes D$,

$$\sum_j (K_j \otimes I_{d_3})(C \otimes D)(K_j \otimes I_{d_3})^\dagger = \sum_j \left(K_j C K_j^\dagger\right) \otimes D = \mathcal{E}(C) \otimes D = (\mathcal{E} \otimes \mathbb{I}_{d_3})(C \otimes D),$$

and both sides are linear in the argument, so they agree on all of $\mathbb{C}^{d_1 d_3 \times d_1 d_3}$. Completeness carries over,

$$\sum_j (K_j \otimes I_{d_3})^\dagger (K_j \otimes I_{d_3}) = \Big(\sum_j K_j^\dagger K_j\Big) \otimes I_{d_3} = I_{d_1} \otimes I_{d_3} = I.$$

Hence $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$ is itself a quantum channel, and by property (3) it preserves positivity. Since this statement holds for every $d_3 \geq 1$, $\mathcal{E}$ is CP. ∎

**CPTP maps.** The five properties above are exactly the abstract mathematical requirements one places on a physical evolution, and they get their own name.

**DEFINITION.** *A linear map $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ that preserves Hermiticity, is positive, is trace preserving, and is completely positive is called a* completely positive trace-preserving *(CPTP) map.*

Collecting the properties established above:

$$\mathcal{E} \text{ is a quantum channel} \quad \Longrightarrow \quad \mathcal{E} \text{ is a CPTP map.}$$

REMARK. *The converse is also true: every CPTP map admits a Kraus form (known as Choi's theorem or the Kraus representation theorem or the Choi-Kraus-Sudarshan theorem). We will state this formally in Lecture 14.*

REMARK. *Listing all the five properties stated above in the definition of CPTP maps is an overkill, while being harmless. In the appendix (§13.3) we prove that properties (1), (4) and (5) imply the remaining two properties. Thus, an equivalent and more concise definition of CPTP maps is: $\mathcal{E}$ is a CPTP map if it is linear, TP and CP.*

**Positive but not completely positive: the transpose map.** Properties (1)–(4) do *not* imply complete positivity. We exhibit a linear map on $\mathbb{C}^{2\times 2}$ that preserves Hermiticity, positivity, and the trace, yet is not CP.

Take $d_1 = d_2 = 2$ and let $\mathcal{E}$ be the *transpose* map,

$$\mathcal{E} : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}, \qquad \mathcal{E}(N) = N^T.$$

Properties (1)–(4) are readily checked:

(1) *Linearity*: $(\alpha_1 N_1 + \alpha_2 N_2)^T = \alpha_1 N_1^T + \alpha_2 N_2^T$.

(2) *Hermiticity*: $(N^T)^\dagger = (N^\dagger)^T$ always, so $N = N^\dagger$ gives $(N^T)^\dagger = N^T$.

(3) *Positivity*: $N^T$ has the same characteristic polynomial, hence the same eigenvalues, as $N$, and is Hermitian when $N$ is; so $N \geq 0 \Rightarrow N^T \geq 0$.

(4) *Trace preservation*: $\mathrm{Tr}(N^T) = \mathrm{Tr}(N)$.

Let $\rho = |\mathrm{EPR}\rangle\langle\mathrm{EPR}|$ with $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$, so $\rho \geq 0$. Expanding and grouping each term as (operator on $A$) $\otimes$ (operator on $B$),

$$\begin{aligned}\rho &= \tfrac{1}{2}\big(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\big) \\ &= \tfrac{1}{2}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\big).\end{aligned}$$

Applying $\mathcal{E}$ to the first factor (transpose on $A$: $|i\rangle\langle j| \mapsto |j\rangle\langle i|$) and leaving $B$ alone,

$$\begin{aligned}(\mathcal{E} \otimes \mathbb{I}_2)(\rho) &= \tfrac{1}{2}\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\big) \\ &= \tfrac{1}{2}\big(|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|\big).\end{aligned}$$

In the ordered basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ this is

$$(\mathcal{E} \otimes \mathbb{I}_2)(\rho) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This Hermitian matrix has determinant $\big(\frac{1}{2}\big)^4(1)(-1)(1) = -\frac{1}{16} < 0$, so it has an odd number of negative eigenvalues — at least one. (Explicitly, its eigenvalues are $\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}$.) Hence $(\mathcal{E} \otimes \mathbb{I}_2)(\rho) \not\geq 0$: the transpose map is positive but not completely positive.

REMARK. *The transpose map on states $\rho \mapsto \rho^T$ is therefore not physically realizable: no quantum device implements $N \mapsto N^T$ on a quantum register, since when applied on a part of an entangled state it would return an operator that is not a valid state.*

## §13.3. Appendix: a concise definition of CPTP maps

Recall the five defining properties of a CPTP map from §13.2: (1) linearity, (2) Hermiticity preservation, (3) positivity preservation, (4) trace preservation, and (5) complete positivity. The following claim justifies the concise definition stated in the remark of §13.2: a CPTP map is a linear map that is trace preserving and completely positive.

**CLAIM.** *Let $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ satisfy properties (1), (4) and (5), i.e. $\mathcal{E}$ is linear, trace preserving, and completely positive. Then $\mathcal{E}$ also satisfies properties (2) and (3), and hence is a CPTP map. Consequently,*

$$\mathcal{E} \text{ is linear, TP and CP} \quad \Longleftrightarrow \quad \mathcal{E} \text{ is a CPTP map.}$$

*Proof. Property (5) implies property (3).* Complete positivity requires that $\mathcal{E} \otimes \mathbb{I}_{d_3 \times d_3}$ preserve positivity for every $d_3 \geq 1$. Take $d_3 = 1$: the trivial channel $\mathbb{I}_{1\times 1}$ acts on scalars. Now consider any operator $N \in \mathbb{C}^{d_1 \times d_1}$ with $N \geq 0$. We have

$$\mathcal{E}(N) = \mathcal{E}(N) \otimes I_1 = (\mathcal{E} \otimes \mathbb{I}_{1\times 1})(N \otimes I_1) \geq 0,$$

since $\mathcal{E}$ is CP and $N \otimes I_1 = N \geq 0$.

*Properties (1) and (3) imply property (2).* Let $N \in \mathbb{C}^{d_1 \times d_1}$ be Hermitian. By the spectral theorem $N = \sum_i \mu_i |v_i\rangle\langle v_i|$ with real eigenvalues $\mu_i$ and an orthonormal eigenbasis $\{|v_i\rangle\}$. Split the sum according to the sign of $\mu_i$,

$$N = N_+ - N_-, \qquad N_+ := \sum_{i\,:\,\mu_i > 0} \mu_i |v_i\rangle\langle v_i|, \qquad N_- := \sum_{i\,:\,\mu_i < 0} (-\mu_i)\, |v_i\rangle\langle v_i|.$$

Both $N_+$ and $N_-$ are positive semidefinite (Hermitian, with non-negative eigenvalues). By linearity,

$$\mathcal{E}(N) = \mathcal{E}(N_+) - \mathcal{E}(N_-).$$

By property (3), $\mathcal{E}(N_+) \geq 0$ and $\mathcal{E}(N_-) \geq 0$; in particular both are Hermitian, and so is their difference. Hence $\mathcal{E}(N)^\dagger = \mathcal{E}(N)$, which is property (2).

Trace preservation is not used in the argument above. Property (4) nonetheless appears in the concise definition because it does not follow from (1) and (5): for instance $N \mapsto 2N$ is linear and completely positive but multiplies every trace by 2.

Finally, $\mathcal{E}$ now satisfies all of (1)–(5), so it is a CPTP map; the reverse implication is immediate, since a CPTP map satisfies (1), (4) and (5) by definition. ■

# *Lecture 14*

## §14.1. Closing the gap: characterization of quantum channels

**Recap.** Lecture 12 (§12.2) and Lecture 13 (§13.1) showed that every physically realizable operation on a quantum register — appending a register, tracing out a register, applying a unitary gate, and measurement, in any finite combination — has a Kraus form. Recall that a linear super-operator with a Kraus form is a *quantum channel* (Lecture 13, §13.2), so

$$\mathcal{E} \text{ is physically realizable} \quad \Longrightarrow \quad \mathcal{E} \text{ is a quantum channel.}$$

Lecture 13 (§13.2) then showed that every quantum channel is a CPTP map:

$$\mathcal{E} \text{ is a quantum channel} \quad \Longrightarrow \quad \mathcal{E} \text{ is a CPTP map.}$$

Recall the definition of a CPTP map: it is linear, preserves Hermiticity, preserves positivity, is trace preserving and is completely positive. We also saw in the appendix to Lecture 13 that for a succinct definition of CPTP we can harmlessly drop Hermiticity and positivity since these are already implied by linearity and CP.

The next steps in our coursework are to prove the converses of the above two implications, that is, to prove the following

(a) $\mathcal{E}$ is a quantum channel $\Rightarrow$ $\mathcal{E}$ is physically realizable

(b) $\mathcal{E}$ is a CPTP map $\Rightarrow$ $\mathcal{E}$ is a quantum channel.

The result in (b) is called *Choi's theorem*, or the *Choi-Kraus-Sudarshan theorem*, or the *Kraus representation theorem*. This is what we will prove in this lecture.

We will prove (a) in Lecture 15 through a technique called Stinespring's dilation. This technique shows that any quantum channel can be physically realized in a sequence of three steps:

1. append some registers to the input register,
2. apply a unitary gate, and
3. trace out some registers.

Such a representation of a quantum channel is called the Stinespring representation. Our proof in Lecture 15 will thus show that every quantum channel has a Stinespring representation. Conversely, every Stinespring representation is a sequence of three physically realizable operations, and hence has a Kraus form, and thus is a quantum channel. Thus, we have

$$\mathcal{E} \text{ is a quantum channel} \iff \mathcal{E} \text{ has a Stinespring representation.}$$

Combining all the results we know, including the ones to be proved in Lecture 14 and Lecture 15, we arrive at the fundamental characterization of quantum channels:

**THEOREM.** *The following four statements are equivalent. Let* $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ *for some* $d_1, d_2 \geq 1$.

1. $\mathcal{E}$ *is physically realizable,*
2. $\mathcal{E}$ *is a quantum channel, i.e., admits a Kraus form,*

3. *$\mathcal{E}$ is a CPTP map, i.e., satisfies linearity, TP and CP,*

4. *$\mathcal{E}$ has a Stinespring representation.*

This is a fundamental result providing a precise characterization of all quantum channels.

## §14.2. Choi's theorem

**THEOREM** (Choi's theorem). *If $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ is a CPTP map, then $\mathcal{E}$ has a Kraus form: there exist finitely many operators $V_1, \ldots, V_t$, each $V_k \in \mathbb{C}^{d_2 \times d_1}$, such that*

$$\mathcal{E}(N) = \sum_{k=1}^{t} V_k N V_k^\dagger \quad \text{for all } N \in \mathbb{C}^{d_1 \times d_1}, \qquad \sum_{k=1}^{t} V_k^\dagger V_k = I_{d_1}.$$

This proof is based on Section 4.4 of Mark M. Wilde, *Quantum Information Theory* (2nd Edition, Cambridge University Press, 2017).

You must think of the given CPTP map $\mathcal{E}$ as an abstract map or a black box that provides an output for a specified input. What we intend to do is show that we can fit a structured mathematical expression to this map.

The proof revolves around a matrix $J$, called the *Choi matrix* or the *Choi representation* of the CPTP map $\mathcal{E}$. We will first see what this matrix is, and make observations about some of its properties, and finally combine these observations to provide a Kraus form for $\mathcal{E}$.

Also, this proof is constructive, it tells us exactly how to construct the Kraus operators starting from a given CPTP map $\mathcal{E}$ through the Choi matrix $J$.

**The Choi matrix.** Let $\mathcal{E}$ be CPTP, hence linear, CP, and TP. Write $N \in \mathbb{C}^{d_1 \times d_1}$ in the computational basis,

$$N = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_1-1} \alpha_{ij} \, |i\rangle\langle j|, \qquad \alpha_{ij} = \text{the } (i,j) \text{ entry of } N,$$

so that, by linearity,

$$\mathcal{E}(N) = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_1-1} \alpha_{ij} \, \mathcal{E}\big(|i\rangle\langle j|\big).$$

Thus the $d_1^2$ matrices $\mathcal{E}(|i\rangle\langle j|) \in \mathbb{C}^{d_2 \times d_2}$, $i, j = 0, \ldots, d_1 - 1$, carry all the information needed to compute $\mathcal{E}$ on any input. We package them into a single $d_1 d_2 \times d_1 d_2$ matrix, arranged in $d_1 \times d_1$ blocks of size $d_2 \times d_2$, with $\mathcal{E}(|i\rangle\langle j|)$ in block position $(i, j)$:

$$J = \begin{pmatrix} \mathcal{E}(|0\rangle\langle 0|) & \mathcal{E}(|0\rangle\langle 1|) & \cdots & \mathcal{E}(|0\rangle\langle d_1-1|) \\ \mathcal{E}(|1\rangle\langle 0|) & \mathcal{E}(|1\rangle\langle 1|) & \cdots & \mathcal{E}(|1\rangle\langle d_1-1|) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{E}(|d_1-1\rangle\langle 0|) & \mathcal{E}(|d_1-1\rangle\langle 1|) & \cdots & \mathcal{E}(|d_1-1\rangle\langle d_1-1|) \end{pmatrix},$$

where the block in row $i$ and column $j$ is the $d_2 \times d_2$ matrix $\mathcal{E}(|i\rangle\langle j|)$.

Now fix a single pair $(i, j)$ and form the $d_1 \times d_1$ block matrix that is zero everywhere except in block position $(i, j)$, where it equals $\mathcal{E}(|i\rangle\langle j|)$:

$$\begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & \mathcal{E}(|i\rangle\langle j|) & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \qquad \text{(the nonzero block sits in row } i\text{, column } j\text{)}.$$

This is precisely the Kronecker product $|i\rangle\langle j| \otimes \mathcal{E}(|i\rangle\langle j|)$. Indeed, the matrix $|i\rangle\langle j| \in \mathbb{C}^{d_1 \times d_1}$ has a 1 in row $i$, column $j$, and 0 everywhere else,

$$|i\rangle\langle j| = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \qquad \text{(the single 1 sits in row } i\text{, column } j\text{)},$$

and forming the Kronecker product with $\mathcal{E}(|i\rangle\langle j|)$ replaces every scalar entry of $|i\rangle\langle j|$ by that scalar times the block $\mathcal{E}(|i\rangle\langle j|)$: each 0 entry becomes a 0 block, and the single 1 entry becomes the block $\mathcal{E}(|i\rangle\langle j|)$ itself,

$$|i\rangle\langle j| \otimes \mathcal{E}(|i\rangle\langle j|) = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \otimes \mathcal{E}(|i\rangle\langle j|) = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & \mathcal{E}(|i\rangle\langle j|) & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

exactly the matrix above. Summing this matrix over all $i, j = 0, \ldots, d_1 - 1$ reassembles the full matrix $J$ shown above, since each pair $(i, j)$ contributes to a different block. In summation notation:

**DEFINITION.** *The* Choi matrix *of $\mathcal{E}$, denoted $J(\mathcal{E})$ or simply $J$, is*

$$J := \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_1-1} |i\rangle\langle j| \otimes \mathcal{E}\big(|i\rangle\langle j|\big) \;\in\; \mathbb{C}^{d_1 d_2 \times d_1 d_2}.$$

The above equation tells us how to construct $J$ starting from $\mathcal{E}$. We need the expression for the reverse direction too: given $J$, what is the mathematical expression for $\mathcal{E}$? We know that $\mathcal{E}$ is completely specified by $\mathcal{E}(|i\rangle\langle j|)$ for all possible $i, j$. How do we extract $\mathcal{E}(|i\rangle\langle j|)$ from $J$? We can do so by extracting the $i^{\text{th}}$ row block and the $j^{\text{th}}$ column block from $J$.

**CLAIM.** $\mathcal{E}(|i\rangle\langle j|) = \big(\langle i| \otimes I_{d_2}\big)\, J\, \big(|j\rangle \otimes I_{d_2}\big)$.

*Proof.* We can see this pictorially, as a block-row selector and a block-column selector multiplying $J$ on the left and right. The operator $\langle i| \otimes I_{d_2}$ is the $d_2 \times d_1 d_2$ block-row matrix with $I_{d_2}$ in block position $i$ and zero blocks elsewhere, and $|j\rangle \otimes I_{d_2}$ is the $d_1 d_2 \times d_2$ block-column matrix with $I_{d_2}$ in block position $j$ and zero blocks elsewhere:

$$\langle i| \otimes I_{d_2} = \begin{bmatrix} 0 & \cdots & 0 & I_{d_2} & 0 & \cdots & 0 \end{bmatrix}, \qquad |j\rangle \otimes I_{d_2} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ I_{d_2} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Left-multiplying $J$ (in its block form shown above) by the block-row selector picks out the

$i$-th block row of $J$:

$$\begin{aligned}\big(\langle i|\otimes I_{d_2}\big)J &= \begin{bmatrix}0 & \cdots & I_{d_2} & \cdots & 0\end{bmatrix}\begin{pmatrix}\mathcal{E}(|0\rangle\langle 0|) & \cdots & \mathcal{E}(|0\rangle\langle d_1-1|)\\ \vdots & & \vdots\\ \mathcal{E}(|i\rangle\langle 0|) & \cdots & \mathcal{E}(|i\rangle\langle d_1-1|)\\ \vdots & & \vdots\\ \mathcal{E}(|d_1-1\rangle\langle 0|) & \cdots & \mathcal{E}(|d_1-1\rangle\langle d_1-1|)\end{pmatrix}\\ &= \begin{bmatrix}\mathcal{E}(|i\rangle\langle 0|) & \cdots & \mathcal{E}(|i\rangle\langle d_1-1|)\end{bmatrix},\end{aligned}$$

and right-multiplying this block row by the block-column selector picks out its $j$-th entry:

$$\big(\langle i|\otimes I_{d_2}\big)J\big(|j\rangle\otimes I_{d_2}\big) = \begin{bmatrix}\mathcal{E}(|i\rangle\langle 0|) & \cdots & \mathcal{E}(|i\rangle\langle j|) & \cdots & \mathcal{E}(|i\rangle\langle d_1-1|)\end{bmatrix}\begin{pmatrix}0\\ \vdots\\ I_{d_2}\\ \vdots\\ 0\end{pmatrix} = \mathcal{E}(|i\rangle\langle j|).$$

The row selector reaches into $J$ and picks out the block row indexed by $i$, and the column selector then picks out the single block in that row indexed by $j$. ■

It follows from this claim that for any $N = \sum_{i,j}\alpha_{i,j}|i\rangle\langle j|$, we have using linearity of $\mathcal{E}$

$$\mathcal{E}(N) = \sum_i\sum_j \alpha_{i,j}\big(\langle i|\otimes I_{d_2}\big)\,J\,\big(|j\rangle\otimes I_{d_2}\big).$$

We now move to the next part of the proof. We would like to factorize $J$ and use it in the expression

$$\mathcal{E}(|i\rangle\langle j|) = \big(\langle i|\otimes I_{d_2}\big)\,J\,\big(|j\rangle\otimes I_{d_2}\big)$$

which will immediately yield the Kraus form. To do so we first observe that $J$ is a positive operator.

**Claim.** $J \geq 0$.

*Proof.* Since $\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E}$ (the identity channel acting trivially on the first, unlabelled factor of $\mathbb{C}^{d_1}\otimes\mathbb{C}^{d_1}$, alongside $\mathcal{E}$ acting on the second) is linear and acts on Kronecker products as $C\otimes D\mapsto C\otimes\mathcal{E}(D)$ (Lecture 13, §13.2), and using $(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$ on each term $|i\rangle\langle j|\otimes|i\rangle\langle j| = (|i\rangle\otimes|i\rangle)(\langle j|\otimes\langle j|)$,

$$\begin{aligned}J &= \sum_{i,j}|i\rangle\langle j|\otimes\mathcal{E}(|i\rangle\langle j|) = (\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E})\Big[\sum_{i,j}|i\rangle\langle j|\otimes|i\rangle\langle j|\Big]\\ &= (\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E})\Big[\Big(\sum_i|i\rangle\otimes|i\rangle\Big)\Big(\sum_j\langle j|\otimes\langle j|\Big)\Big] = (\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E})(|\gamma\rangle\langle\gamma|),\end{aligned}$$

where $|\gamma\rangle = \sum_i|i\rangle\otimes|i\rangle$ and $\sum_j\langle j|\otimes\langle j| = |\gamma\rangle^\dagger$ (the two sums are adjoints of each other). The matrix $|\gamma\rangle\langle\gamma|$ is positive semidefinite: for any $|\phi\rangle$, $\langle\phi|\,|\gamma\rangle\langle\gamma|\,|\phi\rangle = |\langle\gamma\,|\,\phi\rangle|^2 \geq 0$. Since $\mathcal{E}$ is CP, $\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E}$ (a bystander register of dimension $d_1$) preserves positivity, so

$$J = (\mathbb{I}_{d_1\times d_1}\otimes\mathcal{E})(|\gamma\rangle\langle\gamma|) \geq 0.$$

■

Now we factorize $J$. Since $J \geq 0$, fact (1) of the two matrix-theoretic facts of Lecture 8 (§8.2) gives a factorization $J = BB^\dagger$ for some matrix $B$. Let the number of columns of $B$ be $t$, and denote these columns as $|\tilde{\varphi}_k\rangle$, $k = 1, \ldots, t$. Note that $|\tilde{\varphi}_k\rangle$ need not have unit norm and they need not be orthogonal. We have

$$J = BB^\dagger = \sum_{k=1}^{t} |\tilde{\varphi}_k\rangle\langle\tilde{\varphi}_k|, \qquad |\tilde{\varphi}_k\rangle \in \mathbb{C}^{d_1 d_2}.$$

Substituting into the identity $\mathcal{E}(|i\rangle\langle j|) = (\langle i| \otimes I_{d_2}) J (|j\rangle \otimes I_{d_2})$ established above,

$$\mathcal{E}(|i\rangle\langle j|) = \big(\langle i| \otimes I_{d_2}\big)\Big(\sum_{k=1}^{t} |\tilde{\varphi}_k\rangle\langle\tilde{\varphi}_k|\Big)\big(|j\rangle \otimes I_{d_2}\big) = \sum_{k=1}^{t} \Big[\big(\langle i| \otimes I_{d_2}\big)|\tilde{\varphi}_k\rangle\Big]\Big[\langle\tilde{\varphi}_k|\big(|j\rangle \otimes I_{d_2}\big)\Big]. \tag{$*$}$$

The operator $\langle i| \otimes I_{d_2}$ is the $d_2 \times d_1 d_2$ block-row matrix $[\,0 \;\cdots\; 0 \; I_{d_2} \; 0 \;\cdots\; 0\,]$ with $I_{d_2}$ in block position $i$; applied to a vector $|\tilde{\varphi}_k\rangle \in \mathbb{C}^{d_1 d_2}$, viewed as $d_1$ stacked blocks each of size $d_2$, it extracts the $i$-th block of $|\tilde{\varphi}_k\rangle$.

Pictorially, split $|\tilde{\varphi}_k\rangle$ into its $d_1$ stacked blocks (each a vector in $\mathbb{C}^{d_2}$), with the $i$-th one boxed:

$$|\tilde{\varphi}_k\rangle = \begin{pmatrix} \vdots \\ * \\ \boxed{i\text{-th block}} \\ * \\ \vdots \end{pmatrix},$$

and left-multiplying by the same block-row selector as above reaches in and pulls out exactly that block:

$$\big(\langle i| \otimes I_{d_2}\big)|\tilde{\varphi}_k\rangle = \begin{bmatrix} 0 \;\cdots\; 0 & I_{d_2} & 0 \;\cdots\; 0 \end{bmatrix} \begin{pmatrix} \vdots \\ * \\ i\text{-th block} \\ * \\ \vdots \end{pmatrix} = i\text{-th block of } |\tilde{\varphi}_k\rangle.$$

Define $V_k \in \mathbb{C}^{d_2 \times d_1}$ to be the matrix whose $i$-th column is this $i$-th block, i.e.

$$V_k|i\rangle := \big(\langle i| \otimes I_{d_2}\big)|\tilde{\varphi}_k\rangle, \qquad i = 0, \ldots, d_1 - 1.$$

In other word, if we *vectorize* the matrix $V_k$, that is, stack the columns of $V_k$ one below the other, starting from left-most column, we obtain the vector $|\tilde{\varphi}_k\rangle$, we denote this as

$$|\tilde{\varphi}_k\rangle = \mathrm{vec}(V_k).$$

Note that $\mathrm{vec} : \mathbb{C}^{d_2 \times d_1} \to \mathbb{C}^{d_1 d_2}$, and is a linear map (and in fact a bijection). Thus,

$$V_k = \mathrm{vec}^{-1}(|\tilde{\varphi}_k\rangle).$$

Now $\langle\tilde{\varphi}_k|(|j\rangle \otimes I_{d_2}) = (V_k|j\rangle)^\dagger = \langle j|V_k^\dagger$, and $(*)$ becomes

$$\mathcal{E}(|i\rangle\langle j|) = \sum_{k=1}^{t} V_k|i\rangle\langle j|V_k^\dagger.$$

For a general $N = \sum_{i,j} \alpha_{ij}|i\rangle\langle j|$, linearity of $\mathcal{E}$ gives

$$\mathcal{E}(N) = \sum_{i,j} \alpha_{ij}\, \mathcal{E}(|i\rangle\langle j|) = \sum_{i,j} \alpha_{ij} \sum_{k=1}^{t} V_k|i\rangle\langle j|V_k^\dagger = \sum_{k=1}^{t} V_k \Big(\sum_{i,j} \alpha_{ij}|i\rangle\langle j|\Big) V_k^\dagger = \sum_{k=1}^{t} V_k N V_k^\dagger,$$

which is the desired Kraus form with $r = t$. It remains only to verify completeness.

**CLAIM.** $\sum_{k=1}^{t} V_k^\dagger V_k = I_{d_1}$.

*Proof.* It suffices to show $\langle i|\big(\sum_k V_k^\dagger V_k\big)|j\rangle = \delta_{ij}$ for all $i, j$. Using cyclicity of the trace and $\mathrm{Tr}(|a\rangle\langle b|) = \langle b\,|\,a\rangle$,

$$\langle i|\Big(\sum_{k=1}^{t} V_k^\dagger V_k\Big)|j\rangle = \sum_{k=1}^{t}\langle i|V_k^\dagger V_k|j\rangle = \sum_{k=1}^{t}\mathrm{Tr}\big[V_k|j\rangle\langle i|V_k^\dagger\big]$$
$$= \mathrm{Tr}\Big[\sum_{k=1}^{t} V_k|j\rangle\langle i|V_k^\dagger\Big] = \mathrm{Tr}\big[\mathcal{E}(|j\rangle\langle i|)\big].$$

Since $\mathcal{E}$ is trace preserving, $\mathrm{Tr}[\mathcal{E}(|j\rangle\langle i|)] = \mathrm{Tr}[|j\rangle\langle i|] = \langle i\,|\,j\rangle = \delta_{ij}$. Hence $\langle i|(\sum_k V_k^\dagger V_k)|j\rangle = \delta_{ij}$ for all $i, j$, i.e. $\sum_k V_k^\dagger V_k = I_{d_1}$. ■

This completes the proof of Choi's theorem. ■

REMARK. *The procedure used in the proof is essentially the only way to construct Kraus operators for $\mathcal{E}$. It is somewhat straightforward to argue that if $V_1, V_2, \ldots$ are a set of Kraus operators for $\mathcal{E}$ (contructed by whatever means) then necessarily we must have*

$$J = \sum_k (\mathrm{vec}(V_k))\ (\mathrm{vec}(V_k))^\dagger.$$

*Hence, the vectorized form of the Kraus operators yield a valid factorization of $J$. A proof is given in the appendix (§14.4).*

REMARK. *The number of Kraus operators $t$ we ended up with is simply the number of columns of $B$, which need not be the smallest possible: any matrix $B$ with $J = BB^\dagger$ will do (Lecture 8, §8.2), and such factorizations are not unique. The* minimum *number of Kraus operators needed to represent $\mathcal{E}$ is exactly* $\mathrm{rank}(J)$. *Indeed, for* any *factorization $J = BB^\dagger$,* $\mathrm{rank}(B) = \mathrm{rank}(J)$, *so $B$ must have at least* $\mathrm{rank}(J)$ *columns, and hence at least* $\mathrm{rank}(J)$ *Kraus operators are needed. This minimum can be achieved: writing the spectral decomposition $J = \sum_k \lambda_k |v_k\rangle\langle v_k|$ (an orthonormal eigenbasis, $\lambda_k \geq 0$ since $J \geq 0$), exactly* $\mathrm{rank}(J)$ *of the $\lambda_k$ are strictly positive, and taking $B$'s columns to be $\sqrt{\lambda_k}|v_k\rangle$ for only these gives a valid factorization $J = BB^\dagger$ with precisely* $\mathrm{rank}(J)$ *columns.*

*The value* $\mathrm{rank}(J)$ *is called the* Choi rank *of the CPTP map $\mathcal{E}$.*

## §14.3. Unitary freedom in Kraus representations

Note that the proof of Choi's theorem tells us how to construct the Kraus operators. Given a CPTP map $\mathcal{E}$, first find the Choi matrix $J$, and then factorize it as $J = BB^\dagger$ (here we have some flexibility in the choice of $B$), and then list the columns of $B$ as $|\tilde{\varphi}_k\rangle$, and finally the Kraus operators are $V_k = \mathrm{vec}^{-1}(|\tilde{\varphi}_k\rangle)$. Each choice of the factor $B$ gives a different Kraus representation of $\mathcal{E}$. The freedom in the choice of Kraus representation is essentially the freedom we have in the choice of $B$ (including the choice of the number of columns $t$).

The proof above built one particular Kraus form for $\mathcal{E}$ out of one particular factorization $J = BB^\dagger$. Just as in Lecture 8 (§8.2), where the same state $\rho$ could arise from many different ensembles related by a unitary matrix, the same channel $\mathcal{E}$ can have many different Kraus forms, and they are all related to one another by a unitary matrix.

**From factorizations of the Choi matrix to Kraus operators.** Suppose $J = BB^\dagger = CC^\dagger$ are two factorizations of the Choi matrix, with $B$ or $C$ padded with a sufficient number of all-zero columns (Lecture 8, §8.2, "equalising the number of columns") to have the same number $t$ of columns, $|\tilde{\varphi}_1\rangle, \ldots, |\tilde{\varphi}_t\rangle$ for $B$ and $|\tilde{\zeta}_1\rangle, \ldots, |\tilde{\zeta}_t\rangle$ for $C$. By fact (2) of Lecture 8 (§8.2), there is a unitary $U = (u_{jk}) \in \mathbb{C}^{t\times t}$ with $C = BU$, i.e.

$$|\tilde{\zeta}_k\rangle = \sum_{j=1}^{t} u_{jk}\,|\tilde{\varphi}_j\rangle, \qquad k = 1, \ldots, t.$$

The map $\mathrm{vec}^{-1}$ (§14.2) is linear, so the Kraus operators $E_k := \mathrm{vec}^{-1}(|\tilde{\zeta}_k\rangle)$ built from $|\tilde{\zeta}_k\rangle$ are related to the Kraus operators $V_j := \mathrm{vec}^{-1}(|\tilde{\varphi}_j\rangle)$ built from $|\tilde{\varphi}_j\rangle$ by the very same unitary combination:

$$E_k = \mathrm{vec}^{-1}(|\tilde{\zeta}_k\rangle) = \mathrm{vec}^{-1}\Big(\sum_{j=1}^{t} u_{jk}\,|\tilde{\varphi}_j\rangle\Big) = \sum_{j=1}^{t} u_{jk}\,\mathrm{vec}^{-1}(|\tilde{\varphi}_j\rangle) = \sum_{j=1}^{t} u_{jk}\,V_j, \qquad k = 1,\dots,t.$$

Since $\{V_j\}$ and $\{E_k\}$ both arise from valid factorizations of the same Choi matrix $J$, the proof of Choi's theorem shows both are valid Kraus forms of $\mathcal{E}$:

$$\mathcal{E}(N) = \sum_{j=1}^{t} V_j N V_j^\dagger = \sum_{k=1}^{t} E_k N E_k^\dagger \qquad \text{for all } N.$$

We have thus proved the following result.

**THEOREM** (Unitary freedom in Kraus representations). *Let $\{V_j\}_{j=1}^{t_1}$ and $\{E_k\}_{k=1}^{t_2}$ be two finite sets of operators, each satisfying the completeness relation, and pad the shorter list with zero operators so that $t_1 = t_2 =: t$. Then*

$$\sum_{j=1}^{t} V_j N V_j^\dagger = \sum_{k=1}^{t} E_k N E_k^\dagger \ \textit{for all } N$$

$$\iff \quad E_k = \sum_{j=1}^{t} u_{jk}\,V_j \ \textit{for } k = 1,\dots,t, \textit{ for some unitary } U = (u_{jk}) \in \mathbb{C}^{t\times t}.$$

**Example.** Let $\mathcal{E}(N) = V_1 N V_1^\dagger + V_2 N V_2^\dagger$, and take the unitary

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The theorem produces the new Kraus operators

$$E_1 = \frac{1}{\sqrt{2}}V_1 + \frac{1}{\sqrt{2}}V_2, \qquad E_2 = \frac{1}{\sqrt{2}}V_1 - \frac{1}{\sqrt{2}}V_2,$$

and $\{E_1, E_2\}$ represents the very same channel: for any $N$,

$$\begin{aligned} E_1 N E_1^\dagger + E_2 N E_2^\dagger &= \tfrac{1}{2}(V_1+V_2)N(V_1+V_2)^\dagger + \tfrac{1}{2}(V_1-V_2)N(V_1-V_2)^\dagger \\ &= \tfrac{1}{2}\big[V_1 N V_1^\dagger + V_1 N V_2^\dagger + V_2 N V_1^\dagger + V_2 N V_2^\dagger\big] \\ &\quad + \tfrac{1}{2}\big[V_1 N V_1^\dagger - V_1 N V_2^\dagger - V_2 N V_1^\dagger + V_2 N V_2^\dagger\big] \\ &= V_1 N V_1^\dagger + V_2 N V_2^\dagger = \mathcal{E}(N), \end{aligned}$$

the cross terms $V_1 N V_2^\dagger$ and $V_2 N V_1^\dagger$ cancelling between the two brackets.

## §14.4. Appendix: proof of the vectorization remark

This appendix proves the claim made in the first remark of §14.2 — that any set of Kraus operators for $\mathcal{E}$, however constructed, vectorizes into a valid factorization of the Choi matrix $J$. This derivation was not done in the lecture.

**CLAIM.** *Let $V_1,\dots,V_r \in \mathbb{C}^{d_2\times d_1}$ be any Kraus operators for $\mathcal{E}$, i.e. $\mathcal{E}(N) = \sum_{k=1}^{r} V_k N V_k^\dagger$ for all $N \in \mathbb{C}^{d_1\times d_1}$. Then*

$$J = \sum_{k=1}^{r} \mathrm{vec}(V_k)\,\mathrm{vec}(V_k)^\dagger.$$

*Proof.* By definition of the Choi matrix and of $\mathcal{E}$'s Kraus form,

$$J = \sum_{i,j} |i\rangle\langle j| \otimes \mathcal{E}(|i\rangle\langle j|) = \sum_{i,j} |i\rangle\langle j| \otimes \Big( \sum_{k=1}^{r} V_k |i\rangle\langle j| V_k^\dagger \Big) = \sum_{k=1}^{r} \sum_{i,j} |i\rangle\langle j| \otimes V_k |i\rangle\langle j| V_k^\dagger .$$

Using the mixed-product property $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, with $A = |i\rangle$, $C = \langle j|$, $B = V_k|i\rangle$, $D = \langle j|V_k^\dagger$, each term factors as an outer product,

$$\begin{aligned} |i\rangle\langle j| \otimes V_k |i\rangle\langle j| V_k^\dagger &= \big(|i\rangle \otimes V_k|i\rangle\big)\big(\langle j| \otimes \langle j|V_k^\dagger\big) \\ &= \big(|i\rangle \otimes V_k|i\rangle\big)\big(|j\rangle \otimes V_k|j\rangle\big)^\dagger , \end{aligned}$$

so summing over $i, j$,

$$\begin{aligned} \sum_{i,j} |i\rangle\langle j| \otimes V_k |i\rangle\langle j| V_k^\dagger &= \Big( \sum_i |i\rangle \otimes V_k|i\rangle \Big) \Big( \sum_j |j\rangle \otimes V_k|j\rangle \Big)^\dagger \\ &= |w_k\rangle\langle w_k|, \qquad |w_k\rangle := \sum_i |i\rangle \otimes V_k|i\rangle . \end{aligned}$$

But $|w_k\rangle$ is exactly $\mathrm{vec}(V_k)$: stacking the columns $V_k|0\rangle, \ldots, V_k|d_1 - 1\rangle$ of $V_k$ one below the other (the definition of vec from §14.2) is precisely $\sum_i |i\rangle \otimes V_k|i\rangle$, since $|i\rangle \otimes |x\rangle$ places the vector $|x\rangle$ in the $i$-th $d_2$-sized block. Hence

$$J = \sum_{k=1}^{r} |w_k\rangle\langle w_k| = \sum_{k=1}^{r} \mathrm{vec}(V_k)\,\mathrm{vec}(V_k)^\dagger . \qquad \blacksquare$$

# *Homework 7*

1. **Density operators span the entire matrix space.** The class of density operators $\mathcal{D}(\mathbb{C}^d)$ associated with a vector space $\mathbb{C}^d$ are the operators that are positive and have trace 1. We will show in the present question that any operator in $\mathbb{C}^{d\times d}$ can be expressed as a linear combination of density operators. This observation will be used in the next question.

   This question uses some of the problems from earlier Homeworks. This is the sequence of arguments that you need to prove

   (a) Every positive operator is a scalar times a density operator.

   (b) Every Hermitian operator is the difference between two positive operators.
   HINT. Use the spectral decomposition.

   (c) Every operator (matrix in $\mathbb{C}^{d\times d}$) is a linear combination of two Hermitian operators.

   (d) Conclude that every operator is a linear combination of density operators.

2. **Extending the domain of a quantum channel from $\mathcal{D}(\mathbb{C}^d)$ to $\mathbb{C}^{d\times d}$.** This question is based on Appendix B of Mark M Wilde's *Quantum Information Theory*.

   *Context.* From an operational viewpoint a quantum channel is a mathematical abstraction of a physical process that transforms an input quantum state to an output quantum state. In this physical sense, a quantum channel is a map from $\mathcal{D}(\mathbb{C}^{d_1})$ to $\mathcal{D}(\mathbb{C}^{d_2})$, where $d_1$ and $d_2$ are the dimensions of the state spaces of the input and output registers, respectively, that is, formally a quantum channel $\mathcal{E}$ is a map

   $$\mathcal{E} : \mathcal{D}(\mathbb{C}^{d_1}) \to \mathcal{D}(\mathbb{C}^{d_2}). \tag{H7.1}$$

   It is reasonable to impose *convex linearity* on $\mathcal{E}$, that is

   $$\mathcal{E}(p_1\rho_1 + p_2\rho_2) = p_1\mathcal{E}(\rho_1) + p_2\mathcal{E}(\rho_2) \tag{H7.2}$$

   where $p_1, p_2 \geq 0$ and $p_1 + p_2 = 1$ and $\rho_1, \rho_2 \in \mathcal{D}(\mathbb{C}^{d_1})$. This follows from the idea that if the input is chosen between $\rho_1, \rho_2$ with probabilities $p_1, p_2$ then the outputs $\mathcal{E}(\rho_1)$ and $\mathcal{E}(\rho_2)$ occur with probabilities $p_1, p_2$.

   *Question.* We now argue that the domain of any function $\mathcal{E}$ as in (H7.1) that satisfies (H7.2) can be extended to a linear map

   $$\tilde{\mathcal{E}} : \mathbb{C}^{d_1\times d_1} \to \mathbb{C}^{d_2\times d_2}.$$

   In other words, given a convex-linear map $\mathcal{E}$ whose domain is density operators there exists a linear map $\tilde{\mathcal{E}}$ whose domain is *all* operators such that

   $$\tilde{\mathcal{E}}(\rho) = \mathcal{E}(\rho) \text{ for all density operators } \rho \in \mathcal{D}(\mathbb{C}^{d_1}), \tag{H7.3}$$

   see Figure H7.1. This is the mathematical sense in which it is okay to talk about a quantum channel acting on a arbitrary operator (even if that operator is not a density matrix).

   We will now assume that a map $\mathcal{E}$ satisfying (H7.1) and (H7.2) is given to us. We will constructively build its linear extension $\tilde{\mathcal{E}}$, satisfying (H7.3), using the same logical sequence as in question 1.

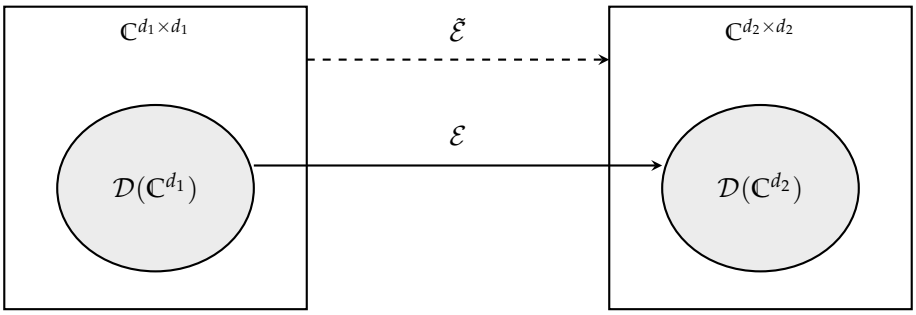



Figure H7.1: The quantum channel $\mathcal{E}$ acts on the convex set of density operators $\mathcal{D}(\mathbb{C}^{d_1}) \subset \mathbb{C}^{d_1 \times d_1}$, mapping it into $\mathcal{D}(\mathbb{C}^{d_2}) \subset \mathbb{C}^{d_2 \times d_2}$. Its linear extension $\tilde{\mathcal{E}}$ acts on the full operator space $\mathbb{C}^{d_1 \times d_1}$, mapping it into $\mathbb{C}^{d_2 \times d_2}$, and agrees with $\mathcal{E}$ on density operators.

(a) Since $\tilde{\mathcal{E}}$ has to be linear, what must be the value of $\tilde{\mathcal{E}}(0)$.
REMARK. The all-zero matrix $O$ does not lie in $\mathcal{D}(\mathbb{C}^{d_1})$ (why?).

(b) Since every positive operator is a scalar times a density operator, how will you define $\tilde{\mathcal{E}}(N)$ for a positive operator $N$?

(c) Now show how $\tilde{\mathcal{E}}$ will act on Hermitian operators.

(d) Finally, consider an arbitrary operator as input to $\tilde{\mathcal{E}}$.

REMARK. Although we did not prove it here, this construction of $\tilde{\mathcal{E}}$ from $\mathcal{E}$ is *consistent* (that is, every input matrix is assigned a unique output matrix, the construction does not contradict itself) and is *unique* (that is, every $\mathcal{E}$ has a unique linear extension $\tilde{\mathcal{E}}$).

3. **Choi representation of quantum channels.** *Context.* In many instances, a quantum channel is specified to us only in terms of how it acts on density operators. We might need to use the idea in question (2) to mathematically characterize its action on all inputs; for instance to find the Choi representation of a quantum channel.

   In this question we will not distinguish a physical quantum channel and its linearization, and use the notation $\mathcal{E}$ for both. This notation is consistent with our lecture notes where we use $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ to denote a quantum channel or a CPTP map.

   *Question.* Consider the case $d_1 = d_2 = 2$. Consider the quantum channel $\mathcal{E}$ that acts on density operators as below

$$\mathcal{E}(\rho) = \frac{1}{2}\rho + \frac{1}{2}|0\rangle\langle 0| \text{ for all } \rho \in \mathcal{D}(\mathbb{C}^2).$$

   $\mathcal{E}$ can be realized by choosing between the input state $\rho$ and the pure state $|0\rangle\langle 0|$ with equal probability.

   (a) Consider the four operators $|i\rangle\langle j|$, $i, j \in \{0, 1\}$. Which of them belong to $\mathcal{D}(\mathbb{C}^2)$ ?

   (b) Determine $\mathcal{E}(|i\rangle\langle j|)$ for all $i, j$.
   REMARK. You will have to rely on question (2) for this.

   (c) What is $J$ and what is the Choi rank of $\mathcal{E}$, i.e., what is $\text{rank}(J)$?

   (d) Find a Kraus representation of $\mathcal{E}$ in which the number of Kraus operators equals the Choi rank.
   HINT. You must factorize $J$ as $BB^\dagger$ where the number of columns of $B$ equals $\text{rank}(J)$. You can use a computer for this if you have to.

4. **A quantum channel with maximum Choi rank.** Consider a quantum channel $\mathcal{E}$ whose Choi representation $J$ is a scalar times the identity matrix, i.e.,

$$J = \alpha I_{d_1 d_2 \times d_1 d_2}.$$

The rank of $J$ is $d_1 d_2$ (assuming $\alpha \neq 0$), which is the maximum possible rank among Choi matrices since they are matrices of size $d_1 d_2 \times d_1 d_2$.

(a) Find the value of $\alpha$.

(b) Find $\mathcal{E}(|i\rangle\langle j|)$ for all $i, j \in \{0, 1, \ldots, d_1 - 1\}$.

(c) Find a Kraus representation for $\mathcal{E}$.

(d) Find a simplified expression for $\mathcal{E}(\rho)$ for all $\rho \in \mathcal{D}(\mathbb{C}^{d_1})$.

5. Argue that $\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$ is an entangled state.

6. **Maximally entangled quantum states.** Consider a composite register $AB$ where the state spaces of both $A$ and $B$ are $\mathbb{C}^d$. A pure state $\psi$ on $AB$ is called *maximally entangled* when the states of the individual registers $A$ and $B$ are both $\frac{1}{d} I_{d \times d}$. Recall that $I/d$ is called the *maximally mixed state*.

Use Schmidt decomposition to identify *all* maximally entangled states.

REMARK. Maximally entangled states are an important resource in quantum communication and computing. For instance, they are used in quantum teleportation and in superdense coding.

REMARK. These states are also the answer to Question 7 of Homework 5.

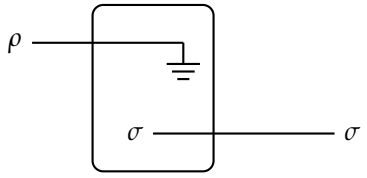
7. **Verifying unitary freedom in Kraus form.** Suppose $\mathcal{E}(N) = \sum_{k=1}^{t} V_k N V_k^\dagger$ and $E_j = \sum_k u_{j,k} V_k$ for some unitary matrix $U$. Directly verify

$$\sum_{k=1}^{t} V_k N V_k^\dagger = \sum_{j=1}^{t} E_j N E_j^\dagger$$

by substituting the expression for $E_j$ on the RHS.

8. Consider the situation where a quantum computer contains a pre-prepared state $\sigma \in \mathbb{C}^{d_2 \times d_2}$ in a register $B$ at its disposal. The input to the computer is a register $A$ (with associated Hilbert space $\mathbb{C}^{d_1}$). Denote the state of this register as $\rho$. The computer does the following: it receives the input register $A$, immediately traces it out, and outputs the register $B$. Thus, the output is always the pre-determined state $\sigma$ for any input state $\rho$.

You must find a Kraus form for this operation (in the language introduced in Lecture 13, this is a *quantum channel* and is known as the *replacement channel*). The box below signifies the quantum computer.




9. **Kraus-like representation of linear maps.** Suppose $\mathcal{E} : \mathbb{C}^{d \times d} \to \mathbb{C}^{d \times d}$ is a linear map, i.e.,

$$\mathcal{E}(\alpha_1 N_1 + \alpha_2 N_2) = \alpha_1 \mathcal{E}(N_1) + \alpha_2 \mathcal{E}(N_2).$$

$\mathcal{E}$ is not necessarily CPTP; we are only given that $\mathcal{E}$ is linear. Also, let $r = \text{rank}(J)$ where $J$ is the Choi representation of $\mathcal{E}$. You must show that there exist $V_1, \ldots, V_r, W_1, \ldots, W_r \in \mathbb{C}^{d \times d}$ such that

$$\mathcal{E}(N) = \sum_{k=1}^{r} V_k N W_k^\dagger \quad \text{for all } N \in \mathbb{C}^{d \times d}.$$

# *Lecture 15*

Lecture 14 (§14.1) recalled the one-way chain physically realizable ⇒ quantum channel ⇒ CPTP map (Lectures 12–13), proved the converse CPTP map ⇒ quantum channel (Choi's theorem, Lecture 14 §14.2), and named — but deferred to this lecture — the remaining converse needed for the four-way characterization theorem of Lecture 14: quantum channel ⇒ physically realizable. This lecture supplies that missing proof via a technique called *Stinespring's dilation* (§15.1), and then turns to a natural follow-up question: which quantum channels are reversible (§15.2)?

## §15.1. Stinespring dilation

**The technique.** Stinespring's dilation is a mathematical tool that lets us physically realize *any* quantum channel using a sequence of three steps:

(1) append one or more independently prepared registers to the input register,

(2) apply a single unitary gate on all the registers, and

(3) discard (trace out) one or more of the registers.

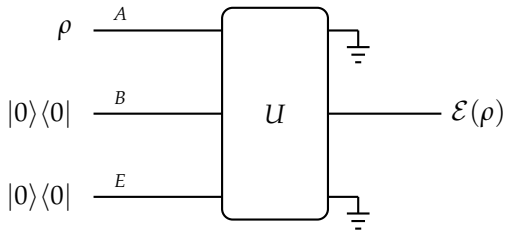
Such a representation of a quantum channel (equivalently, of a CPTP map) is called a *Stinespring dilation* or *Stinespring representation*.

The Stinespring representation is not unique. The number of registers appended to the input register and the unitary gate used are not unique. We present one such representation for the general case where $d_1$ and $d_2$ need not be equal, and consider a thorough treatment of the special case $d_1 = d_2$.

Concretely, let $\mathcal{E} : \mathbb{C}^{d_1 \times d_1} \to \mathbb{C}^{d_2 \times d_2}$ be a quantum channel with Kraus form

$$\mathcal{E}(\rho) = \sum_{j=0}^{r-1} K_j \rho K_j^\dagger \qquad \text{for all } \rho \in \mathbb{C}^{d_1 \times d_1}, \qquad \sum_{j=0}^{r-1} K_j^\dagger K_j = I_{d_1}.$$

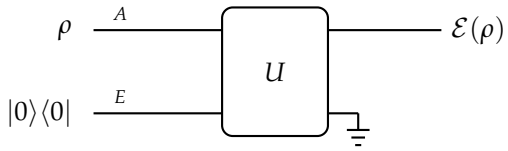
When $d_1 \neq d_2$, we can obtain a Stinespring representation by appending *two* ancilla registers to the input register $A$ (which holds $\rho \in \mathbb{C}^{d_1 \times d_1}$): a register $B$ of dimension $d_2$ (that will hold the output state) and a register $E$ of dimension $r$ (the 'environment' register that will create necessary entanglement with $B$ to produce the required quantum channel), both prepared in the fixed state $|0\rangle\langle 0|$. A single unitary $U$ is applied to the joint register $ABE$, after which $A$ and $E$ are discarded and $B$ alone is retained:




We will not prove this general statement. Instead we prove only the special case $d_1 = d_2 = d$, where the extra register $B$ is unnecessary.

The Appendix (which was not covered during the lecture) tells how the proof can be modified to work when $d_1 \neq d_2$.

**The case $d_1 = d_2 = d$.** When $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$, the input register $A$ itself can act as the output register once the ancilla (that is, the environment register $E$) is discarded: append a single register $E$ of dimension $r$ (or any dimension $\geq r$) prepared in $|0\rangle\langle 0|$, apply a unitary $U$ on $AE$, and discard $E$:




That is,

$$\mathcal{E}(\rho) = \mathrm{Tr}_E\big[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\big] \qquad \text{for all } \rho \in \mathbb{C}^{d\times d},$$

which we call a *Stinespring representation* of $\mathcal{E}$. We now prove that every quantum channel on $\mathbb{C}^{d\times d}$ admits such a representation. To be precise, we need to show that there exists a unitary operator $U$ as described in the following theorem.

**THEOREM** (Stinespring dilation, $d_1 = d_2 = d$)**.** *Let $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ be a quantum channel with Kraus operators $K_0, \ldots, K_{r-1} \in \mathbb{C}^{d\times d}$, so that $\mathcal{E}(\rho) = \sum_{j=0}^{r-1} K_j \rho K_j^\dagger$ and $\sum_{j=0}^{r-1} K_j^\dagger K_j = I_d$. Then there exists a unitary $U \in \mathbb{C}^{dr\times dr}$ such that*

$$\mathcal{E}(\rho) = \mathrm{Tr}_E\big[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\big] \qquad \textit{for all } \rho \in \mathbb{C}^{d\times d}.$$

The proof needs two ingredients, established next: a fact about extending an orthonormal set of vectors to a unitary matrix, and a lemma that lets us check the theorem only on pure states $\rho = |\psi\rangle\langle\psi|$.

**Extending an orthonormal set to a unitary.** The following linear-algebra fact is one of the key points behind the construction: any two orthonormal sets of vectors of the same size, in the same vector space, are related by *some* unitary matrix. This unitary matrix is not unique if the sets of orthonormal vectors are not bases of the vector space.

**CLAIM.** *Let $|a_1\rangle, \ldots, |a_L\rangle$ and $|b_1\rangle, \ldots, |b_L\rangle$ be two orthonormal sets of vectors in $\mathbb{C}^n$ (the same number $L \leq n$ of vectors in each). Then there exists a unitary $U \in \mathbb{C}^{n\times n}$ such that $U|a_i\rangle = |b_i\rangle$ for every $i = 1, \ldots, L$.*

*Proof.* This proof was not done during the lecture, but is included here for completeness.

Extend $|a_1\rangle, \ldots, |a_L\rangle$ to an orthonormal basis $|a_1\rangle, \ldots, |a_n\rangle$ of $\mathbb{C}^n$, and likewise extend $|b_1\rangle, \ldots, |b_L\rangle$ to an orthonormal basis $|b_1\rangle, \ldots, |b_n\rangle$ of $\mathbb{C}^n$ (both extensions exist by the standard basis-extension / Gram–Schmidt argument). Define

$$U := \sum_{i=1}^{n} |b_i\rangle\langle a_i|.$$

Since $\{|a_i\rangle\}_{i=1}^n$ is an orthonormal basis, $U|a_k\rangle = \sum_{i=1}^n |b_i\rangle\langle a_i \,|\, a_k\rangle = |b_k\rangle$ for every $k = 1, \ldots, n$, and in particular for $k = 1, \ldots, L$, giving the required action. It remains to check $U$ is unitary:

$$U^\dagger U = \Big(\sum_{i=1}^{n} |a_i\rangle\langle b_i|\Big)\Big(\sum_{k=1}^{n} |b_k\rangle\langle a_k|\Big) = \sum_{i=1}^{n}\sum_{k=1}^{n} |a_i\rangle\langle b_i \,|\, b_k\rangle\langle a_k| = \sum_{i=1}^{n} |a_i\rangle\langle a_i| = I_n,$$

using orthonormality of $\{|b_i\rangle\}$ ($\langle b_i \,|\, b_k\rangle = \delta_{ik}$) and completeness of the basis $\{|a_i\rangle\}$. A square matrix with $U^\dagger U = I_n$ is unitary. ∎

**Verification is required for pure states only.** It suffices to verify the Stinespring representation on pure states $\rho = |\psi\rangle\langle\psi|$; equality on all states $\rho \in \mathcal{D}(\mathbb{C}^d)$ then follows automatically, by linearity.

**CLAIM.** *Let $\mathcal{E}, \mathcal{F} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ be quantum channels. If $\mathcal{E}(|\psi\rangle\langle\psi|) = \mathcal{F}(|\psi\rangle\langle\psi|)$ for every pure state $|\psi\rangle \in \mathbb{C}^d$, then $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for every $\rho \in \mathcal{D}(\mathbb{C}^d)$.*

*Proof.* Every $\rho \in \mathcal{D}(\mathbb{C}^d)$ arises from some ensemble, $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ (e.g. its spectral decomposition). By linearity of $\mathcal{E}$ and $\mathcal{F}$,

$$\begin{aligned}\mathcal{E}(\rho) &= \mathcal{E}\Big(\sum_i p_i|\psi_i\rangle\langle\psi_i|\Big) = \sum_i p_i\,\mathcal{E}(|\psi_i\rangle\langle\psi_i|)\\ &= \sum_i p_i\,\mathcal{F}(|\psi_i\rangle\langle\psi_i|) = \mathcal{F}\Big(\sum_i p_i|\psi_i\rangle\langle\psi_i|\Big) = \mathcal{F}(\rho).\end{aligned}$$

■

**Proof of the Stinespring dilation theorem.** Fix the Kraus operators $K_0, \ldots, K_{r-1}$ of $\mathcal{E}$, and work in $\mathbb{C}^d \otimes \mathbb{C}^r$, the tensor product of the input register $A$ (computational basis $|0\rangle, \ldots, |d-1\rangle$) and the environment register $E$ (computational basis $|0\rangle, \ldots, |r-1\rangle$). Consider two collections of $d$ vectors in $\mathbb{C}^d \otimes \mathbb{C}^r \cong \mathbb{C}^{dr}$:

$$\text{Collection 1:}\quad |i\rangle_A \otimes |0\rangle_E, \qquad i = 0, \ldots, d-1,$$

and

$$\text{Collection 2:}\quad |c_i\rangle := \sum_{j=0}^{r-1} (K_j|i\rangle)_A \otimes |j\rangle_E, \qquad i = 0, \ldots, d-1.$$

The first collection is clearly orthonormal, since $\{|i\rangle\}$ is an orthonormal basis of $A$ and $|0\rangle_E$ is a fixed unit vector. The second collection is orthonormal too:

$$\begin{aligned}\langle c_i \,|\, c_l\rangle &= \Big(\sum_{j=0}^{r-1} K_j|i\rangle \otimes |j\rangle\Big)^\dagger \Big(\sum_{j'=0}^{r-1} K_{j'}|l\rangle \otimes |j'\rangle\Big)\\ &= \sum_{j=0}^{r-1}\sum_{j'=0}^{r-1} \langle i|K_j^\dagger K_{j'}|l\rangle\ \langle j \,|\, j'\rangle\\ &= \sum_{j=0}^{r-1} \langle i|K_j^\dagger K_j|l\rangle\\ &= \langle i|\Big(\sum_{j=0}^{r-1} K_j^\dagger K_j\Big)|l\rangle\\ &= \langle i|I_d|l\rangle = \langle i \,|\, l\rangle = \delta_{il},\end{aligned}$$

using $\langle j \,|\, j'\rangle = \delta_{jj'}$ and the completeness relation $\sum_j K_j^\dagger K_j = I_d$.

Both collections are orthonormal sets of $d$ vectors in $\mathbb{C}^{dr}$, so the orthonormal-extension claim above promises that there exists a unitary $U \in \mathbb{C}^{dr\times dr}$ such that

$$U\big(|i\rangle_A \otimes |0\rangle_E\big) = \sum_{j=0}^{r-1} K_j|i\rangle \otimes |j\rangle_E \qquad \text{for every } i = 0, \ldots, d-1.$$

Now let $|\psi\rangle = \sum_i \alpha_i |i\rangle \in \mathbb{C}^d$ be any pure state. By linearity of $U$,

$$\begin{aligned} U\big(|\psi\rangle \otimes |0\rangle_E\big) &= \sum_i \alpha_i \, U\big(|i\rangle \otimes |0\rangle_E\big) \\ &= \sum_i \alpha_i \sum_{j=0}^{r-1} K_j |i\rangle \otimes |j\rangle_E \\ &= \sum_{j=0}^{r-1} K_j \Big( \sum_i \alpha_i |i\rangle \Big) \otimes |j\rangle_E \\ &= \sum_{j=0}^{r-1} K_j |\psi\rangle \otimes |j\rangle_E . \end{aligned}$$

Now, note that

$$U\left(|\psi\rangle \otimes |0\rangle\right) = \sum_{j=0}^{r-1} K_j |\psi\rangle \otimes |j\rangle_E ,$$

is the state of $AE$ immediately after applying the unitary (see the earlier figure). In order to perform the partial trace we need the density operator version of this state, which is

$$U\big(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|\big)U^\dagger$$

Expanding this expression we obtain

$$\Big( \sum_{j=0}^{r-1} K_j |\psi\rangle \otimes |j\rangle \Big) \Big( \sum_{i=0}^{r-1} \langle\psi| K_i^\dagger \otimes \langle i| \Big) = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} K_j |\psi\rangle\langle\psi| K_i^\dagger \otimes |j\rangle\langle i| .$$

Tracing out $E$, and using $\mathrm{Tr}(|j\rangle\langle i|) = \langle i \,|\, j\rangle = \delta_{ij}$,

$$\mathrm{Tr}_E\big[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger\big] = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} K_j |\psi\rangle\langle\psi| K_i^\dagger \, \mathrm{Tr}(|j\rangle\langle i|) = \sum_{j=0}^{r-1} K_j |\psi\rangle\langle\psi| K_j^\dagger = \mathcal{E}(|\psi\rangle\langle\psi|).$$

Thus, using

$$\mathcal{F}(\rho) := \mathrm{Tr}_E\big[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\big],$$

to denote the quantum channel realized by the Stinespring circuit (append register, perform unitary, discard register), we have shown $\mathcal{F}(|\psi\rangle\langle\psi|) = \mathcal{E}(|\psi\rangle\langle\psi|)$ for every pure state $|\psi\rangle \in \mathbb{C}^d$. That is, this circuit coincides with the given quantum channel on all pure state inputs. We thus conclude that $\mathcal{F}(\rho) = \mathcal{E}(\rho)$ for every $\rho \in \mathcal{D}(\mathbb{C}^d)$, which is exactly the statement of the theorem. ■

REMARK. *The Stinespring representation of a quantum channel is not unique: different choices of Kraus operators for $\mathcal{E}$ (related by the unitary freedom of Lecture 14 §14.3), or different valid choices of the extending unitary $U$ in the orthonormal-extension claim above, yield different $U$'s realizing the same $\mathcal{E}$.*

REMARK. *Even the* dimension *of the ancilla register $E$ need not be the same across two Stinespring representations of the same channel: the proof above used the smallest natural choice,* $\dim E = r$ *(the number of Kraus operators), but any* $\dim E \geq r$ *also works, padding the Kraus set with extra zero operators.*

Together with Choi's theorem (Lecture 14 §14.2), this completes the proof of quantum channel ⇒ physically realizable: appending a register, applying a unitary, and discarding a register are each physically realizable operations (Lectures 12–13), and a finite composition of physically realizable operations is physically realizable. This closes the loop on all four implications of the characterization theorem stated in Lecture 14 §14.1.

## §15.2. Reversible quantum channels

**Erratum/Important Remark.** During Lecture 15 we called these quantum channels *invertible* as well as *reversible*. The technically precise usage is *reversible*. *Invertibility* of a channel could mean something else, although some authors still use *invertible* and *reversible* synonymously. It is safer if we stick to the adjective *reversible*.

**Definition.** Given a quantum channel $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$, we say that $\mathcal{E}$ is *reversible* if there exists a quantum channel $\mathcal{F} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ such that $\mathcal{F} \circ \mathcal{E} = \mathbb{I}$, the identity channel. That is,

$$\mathcal{F}(\mathcal{E}(\rho)) = \rho \qquad \text{for all } \rho \in \mathcal{D}(\mathbb{C}^d).$$

REMARK. *Since $\mathcal{D}(\mathbb{C}^d)$ spans $\mathbb{C}^{d\times d}$ as a complex vector space, $\mathcal{F}(\mathcal{E}(\rho)) = \rho$ for all $\rho \in \mathcal{D}(\mathbb{C}^d)$ already forces $\mathcal{F}(\mathcal{E}(N)) = N$ for* every *matrix $N \in \mathbb{C}^{d\times d}$, by linearity of $\mathcal{F} \circ \mathcal{E}$. (Indeed, any $N \in \mathbb{C}^{d\times d}$ decomposes as $N = H_1 + iH_2$ with $H_1 = \frac{1}{2}(N + N^\dagger)$, $H_2 = \frac{1}{2i}(N - N^\dagger)$ Hermitian; and any Hermitian $H$ has a spectral decomposition $H = \sum_k \lambda_k |v_k\rangle\langle v_k|$ with $\lambda_k \in \mathbb{R}$ and each $|v_k\rangle\langle v_k| \in \mathcal{D}(\mathbb{C}^d)$, so $H$ — and hence $N$ — is a complex-linear combination of density operators.)*

**A linear algebra fact.** The characterization of reversible channels rests on the following fact, which says that if a pure state's projector splits as a sum of (not necessarily normalized or orthogonal) rank-one projectors, each of those must itself be proportional to the original state.

**CLAIM.** *Let $|\psi\rangle \in \mathbb{C}^d$ be a unit vector and let $|a_1\rangle, \ldots, |a_n\rangle \in \mathbb{C}^d$ be such that $|\psi\rangle\langle\psi| = \sum_{j=1}^n |a_j\rangle\langle a_j|$. Then $|a_j\rangle = \alpha_j|\psi\rangle$ for some scalar $\alpha_j \in \mathbb{C}$, for every $j = 1, \ldots, n$.*

*Proof.* This proof was not done during the lecture.

We invoke the unitary freedom in ensemble representations (Lecture 8, §8.2). Since $|\psi\rangle$ is a unit vector, $|\psi\rangle\langle\psi| = BB^\dagger$ with the single-column matrix $B := |\psi\rangle \in \mathbb{C}^{d\times 1}$; and by hypothesis $|\psi\rangle\langle\psi| = \sum_{j=1}^n |a_j\rangle\langle a_j| = CC^\dagger$ with $C := \begin{bmatrix} |a_1\rangle & \cdots & |a_n\rangle \end{bmatrix} \in \mathbb{C}^{d\times n}$. Padding $B$ with $n-1$ zero columns (Lecture 8, §8.2, "equalising the number of columns" — this leaves $BB^\dagger$ unchanged) gives $\tilde{B} := \begin{bmatrix} |\psi\rangle & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix} \in \mathbb{C}^{d\times n}$, with $\tilde{B}\tilde{B}^\dagger = |\psi\rangle\langle\psi| = CC^\dagger$ and the same number of columns as $C$. By fact (2) of Lecture 8 (§8.2), there is a unitary $U = (u_{kj}) \in \mathbb{C}^{n\times n}$ with $C = \tilde{B}U$. Comparing the $j$-th column on both sides, and using that only the first column of $\tilde{B}$ is nonzero,

$$|a_j\rangle = \sum_{k=1}^n \tilde{B}_{:,k}\, u_{kj} = |\psi\rangle\, u_{1j},$$

so $|a_j\rangle = \alpha_j|\psi\rangle$ with $\alpha_j := u_{1j}$, for every $j = 1, \ldots, n$. ∎

**Characterization of reversible channels.**

**THEOREM.** *A quantum channel $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ is reversible if and only if $\mathcal{E}(\rho) = U\rho U^\dagger$ for some unitary $U \in \mathbb{C}^{d\times d}$.*

*Proof.* ($\Leftarrow$) Suppose $\mathcal{E}(\rho) = U\rho U^\dagger$ for a unitary $U$. Define $\mathcal{F}(\sigma) := U^\dagger \sigma U$; this is a quantum channel (a single Kraus operator $U^\dagger$, with completeness $(U^\dagger)^\dagger(U^\dagger) = UU^\dagger = I_d$, since $U$ is unitary). Then

$$\mathcal{F}(\mathcal{E}(\rho)) = U^\dagger\big(U\rho U^\dagger\big)U = (U^\dagger U)\rho(U^\dagger U) = \rho \qquad \text{for all } \rho,$$

so $\mathcal{F} \circ \mathcal{E} = \mathbb{I}$ and $\mathcal{E}$ is reversible.

($\Rightarrow$) Suppose $\mathcal{E}$ is reversible, with inverse channel $\mathcal{F}$. Let $E_1, \ldots, E_p$ be Kraus operators for $\mathcal{E}$ and $F_1, \ldots, F_q$ Kraus operators for $\mathcal{F}$; padding the shorter list with zero matrices (which changes neither channel nor its completeness relation), assume both lists have the same length $m := \max(p, q)$: $E_1, \ldots, E_m$ and $F_1, \ldots, F_m$.

By composing Kraus forms (Lecture 13), $\mathcal{F} \circ \mathcal{E}$ has Kraus operators $\{F_i E_j\}_{i,j=1}^m$, so

$$\mathcal{F}(\mathcal{E}(\rho)) = \sum_{i=1}^{m} \sum_{j=1}^{m} F_i E_j \, \rho \, E_j^\dagger F_i^\dagger = \rho \qquad \text{for all } \rho.$$

In particular, for any pure state $|\psi\rangle \in \mathbb{C}^d$, taking $\rho = |\psi\rangle\langle\psi|$,

$$|\psi\rangle\langle\psi| = \sum_{i=1}^{m} \sum_{j=1}^{m} \big(F_i E_j |\psi\rangle\big)\big(F_i E_j |\psi\rangle\big)^\dagger.$$

By the proportionality claim above (with the $m^2$ vectors $F_i E_j |\psi\rangle$ playing the role of the $|a_j\rangle$'s there), each $F_i E_j |\psi\rangle$ is proportional to $|\psi\rangle$ — and this holds for every $|\psi\rangle \in \mathbb{C}^d$ and every $i, j = 1, \ldots, m$. That is, for each fixed pair $(i, j)$, every vector in $\mathbb{C}^d$ is an eigenvector of $F_i E_j$.

We utilize another linear algebra fact: *if $M \in \mathbb{C}^{d \times d}$ is such that every $|\psi\rangle \in \mathbb{C}^d$ is an eigenvector of $M$, then $M = \alpha I_d$ for some $\alpha \in \mathbb{C}$.* Applying this with $M = F_i E_j$ gives scalars $\alpha_{ij} \in \mathbb{C}$ with

$$F_i E_j = \alpha_{ij} \, I_d \qquad \text{for every } i, j = 1, \ldots, m.$$

By completeness condition applied to the Kraus operators of $\mathcal{F} \circ \mathcal{E}$, we have

$$I = \sum_{i,j} E_j^\dagger F_i^\dagger F_i E_j = \sum_{i,j} \alpha_{ij}^* \alpha_{ij} I = \sum_{i,j} |\alpha_{ij}|^2 I$$

and thus

$$\sum_{i,j} |\alpha_{ij}|^2 = 1.$$

Thus, at least one $\alpha_{ij}$ is non-zero. Without loss of generality assume that $\alpha_{11} \neq 0$. We have then

$$F_1 E_1 = \alpha_{11} I$$

which implies both $F_1$ and $E_1$ are invertible. Now, we want to show that all $E_j$ are just scalar multiples of each other. Start from

$$F_1 E_1 = \alpha_{11} I, \; F_1 E_2 = \alpha_{12} I, \; \ldots, F_1 E_m = \alpha_{1m} I.$$

Since $F_1^{-1}$ exists, we then have

$$E_1 = \alpha_{11} F_1^{-1}, \; E_2 = \alpha_{12} F_1^{-1}, \; \ldots, E_m = \alpha_{1m} F_1^{-1},$$

which shows that all Kraus operators of $\mathcal{E}$ are just scalar multiples of a single operator.

Thus, we have

$$\begin{aligned}
\mathcal{E}(\rho) &= \sum_j E_j \rho E_j^\dagger \\
&= \sum_j \alpha_{1j} F_1^{-1} \; \rho \; \alpha_{1j}^* (F_1^{-1})^\dagger \\
&= \left( \sum_j |\alpha_{1j}|^2 \right) F_1^{-1} \; \rho \; (F_1^{-1})^\dagger \\
&= \left( \sqrt{\sum_j |\alpha_{1j}|^2} F_1^{-1} \right) \; \rho \; \left( \sqrt{\sum_j |\alpha_{1j}|^2} F_1^{-1} \right)^\dagger \\
&= K \rho K^\dagger
\end{aligned}$$

where $K = \sqrt{\sum_j |\alpha_{1j}|^2} F_1^{-1}$. Since this is a Kraus form with a single Kraus operator $K$ we know that $K$ must be unitary. ■

## §15.3. Appendix: Stinespring dilation for any $d_1, d_2$

Remember the characterization of the unitary $U$ on which the proof for the case $d_1 = d_2 = d$ relied

$$U\left(|\psi\rangle_A \otimes |0\rangle_E\right) = \sum_{j=0}^{r-1} \left(K_j|\psi\rangle\right)_A \otimes |j\rangle_E,$$

Now recall the circuit for Stinespring dilation for arbitrary $d_1, d_2$. We had two ancillary registers: one output register $B$ and one environment register $E$. In this case, we need to 'move' the information present in $A$ to $B$ via the Kraus operators $K_j$ and entangle this information with the register in $E$. We do this as follows

$$U\left(|\psi\rangle_A \otimes |0\rangle_B \otimes |0\rangle_E\right) = \sum_{j=0}^{r-1} |0\rangle_A \otimes \left(K_j|\psi\rangle\right)_B \otimes |j\rangle_E = |0\rangle_A \otimes \left(\sum_{j=0}^{r-1} \left(K_j|\psi\rangle\right)_B \otimes |j\rangle_E\right).$$

Thus, $A$ and $BE$ are in a product state, and hence, tracing out $A$ immediately shows that the state of $BE$ is

$$\sum_{j=0}^{r-1} \left(K_j|\psi\rangle\right)_B \otimes |j\rangle_E$$

We are now left with tracing out $E$ to arrive at the state of $B$. This is along the same lines as the proof of the case $d_1 = d_2$.

The fact that $U$ defined as above is unitary again follows from the completeness relation of $\{K_j\}$.

# *Lecture 16*

These notes are based on Chapter 3 of John Preskill's lecture notes for *Ph 219/CS 219* and Chapters 1 and 10 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*.

Lecture 15 completed the characterization of quantum channels and proved that a channel $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ is reversible if and only if $\mathcal{E}(\rho) = U\rho U^\dagger$ for some unitary $U$. This lecture opens with two quick consequences of that theorem: an equivalent, order-reversed notion of reversibility, and a mild relaxation of the definition of a quantum channel called a *quantum operation* (§16.1). It then turns to the lecture's main topic, *quantum noise* (§16.2): the irreversible channels that arise when a register is allowed to interact, uncontrolled, with an inaccessible environment, worked out in full for the qubit dephasing channel (§16.3) and the amplitude-damping channel (§16.4, with the Kraus-form and density-operator derivations continued in the Appendix, §16.5).

## §16.1. A note on terminology

**Reversible channels, revisited.** Recall (Lecture 15, §15.2) that a quantum channel $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ is *reversible* if there is a quantum channel $\mathcal{F}$ such that $\mathcal{F} \circ \mathcal{E} = \mathbb{I}$, the identity channel.

We reserve and use the word *reversible* for such quantum channels. Some authors use the word *invertible* to mean something other than *reversible*; we will not be talking about invertible channels in this course. See Appendix for information about invertible channels.

Lecture 15 went on to prove:

$$\mathcal{E} \text{ is reversible } \iff \mathcal{E}(N) = UNU^\dagger \text{ for every } N \in \mathbb{C}^{d\times d},$$

for some unitary $U \in \mathbb{C}^{d\times d}$.

A natural question is whether reversibility still requires an inverse channel that undoes $\mathcal{E}$ when applied *after* it ($\mathcal{F} \circ \mathcal{E}$), or whether an inverse applied *before* $\mathcal{E}$ ($\mathcal{E} \circ \mathcal{F}$) would do just as well. The following corollary, an easy consequence of the theorem above, says the two notions coincide.

**COROLLARY.** *A quantum channel $\mathcal{E} : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ is reversible if and only if there exists a quantum channel $\mathcal{F}$ such that $\mathcal{E} \circ \mathcal{F} = \mathbb{I}$.*

*Proof.* ($\Rightarrow$) Suppose $\mathcal{E}$ is reversible. By the theorem above, $\mathcal{E}(\rho) = U\rho U^\dagger$ for some unitary $U$. Define $\mathcal{F}(\rho) := U^\dagger \rho U$; this is a quantum channel (a single Kraus operator $U^\dagger$, with completeness $(U^\dagger)^\dagger(U^\dagger) = UU^\dagger = I$). Then, for all $\rho$,

$$\begin{aligned}(\mathcal{E} \circ \mathcal{F})(\rho) &= \mathcal{E}\left(U^\dagger \rho U\right) \\ &= U\left(U^\dagger \rho U\right)U^\dagger \\ &= (UU^\dagger)\rho(UU^\dagger) \\ &= \rho,\end{aligned}$$

so $\mathcal{E} \circ \mathcal{F} = \mathbb{I}$.

($\Leftarrow$) Suppose there is a quantum channel $\mathcal{F}$ with $\mathcal{E} \circ \mathcal{F} = \mathbb{I}$. Then $\mathcal{F}$ is itself reversible: $\mathcal{E} \circ \mathcal{F} = \mathbb{I}$ is exactly the statement that applying $\mathcal{E}$ *after* $\mathcal{F}$ recovers the identity channel, so $\mathcal{E}$ plays the role of the inverse channel required by the definition of reversibility (with the roles of the two channels in that definition swapped). By the theorem above, $\mathcal{F}(\rho) = U\rho U^\dagger$ for some unitary $U$. Since $\mathcal{E} \circ \mathcal{F} = \mathbb{I}$,

$$\mathcal{E}\left(U\rho U^\dagger\right) = \rho \qquad \text{for all } \rho \in \mathcal{D}(\mathbb{C}^d).$$

Extending by linearity to all of $\mathbb{C}^{d\times d}$ (as in Lecture 15's remark following the definition of reversibility),

$$\mathcal{E}\left(U\rho U^\dagger\right) = \rho \qquad \text{for every } \rho \in \mathbb{C}^{d\times d}.$$

Writing $N := U\rho U^\dagger$ — so that $\rho = U^\dagger N U$, and $N$ ranges over all of $\mathbb{C}^{d\times d}$ as $\rho$ does, since $U$ is invertible — this reads

$$\mathcal{E}(N) = U^\dagger N U \qquad \text{for every } N \in \mathbb{C}^{d\times d}.$$

Since $U^\dagger$ is unitary, this is exactly the form required by the theorem above (with $U^\dagger$ playing the role of "the unitary"), so $\mathcal{E}$ is reversible. ■

**Quantum channels versus quantum operations.**

**DEFINITION.** *A linear map $\mathcal{E} : \mathbb{C}^{d_1\times d_1} \to \mathbb{C}^{d_2\times d_2}$ is called a* quantum operation *if it has a Kraus form $\mathcal{E}(N) = \sum_j K_j N K_j^\dagger$ (finitely many $K_j \in \mathbb{C}^{d_2\times d_1}$) such that*

$$\sum_j K_j^\dagger K_j \leq I_{d_1},$$

*that is,*

$$I_{d_1} - \sum_j K_j^\dagger K_j \geq 0.$$

A quantum channel (Lecture 13) is exactly a quantum operation whose Kraus operators satisfy the completeness relation with *equality*, $\sum_j K_j^\dagger K_j = I_{d_1}$; every quantum channel is therefore a quantum operation, but a quantum operation need not be a channel. Quantum operations can be used to model the scenarios where we partially observe the classical outcome of the measurement.

We will primarily use quantum channels throughout this course, but be aware of the meaning of the technical term 'quantum operation'.

## §16.2. Quantum noise

Quantum noise arises from irreversible quantum channels, which occur when a quantum register interacts with the environment/bath and the environment is not accessible to us.

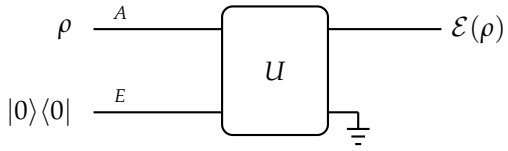
Noise can arise in a quantum computer in any of the following stages (also known as 'locations' in fault-tolerant quantum computing)

- state preparation (such as preparing a quantum register in a pre-determined state, say $|0\rangle$),
- application of a unitary gate,
- storage of quantum information (or waiting for the next step of a quantum algorithm),
- measurement.

The fundamental problem in fault-tolerant quantum computing (FTQC) is to design a reliable quantum computer using unreliable locations (i.e., components/stages). Surprisingly, this is possible if the probability of error at each location is not too high.

In this course, we will be concerned with errors in the wait/storage location and correcting them using quantum error correcting codes. A general FTQC is built on top of these basic quantum error correction techniques.

**The general picture.** Suppose we prepare a state $\rho$ in register $A$. At this point in time, the register $A$ and the environment $E$ are in a product state $\rho_A \otimes |0\rangle\langle 0|_E$. Because of the physical interaction between $A$ and $E$, over some time the state of $AE$ evolves unitarily to $U(\rho \otimes |0\rangle\langle 0|)U^\dagger$:




so that the state of $A$ alone (tracing out $E$) is

$$\mathcal{E}(\rho) = \mathrm{Tr}_E\left[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\right] = \sum_j E_j \rho E_j^\dagger,$$

with the Kraus operators $E_j$ satisfying the completeness relation

$$\sum_j E_j^\dagger E_j = I.$$

This quantum channel with operators $\{E_j\}$ arises because of two reasons:

1. Unintended interaction with the environment: a lot of effort goes into isolating quantum memories from their environments. Nevertheless, complete physical isolation of $A$ is impossible. The overall unitary evolution of $AE$ is based on the Hamiltonian of the composite system $AE$ (which is closed and hence can evolve unitarily only).

2. Inability to access the environment: typically, the environment system is not accessible to the experimenter. It can not be controlled or measured. This lack-of-access is modelled as 'tracing out $E$'. If the register $E$ was indeed accessible, then the unitary map (that acts on $AE$, not just on $A$) can be reversed and no information will be lost.

**Quantum channels produce ensembles.** Applying $\mathcal{E}$ to a pure state $|\psi\rangle\langle\psi|$,

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_j E_j|\psi\rangle\langle\psi|E_j^\dagger = \sum_j \||E_j|\psi\rangle\|^2 \left(\frac{E_j|\psi\rangle}{\||E_j|\psi\rangle\|}\right)\left(\frac{E_j|\psi\rangle}{\||E_j|\psi\rangle\|}\right)^\dagger,$$

which is the density operator of the ensemble of pure states

$$\left\{\left(\||E_j|\psi\rangle\|^2,\ \frac{E_j|\psi\rangle}{\||E_j|\psi\rangle\|}\right)\right\}_j$$

(omitting any $j$ with $E_j|\psi\rangle = 0$); these are indeed probabilities, since

$$\sum_j \||E_j|\psi\rangle\|^2 = \langle\psi|\left(\sum_j E_j^\dagger E_j\right)|\psi\rangle = \langle\psi\,|\,\psi\rangle = 1.$$

We can think of $\mathcal{E}$ as acting on the pure input state $|\psi\rangle$ to create an ensemble, where one of the normalized versions of $E_j|\psi\rangle$ shows up in the output with appropriate probability. Note that this probability $\||E_j|\psi\rangle\|^2$ depends on both $E_j$ and $|\psi\rangle$.

We will now see examples of quantum channels acting on qubit systems, $\rho \in \mathcal{D}(\mathbb{C}^2)$. The first two examples, phase damping and amplitude damping, are **two of the most practically relevant quantum noise models.**

## §16.3. Dephasing (phase-damping) channel

Let $A$ denote the qubit which stores the quantum information of interest to us. Let the qubit $E$ denote the 'environment' (a stray particle) that inadvertently comes into contact with $A$, and scatters away. This interaction changes the state of $E$ and makes it entangled with $A$. We will assume that $E$ is in state $|0\rangle$ just before this interaction.

We need information about the unitary $U$ to derive and analyze this quantum channel. Note that $U$ acts on $AE$ (with a 4-dimensional Hilbert space). The state space of $AE$ has computational basis

$$|0\rangle_A \otimes |0\rangle_E, |0\rangle_A \otimes |1\rangle_E, |1\rangle_A \otimes |0\rangle_E, |1\rangle_A \otimes |1\rangle_E.$$

Thus, the four columns and four rows of $U$ are indexed as $00, \ldots, 11$. To describe the unitary $U$ completely we need to know all the four columns of $U$: $U|00\rangle, \ldots, U|11\rangle$. But, in our setting we only need to know about two columns of $U$: $U|00\rangle$ and $U|10\rangle$ since the state of $E$ is promised to be $|0\rangle$ at the end of state preparation. We will denote the $4 \times 2$ matrix consisting of these two columns of $U$ as $V$,

$$V := \begin{bmatrix} U|00\rangle_{AE} & U|10\rangle_{AE} \end{bmatrix}.$$

The 'partial unitary' $V$ is described as follows. The interaction acts on the computational basis of $AE$ as

$$\begin{aligned} |0\rangle_A \otimes |0\rangle_E &\mapsto |0\rangle_A \otimes \big(\cos\theta|0\rangle + \sin\theta|1\rangle\big)_E, \\ |1\rangle_A \otimes |0\rangle_E &\mapsto |1\rangle_A \otimes \big(\cos\theta|0\rangle - \sin\theta|1\rangle\big)_E, \end{aligned}$$

where $\theta$ is a parameter that characterizes the dephasing channel. Note that this is how $A$ and $E$ interact when $A$ is initialized to one of the two possible classical states ('bits'). If $A$ is initialized to an arbitrary pure state, then using the linearity of $U$ (or $V$) we will see a superposition of these two output states.

Note that *if* $A$ is in the computational basis state $|0\rangle$ or $|1\rangle$, it continues to stay in the same state even after the interaction. In such cases, the state of $E$ after interaction depends on what the classical state of $A$ is. Thus, some information about the state of $A$ has leaked into the environment $E$. *Caution:* in general, the state of $A$ *does indeed change* because of the interaction with $E$; this happens whenever $A$ is in a superposition state.

**Action on a general qubit state.** If $A$ is initialized to a pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, write

$$|\varphi_1\rangle := \cos\theta|0\rangle + \sin\theta|1\rangle \text{ and } |\varphi_2\rangle := \cos\theta|0\rangle - \sin\theta|1\rangle$$

for the two states appearing above. By linearity the unitary interaction produces the state

$$\begin{aligned} U(|\psi\rangle_A \otimes |0\rangle_E) &= U(\alpha|0\rangle_A \otimes |0\rangle_E + \beta|1\rangle_A \otimes |0\rangle_E) \\ &= \alpha|0\rangle_A \otimes |\varphi_1\rangle_E + \beta|1\rangle_A \otimes |\varphi_2\rangle_E. \end{aligned}$$

The density operator of $AE$ is

$$\begin{aligned} &\alpha\alpha^*|0\rangle\langle 0| \otimes |\varphi_1\rangle\langle\varphi_1| + \beta\beta^*|1\rangle\langle 1| \otimes |\varphi_2\rangle\langle\varphi_2| \\ &+ \alpha\beta^*|0\rangle\langle 1| \otimes |\varphi_1\rangle\langle\varphi_2| + \alpha^*\beta|1\rangle\langle 0| \otimes |\varphi_2\rangle\langle\varphi_1|. \end{aligned}$$

Since $\theta$ is real, $|\varphi_1\rangle, |\varphi_2\rangle$ are unit vectors with $\langle\varphi_1 \,|\, \varphi_1\rangle = \langle\varphi_2 \,|\, \varphi_2\rangle = 1$ and $\langle\varphi_1 \,|\, \varphi_2\rangle = \langle\varphi_2 \,|\, \varphi_1\rangle = \cos^2\theta - \sin^2\theta = \cos 2\theta$. Tracing out $E$ (using $\mathrm{Tr}_E[\,\cdot \otimes |a\rangle\langle b|\,] = \langle b \,|\, a\rangle\,(\cdot)$) gives

$$\mathcal{E}(|\psi\rangle\langle\psi|) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| + \cos 2\theta\big(\alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0|\big),$$

that is, in matrix form,

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \begin{bmatrix} |\alpha|^2 & \alpha\beta^*\cos 2\theta \\ \alpha^*\beta\cos 2\theta & |\beta|^2 \end{bmatrix}.$$

This is to be compared with the original density matrix,

$$|\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}.$$

The dephasing channel leaves the diagonal entries unchanged and scales the off-diagonal entries by $\cos 2\theta$.

REMARK. *At $\theta = \pi/4$, $\cos 2\theta = 0$, so $\mathcal{E}(|\psi\rangle\langle\psi|) = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$, the* completely dephasing channel. *This is identical to measuring $|\psi\rangle$ on the computational basis and ignoring the measurement outcome (Lecture 13, §13.1, measurement without classical control): the off-diagonal entries are zeroed-out entirely, leaving only the diagonal values as such.*

REMARK. *For any state $|\psi\rangle$, the following measurements yield the same statistical outcomes*

- *measurement on $|\psi\rangle$ in the computational basis,*
- *measurement on $\mathcal{E}(|\psi\rangle\langle\psi|)$ in the computational basis.*

*Note that this does not imply that $|\psi\rangle$ and $\mathcal{E}(|\psi\rangle\langle\psi|)$ are the same states. They are evidently different for any $\cos 2\theta \neq 1$. There exist projective measurements that give distinct statistical outcomes for these two states, but measurement in computational basis is not one such measurement.*

**Kraus form of the dephasing channel.** Since $|\zeta\rangle := U(|\psi\rangle_A \otimes |0\rangle_E) \in \mathbb{C}^4$ depends linearly on $|\psi\rangle \in \mathbb{C}^2$, we may write $|\zeta\rangle = V|\psi\rangle$ for some $V \in \mathbb{C}^{4\times 2}$, where the columns of $V$ are the images of the computational basis: $V|0\rangle = U(|0\rangle_A \otimes |0\rangle_E)$ and $V|1\rangle = U(|1\rangle_A \otimes |0\rangle_E)$. Ordering the computational basis of $AE$ as $|00\rangle, |01\rangle, |10\rangle, |11\rangle$,

$$V|0\rangle = \cos\theta|00\rangle + \sin\theta|01\rangle, \qquad V|1\rangle = \cos\theta|10\rangle - \sin\theta|11\rangle,$$

so that, with $c := \cos\theta$ and $s := \sin\theta$,

$$V = \begin{bmatrix} c & 0 \\ s & 0 \\ 0 & c \\ 0 & -s \end{bmatrix}.$$

The state of $AE$ after the interaction is $|\zeta\rangle\langle\zeta| = V|\psi\rangle\langle\psi|V^\dagger$, and the state of $A$ alone (tracing out $E$) is

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_{j=0}^{1} (I \otimes \langle j|)\big(V|\psi\rangle\langle\psi|V^\dagger\big)(I \otimes |j\rangle) = \sum_{j=0}^{1} K_j|\psi\rangle\langle\psi|K_j^\dagger,$$

where the Kraus operators are

$$K_j := (I \otimes \langle j|)\, V.$$

Computing $K_0$ and $K_1$ directly from the block form of $V$ above (selecting, respectively, the rows of $V$ paired with $|0\rangle_E$ and with $|1\rangle_E$):

$$K_0 = (I \otimes \langle 0|)V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ s & 0 \\ 0 & c \\ 0 & -s \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix},$$

$$K_1 = (I \otimes \langle 1|)V = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c & 0 \\ s & 0 \\ 0 & c \\ 0 & -s \end{bmatrix} = \begin{bmatrix} s & 0 \\ 0 & -s \end{bmatrix}.$$

That is,

$$K_0 = c\, I, \qquad K_1 = s\, Z.$$

As a check, completeness holds:

$$K_0^\dagger K_0 + K_1^\dagger K_1 = c^2 I + s^2 Z^\dagger Z = (c^2 + s^2) I = I,$$

using $Z^2 = I$. The dephasing channel therefore has the compact two-Kraus-operator form

$$\mathcal{E}(\rho) = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger = \cos^2\theta\, \rho + \sin^2\theta\, Z\rho Z.$$

Thus, the dephasing channel creates the ensemble

$$|\psi\rangle \mapsto \left\{ \left(c^2, |\psi\rangle\right),\ \left(s^2, Z|\psi\rangle\right) \right\}.$$

That is, the dephasing channel applies the phase-flip operator (phase-flip error) $Z$ with probability $s^2$ and leaves the qubit as it is with probability $c^2$.

## §16.4. Amplitude-damping channel

In this setting $A$ denotes a qubit realized through the energy levels of an atom. The two classical states of $A$ are the ground state $|0\rangle$ and the excited state $|1\rangle$. The environment $E$ is simply a count of photons interacting with the atom. We start with no photons, i.e., $|0\rangle$ on register $E$, and we might see one photon $|1\rangle_E$ if an excited atom classically decays to its ground state by emitting a single photon.

Now, the interaction unitary acts on the computational basis of $AE$ as follows,

$$\begin{aligned} |0\rangle_A \otimes |0\rangle_E &\mapsto |0\rangle_A \otimes |0\rangle_E, \\ |1\rangle_A \otimes |0\rangle_E &\mapsto \sqrt{\gamma}\,|0\rangle_A \otimes |1\rangle_E + \sqrt{1-\gamma}\,|1\rangle_A \otimes |0\rangle_E, \end{aligned} \qquad \gamma \in [0,1].$$

Note that if the system starts in the state $|1\rangle_A \otimes |0\rangle_E$ and only classical states and transitions are allowed, then we might see only the following two classical outcomes

- the atom continues to stay excited while releasing no photon: $|1\rangle_A \otimes |0\rangle_E$, or
- the atom emits a single photon and reaches the ground state: $|0\rangle_A \otimes |1\rangle_E$.

In the case of the amplitude-damping channel, the excited atom $|1\rangle_A$ quantumly decays into a superposition of the above two classical possibilities. Since the change from $|1\rangle_A$ to $|0\rangle_A$ is accompanied by the emission of a photon we arrive at the entangled state

$$\sqrt{\gamma}\,|0\rangle_A \otimes |1\rangle_E + \sqrt{1-\gamma}\,|1\rangle_A \otimes |0\rangle_E.$$

The derivation of the Kraus form was left as homework. I am including the derivation in the appendix for your reference.

## §16.5. Appendix

**Invertible channels.** A quantum channel $\mathcal{E}$ is said to be *invertible* if there exists a function/map (not necessarily a CPTP map) $\mathcal{F}$ such that $\mathcal{F} \circ \mathcal{E} = \mathbb{I}$. In this case $\mathcal{F}$ is simply the mathematical inverse of $\mathcal{E}$ and $\mathcal{F}$ need not be physically realizable.

As an example, consider the quantum channel acting on qubits

$$\mathcal{E}(\rho) = \frac{1}{2}\rho + \frac{1}{4} I_{2\times 2}.$$

That is, $\mathcal{E}$ returns $\rho$ or $I/2$ with equal probabilities. This is a valid physical operation and has a Kraus form. But this is not a reversible operation since it can not be effected using a single unitary gate.

However, as a map $\mathcal{E}$ has an inverse, observe that

$$\rho = 2\mathcal{E}(\rho) - \frac{1}{2} I_{2\times 2}.$$

The RHS above, i.e., the map

$$\sigma \mapsto 2\sigma - \frac{1}{2} I_{2\times 2}$$

is not a CPTP map; it is not physically realizable. Thus, $\mathcal{E}$ is invertible but not reversible. A quantum computer or circuit can not undo the application of $\mathcal{E}$.

Note that every reversible channel is invertible. As the example above shows, some invertible channels are not reversible.

**Kraus form of amplitude damping channel.** Since $|\zeta\rangle := U(|\psi\rangle_A \otimes |0\rangle_E) \in \mathbb{C}^4$ depends linearly on $|\psi\rangle \in \mathbb{C}^2$, we may write $|\zeta\rangle = V|\psi\rangle$ for some $V \in \mathbb{C}^{4\times 2}$, where the columns of $V$ are the images of the computational basis:

$$V|0\rangle = U(|0\rangle_A \otimes |0\rangle_E) \text{ and } V|1\rangle = U(|1\rangle_A \otimes |0\rangle_E).$$

Ordering the computational basis of $AE$ as $|00\rangle, |01\rangle, |10\rangle, |11\rangle$,

$$V|0\rangle = |00\rangle, \qquad V|1\rangle = \sqrt{\gamma}\,|01\rangle + \sqrt{1-\gamma}\,|10\rangle,$$

so that, with $g := \sqrt{\gamma}$ and $h := \sqrt{1-\gamma}$,

$$V = \begin{bmatrix} 1 & 0 \\ 0 & g \\ 0 & h \\ 0 & 0 \end{bmatrix}.$$

The state of $AE$ after the interaction is $|\zeta\rangle\langle\zeta| = V|\psi\rangle\langle\psi|V^\dagger$, and the state of $A$ alone (tracing out $E$) is

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_{j=0}^{1} (I \otimes \langle j|)\big(V|\psi\rangle\langle\psi|V^\dagger\big)(I \otimes |j\rangle) = \sum_{j=0}^{1} K_j |\psi\rangle\langle\psi| K_j^\dagger,$$

where the Kraus operators are

$$K_j := (I \otimes \langle j|)\, V.$$

Computing $K_0$ and $K_1$ directly from the block form of $V$ above (selecting, respectively, the rows of $V$ paired with $|0\rangle_E$ and with $|1\rangle_E$):

$$K_0 = (I \otimes \langle 0|)V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & g \\ 0 & h \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & h \end{bmatrix},$$

$$K_1 = (I \otimes \langle 1|)V = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & g \\ 0 & h \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix}.$$

As a check, completeness holds:

$$K_0^\dagger K_0 + K_1^\dagger K_1 = \begin{bmatrix} 1 & 0 \\ 0 & h^2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & g^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & g^2 + h^2 \end{bmatrix} = I,$$

using $g^2 + h^2 = \gamma + (1-\gamma) = 1$. The amplitude-damping channel therefore has the Kraus form

$$\mathcal{E}(\rho) = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger,$$

with Kraus operators

$$K_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad K_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}.$$

**Density operator (matrix) form of the amplitude-damping channel.** Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, so that $\rho := |\psi\rangle\langle\psi|$ has matrix form

$$\rho = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}.$$

Applying the Kraus form $\mathcal{E}(\rho) = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger$ found above, we compute each term separately. First,

$$K_0\rho K_0^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix},$$

which gives

$$K_0\rho K_0^\dagger = \begin{bmatrix} |\alpha|^2 & \sqrt{1-\gamma}\,\alpha\beta^* \\ \sqrt{1-\gamma}\,\alpha^*\beta & (1-\gamma)|\beta|^2 \end{bmatrix}.$$

Next,

$$K_1\rho K_1^\dagger = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix},$$

which gives

$$K_1\rho K_1^\dagger = \begin{bmatrix} \gamma|\beta|^2 & 0 \\ 0 & 0 \end{bmatrix}.$$

Adding the two terms, the amplitude-damping channel has the density operator (matrix) form

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \begin{bmatrix} |\alpha|^2 + \gamma|\beta|^2 & \sqrt{1-\gamma}\,\alpha\beta^* \\ \sqrt{1-\gamma}\,\alpha^*\beta & (1-\gamma)|\beta|^2 \end{bmatrix}.$$

As a check, the trace of this matrix is

$$\left(|\alpha|^2 + \gamma|\beta|^2\right) + (1-\gamma)|\beta|^2 = |\alpha|^2 + |\beta|^2 = 1,$$

as required of a valid density operator.

For $\rho = |\psi\rangle\langle\psi|$ compare $\rho$ with $\mathcal{E}(\rho)$. The two off-diagonal terms are scaled by the same constant (similar to phase-damping channel where the constant was $\cos 2\theta$). But the diagonal terms are also changed (this is unlike phase-damping); some fraction of the value of the $|1\rangle\langle 1|$ term is moved to the $|0\rangle\langle 0|$ term, and this corresponds to the decay of the excited atom to its ground state.

**Ensemble at the amplitude-damping channel's output.** Unlike the dephasing channel's $K_0, K_1$, neither Kraus operator here is proportional to a unitary except in the trivial case $\gamma = 0$ ($K_1^\dagger K_1 = \mathrm{diag}(0,\gamma)$ is a multiple of $I$ — namely the zero matrix — only when $\gamma = 0$; at $\gamma = 1$ it equals $\mathrm{diag}(0,1)$, which is not a multiple of $I$ either). Note that for $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we have

$$\begin{aligned} K_0|\psi\rangle &= \alpha|0\rangle + \sqrt{1-\gamma}\,\beta|1\rangle \\ K_1|\psi\rangle &= \sqrt{\gamma}\,\beta|0\rangle, \end{aligned}$$

so that $\mathcal{E}$ acting on $|\psi\rangle\langle\psi|$ produces the ensemble of pure states

$$\left\{ \left( |\alpha|^2 + (1-\gamma)|\beta|^2,\ \frac{\alpha|0\rangle + \sqrt{1-\gamma}\,\beta|1\rangle}{\sqrt{|\alpha|^2 + (1-\gamma)|\beta|^2}} \right),\ \left( \gamma|\beta|^2,\ |0\rangle \right) \right\}.$$

# *Homework 8*

1. **Local operations and reduced states.** Consider an arbitrary state $\rho_{AB}$ on the composite register $AB$, where the state spaces of $A$ and $B$ are $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, respectively. Let

$$\mathcal{E} : \mathbb{C}^{d_2 \times d_2} \to \mathbb{C}^{d_2 \times d_2}$$

be an arbitrary quantum channel. You need to show that the reduced state of $A$ (obtained by tracing out $B$) is the same irrespective of whether or not $\mathcal{E}$ is applied locally on $B$, i.e., you must show that

$$\mathrm{Tr}_B(\rho_{AB}) = \mathrm{Tr}_B\left(\mathbb{I} \otimes \mathcal{E}\left(\rho_{AB}\right)\right).$$

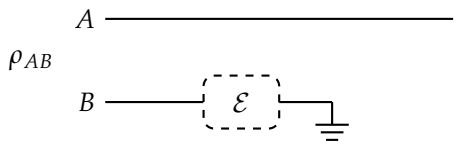



*Figure.* Register $A$ is left untouched; register $B$ is discarded, optionally after a local channel $\mathcal{E}$ is applied to it (dashed box). You must show that the resulting state of $A$ is the same whether or not $\mathcal{E}$ is applied to $B$ before discarding it.

HINT. Write $\rho_{AB}$ as a linear combination of Kronecker products.

REMARK. As long as we are only concerned about the state of $A$ what happens to register $B$ is immaterial to us. This is true in the classical case too: if random variables $X, Y$ have a joint distribution, the marginal distribution of $X$ is the same whether or not some function $f$ is applied on $Y$.

REMARK. We will use this now to arrive at an interpretation of quantum channels.

2. **An interpretation of quantum channels.** Let $\mathcal{E} : \mathbb{C}^{d \times d} \to \mathbb{C}^{d \times d}$ be a quantum channel with

$$\mathcal{E}(\rho) = \sum_{j=0}^{r-1} E_j \rho E_j^\dagger.$$

The Stinespring representation of this channel uses an environment register with state space of dimension $r$ or more, and uses the unitary

$$|\psi\rangle_A \otimes |0\rangle_E \to \sum_{j=0}^{r-1} E_j|\psi\rangle \otimes |j\rangle.$$

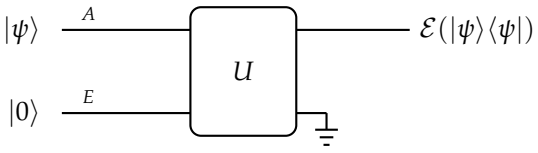



*Figure.* The Stinespring representation of $\mathcal{E}$: append an environment register $E$ prepared in $|0\rangle\langle 0|$, apply a single unitary $U$ on $AE$, and discard $E$.

Note that the register $E$ is discarded after the unitary operation $U$.

(a) What happens to the state of register $A$ if a measurement is performed on $E$ in its computational basis right after the unitary (before tracing out), and the measurement outcome is known to the experimenter?

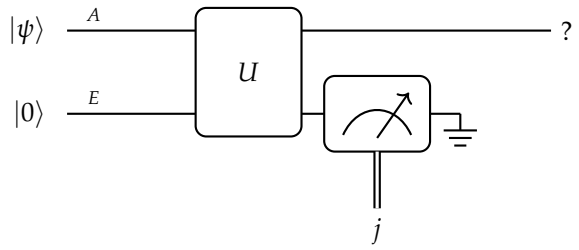



*Figure.* The same circuit as before, except $E$ is now measured in the computational basis right after $U$ (instead of being discarded), producing a classical outcome $j$ that the experimenter observes. What is the state of $A$, given $j$?

(b) What is the state of $A$ if the measurement outcome $j$ is not accessible to the experimenter? That is, the register $E$ is measured in the computational basis and the outcome is lost/forgotten.

REMARK. The channel $|\psi\rangle\langle\psi| \mapsto \sum_j E_j|\psi\rangle\langle\psi|E_j^\dagger$ can be interpreted as one of the Kraus operators being 'applied' to the state $|\psi\rangle$ producing

$$\frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|} \text{ with probability } p_j = \|E_j|\psi\rangle\|^2.$$

The environment $E$ knows which operator $E_j$ was 'applied'. Since $E$ is inaccessible to us, we end up experiencing an ensemble

$$\left\{ p_j, \frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|} \right\}_j \text{ instead of a pure state } \frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|}.$$

This is one interpretation of a quantum channel.

3. **Unitary freedom in purification.** Let $\rho$ be any state of register $A$, and let $R$ be a reference system such that the pure state $|\psi\rangle_{AR}$ on $AR$ reduces to state $\rho$ if we trace out $R$.

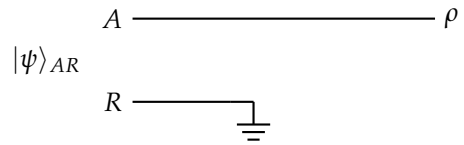



*Figure.* The pure state $|\psi\rangle_{AR}$ on the joint system $AR$; discarding (tracing out) the reference system $R$ leaves register $A$ in the mixed state $\rho$. The state $|\psi\rangle_{AR}$ is called a *purification* of $\rho$.

*Question.* What is the state of $A$ if a unitary $U$ is applied locally to $R$ before tracing it out?

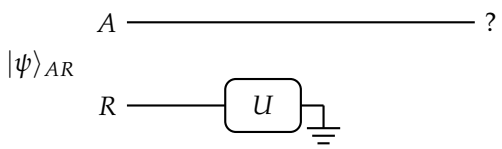


*Figure.* The same purification $|\psi\rangle_{AR}$, except a unitary $U$ acting only on $R$ is applied before $R$ is discarded.

REMARK. This shows that $|\psi\rangle_{AR}$ and $I_A \otimes U_R|\psi\rangle_{AR}$ are both valid purifications of $\rho$. In fact (we did not prove this), these are the only possible purifications of $\rho$, that is: $|\psi\rangle$ and $|\varphi\rangle$ are both purifications of $\rho$ *if and only if* there exists a unitary $U$ such that

$$|\varphi\rangle = I_A \otimes U_R|\psi\rangle.$$

4. **Ensemble interpretation of quantum channels.** We know that a quantum channel $\mathcal{E}$ can be interpreted as a process that produces an ensemble

$$\frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|} \text{ with probability } p_j = \|E_j|\psi\rangle\|^2$$

when the input state is $|\psi\rangle$. Here $\{E_j\}$ are Kraus operators of $\mathcal{E}$. However, the Kraus form of $\mathcal{E}$ is not unique. Suppose $\{K_i\}$ is another set of Kraus operators of $\mathcal{E}$, then we can interpret $\mathcal{E}$ as a process that creates the ensemble

$$\frac{K_i|\psi\rangle}{\|K_i|\psi\rangle\|} \text{ with probability } q_i = \|K_i|\psi\rangle\|^2.$$

So, now we have two interpretations of the same channel $\mathcal{E}$. Do these two interpretations contradict each other? Why or why not?

5. **Commutativity of quantum channels.**

   (a) You must prove or disprove this statement: any two quantum channels commute. That is, if $\mathcal{E}$ and $\mathcal{F}$ are quantum channels, then

   $$\mathcal{E} \circ \mathcal{F} = \mathcal{F} \circ \mathcal{E}.$$

   (b) Do the phase-damping channel and the amplitude-damping channel commute?

6. **Generalized amplitude-damping channel.** We will consider the setting of amplitude damping, and generalize it to the case where the environment (photon) need not be in state $|0\rangle$ before the interaction. We will first consider the case $|1\rangle$ in register $E$ (which is a reversal of amplitude damping) and then consider a mixture $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$ on $E$. Such a mixture is the practically more relevant model.

   (a) *A reversal of amplitude damping.* Assume that $E$ (photon) starts in $|1\rangle$. The unitary interaction with input register $A$ (atom) is as follows

   $$|1\rangle_A \otimes |1\rangle_E \mapsto |1\rangle_A \otimes |1\rangle_E$$
   $$|0\rangle_A \otimes |1\rangle_E \mapsto \sqrt{\gamma}|1\rangle_A \otimes |0\rangle_E + \sqrt{1-\gamma}|0\rangle_A \otimes |1\rangle_E$$

   Find the Kraus form for this channel.

   (b) *Generalized amplitude damping.* Now suppose that $E$ starts in a mixed state $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$. Find the Kraus form for the resulting channel.

7. **Thermal relaxation error.** This is one of the quantum noise models used in IBM's quantum computing software Qiskit and is practically relevant. If a qubit is prepared at time 0 and is made to wait for some time $t$ then thermal relaxation is the channel used to model the quantum noise experienced by this qubit over time $t$.

This channel is the composition of the phase-damping and generalized-amplitude-damping channels. However, we will consider the special case $p = 1$ for generalized amplitude damping, that is, simply a combination of the phase-damping and amplitude-damping channels.

*Background.* A qubit $A$ prepared in state $\alpha|0\rangle + \beta|1\rangle$ at time 0 interacts with the environment as it is made to 'wait' for a prescribed amount of time $t > 0$. The parameters of the unitary interaction with the environment depend on this wait time $t$ as follows.

For phase damping, the parameter $\theta$ is given by

$$\cos 2\theta = \exp(-t/T_\phi),$$

where the constant $T_\phi$ is called the *pure dephasing time*. This constant characterizes the interaction between qubit $A$ and the dephasing environment.

For the amplitude damping channel, the parameter $\gamma$ is related to time $t$ as

$$\gamma = 1 - \exp(-t/T_1)$$

where the system constant $T_1$ is known as the *energy relaxation time*.

(a) The *thermal relaxation error channel* $\mathcal{E}$ is the composition of the dephasing channel with parameter $T_\phi$ and the amplitude-damping channel with parameter $T_1$. If the state of register $A$ at time 0 is $\alpha|0\rangle + \beta|1\rangle$, find the density operator of $A$ at time $t$, under thermal relaxation error, in terms of $\alpha, \beta, T_1, T_\phi$.

(b) Spend some time inspecting the structure of $\mathcal{E}(|\psi\rangle\langle\psi|)$. You will notice that:

- as time $t$ increases the off-diagonal terms decay at the same rate.
- a fraction of the value in the lower-right entry of the matrix is transferred to the upper-left entry of the matrix.

We now define another parameter of the channel $\mathcal{E}$ denoted as $T_2$ and called the *coherence time*. We define $T_2$ to be the constant such that at time $t > 0$ the off-diagonal terms decay by a factor of $\exp(-t/T_2)$, i.e., the off-diagonal terms change as

$$\alpha^*\beta \mapsto \exp(-t/T_2)\alpha^*\beta, \text{ and } \alpha\beta^* \mapsto \exp(-t/T_2)\alpha\beta^*.$$

What is the relation between $T_1, T_2, T_\phi$?

REMARK. Typically, the thermal relaxation noise channel is specified in terms of $T_1, T_2$ instead of $T_1, T_\phi$.

(c) What is the state of register $A$ as $t \to \infty$?

8. **Invertible versus reversible channels.** Prove that the qubit channel ($d_1 = d_2 = 2$)

$$\rho \mapsto \frac{1}{2}\rho + \frac{1}{4}I_{2\times 2}$$

is invertible but not reversible. That is, you must prove that its inverse map is not a quantum channel.

# *Lecture 17*

These notes are based on Chapter 3 of John Preskill's lecture notes for *Ph 219/CS 219* and Chapter 1 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*.

We first see two more examples of qubit quantum channels. We then see the first example of a quantum error correcting code.

## §17.1. Quantum channel examples

We saw two examples of qubit channels in the previous lecture: dephasing and amplitude-damping channels. Their composition is called the *thermal relaxation error* channel. Thermal relaxation is a practically relevant noise model, and is used in IBM Qiskit. One of the questions in Homework 8 is about thermal relaxation error channel.

**The depolarizing channel.** This channel is highly symmetric and structured, and is often used by theoreticians to analyze the performance of a quantum error correcting code. The depolarizing channel $\mathcal{E} : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}$ is characterized by a single parameter $p \in [0, 1]$:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3} X\rho X + \frac{p}{3} Y\rho Y + \frac{p}{3} Z\rho Z.$$

The above expression uses the fact that if $A$ is a Pauli matrix, i.e., if $A \in \{I, X, Y, Z\}$ then $A = A^\dagger$.

The depolarizing channel can be realized using the following experiment. We generate a classical random variable that takes values $0, 1, 2, 3$ with probabilities $1-p, p/3, p/3, p/3$, respectively. We apply the unitary gate $I$ if the random variable takes the value 0, we apply gate $X$ if the value of the random variable is 1, etc. Note that (as with any non-trivial channel) this is not the only way by which a depolarization channel can be physically realized.

The above expression for $\mathcal{E}$ immediately leads to the Kraus form with four Kraus operators

$$K_0 = \sqrt{1-p}I, K_1 = \sqrt{\frac{p}{3}}X, K_2 = \sqrt{\frac{p}{3}}Y, K_3 = \sqrt{\frac{p}{3}}Z.$$

We can rewrite the depolarization expression in another way. This requires the following result (which was stated but not proved during the lecture).

**CLAIM.** *For every qubit state $\rho \in \mathcal{D}(\mathbb{C}^2)$,*

$$\frac{1}{4}\rho + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z = \frac{1}{2}I.$$

*Proof.* Write $\rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, so that $a + d = \mathrm{Tr}\rho = 1$. Direct computation with the Pauli matrices gives

$$X\rho X = \begin{bmatrix} d & c \\ b & a \end{bmatrix}, \qquad Y\rho Y = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}, \qquad Z\rho Z = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}.$$

Adding these three matrices to $\rho$ itself, the off-diagonal entries cancel in pairs ($b + c - c - b = 0$, and symmetrically $c + b - b - c = 0$ in the $(2,1)$ entry), while each diagonal entry is counted four times:

$$\rho + X\rho X + Y\rho Y + Z\rho Z = \begin{bmatrix} 2(a+d) & 0 \\ 0 & 2(a+d) \end{bmatrix} = 2(a+d)\, I = 2I,$$

using $a + d = 1$. Dividing by 4 gives the claim. ∎

Using this fact, the depolarizing channel simplifies to a closed form that does not mention $X, Y, Z$ explicitly. Adding and subtracting $\frac{p}{3}\rho$,

$$\mathcal{E}(\rho) = \Big(1 - \frac{4p}{3}\Big)\rho + \frac{p}{3}(\rho + X\rho X + Y\rho Y + Z\rho Z) = \Big(1 - \frac{4p}{3}\Big)\rho + \frac{p}{3} \cdot 4 \cdot \Big(\frac{1}{2}I\Big),$$

that is,

$$\mathcal{E}(\rho) = \Big(1 - \frac{4p}{3}\Big)\rho + \frac{4p}{3}\,\frac{1}{2}I.$$

When $4p/3 \leq 1$, this expression gives us another method to realize the depolarization channel. An experimenter generates a binary random variable with probability of 0 being $1 - 4p/3$ and probability of 1 being $4p/3$. The experimenter has access to qubit $B$ that is initialized in the maximally mixed state $I/2$. Given an input register $A$ with state $\rho$, the experimenter does the following: he generates one instance of the classical random variable, if the random variable takes the value 0 he simply returns the register $A$, else he returns the register $B$.

**The qubit erasure (photon-loss) channel.** Suppose a qubit is physically realized by the polarization of a single photon: $|0\rangle \mapsto$ horizontal polarization, $|1\rangle \mapsto$ vertical polarization. In transit from sender to receiver, there is a possibility that the photon is absorbed or otherwise lost to the environment. Assume that the polarization state of the photon is unaffected if the photon itself is not lost.

At the sender's end we have two distinct classical states: horizontal and vertical polarizations. At the receiver we have three classical states: horizontal polarization, vertical polarization and 'no photon'. Recall that in quantum formalism the dimension of the state space equals the number of possible classical states of the system. Each classical state is assigned a standard basis vector from the state space.

Thus, at the sender the system state space is $\mathbb{C}^2$ and the classical states are:

$$\text{photon is in horizontal polarization} \mapsto \begin{bmatrix}1\\0\end{bmatrix} =: |0\rangle$$

$$\text{photon is in vertical polarization} \mapsto \begin{bmatrix}0\\1\end{bmatrix} =: |1\rangle$$

Similarly, on the receiving end there are *three* possible classical states, which we take as an orthonormal basis of $\mathbb{C}^3$:

$$\text{photon present, horizontally polarized} \mapsto \begin{bmatrix}1\\0\\0\end{bmatrix} =: |0\rangle,$$

$$\text{photon present, vertically polarized} \mapsto \begin{bmatrix}0\\1\\0\end{bmatrix} =: |1\rangle,$$

$$\text{photon lost} \mapsto \begin{bmatrix}0\\0\\1\end{bmatrix} =: |2\rangle.$$

The channel therefore maps $\mathcal{E} : \mathbb{C}^{2\times 2} \to \mathbb{C}^{3\times 3}$. We define the operator $A : \mathbb{C}^2 \to \mathbb{C}^3$,

$$A := \begin{bmatrix}1 & 0\\0 & 1\\0 & 0\end{bmatrix},$$

which embeds a qubit state as the first two coordinates of $\mathbb{C}^3$, that is $A|0\rangle = |0\rangle$, $A|1\rangle = |1\rangle$. If the photon is *not* lost, its polarization state is transmitted faithfully: $|\psi\rangle \mapsto A|\psi\rangle$, i.e.,

$$|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha\\ \beta\\ 0\end{bmatrix} = A|\psi\rangle.$$

If the photon *is* lost, the output is deterministically the classical state $|2\rangle$, regardless of $|\psi\rangle$: $|\psi\rangle \mapsto |2\rangle$ (a lost photon carries no information about its polarization).

Suppose the probability of photon loss is $p$. Then, on a general qubit state $\rho$,

$$\mathcal{E}(\rho) = (1-p)\, A\rho A^\dagger + p\, |2\rangle\langle 2|.$$

REMARK. *This expression is* not *a Kraus form: the second term $p|2\rangle\langle 2|$ is a fixed operator, not of the form $K\rho K^\dagger$ for a single fixed $K$ acting on $\rho$ by conjugation.*

A valid Kraus form for this channel consists of the following three Kraus operators

$$K_0 = \sqrt{1-p}\, A, \qquad K_1 = \sqrt{p}\, |2\rangle\langle 0| = \sqrt{p} \begin{bmatrix}0&0\\0&0\\1&0\end{bmatrix}, \qquad K_2 = \sqrt{p}\, |2\rangle\langle 1| = \sqrt{p} \begin{bmatrix}0&0\\0&0\\0&1\end{bmatrix}.$$

As a check, completeness holds:

$$K_0^\dagger K_0 + K_1^\dagger K_1 + K_2^\dagger K_2 = (1-p)A^\dagger A + p\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) = (1-p)I + pI = I,$$

using that $A^\dagger A = I_2$. It is also easy to check that $\sum_i K_i \rho K_i^\dagger = (1-p)A\rho A^\dagger + p|2\rangle\langle 2|$: the $K_0$ term reproduces $(1-p)A\rho A^\dagger$ immediately, while $K_1, K_2$ contribute

$$K_1\rho K_1^\dagger + K_2 \rho K_2^\dagger = p\, |2\rangle\langle 0|\, \rho\, |0\rangle\langle 2| + p\, |2\rangle\langle 1|\, \rho\, |1\rangle\langle 2| = p\big(\langle 0|\rho|0\rangle + \langle 1|\rho|1\rangle\big)|2\rangle\langle 2|,$$

since $\langle 0|\rho|0\rangle$ and $\langle 1|\rho|1\rangle$ are scalars, so each pulls out in front of $|2\rangle\langle 2|$. The bracketed sum is exactly $\mathrm{Tr}\rho$, which equals 1 for a state $\rho$, so $K_1\rho K_1^\dagger + K_2\rho K_2^\dagger = p|2\rangle\langle 2|$, and altogether $\sum_i K_i\rho K_i^\dagger = (1-p)A\rho A^\dagger + p|2\rangle\langle 2|$, as claimed.

This channel is called the *photon-loss channel* and is an example of a *qubit erasure channel*: with probability $p$ it flags the loss unambiguously via the outcome $|2\rangle$, which is orthogonal to both $|0\rangle$ and $|1\rangle$ — so the receiver always knows *whether* an erasure occurred, even without knowing what the transmitted state would have been.

## §17.2. An example of quantum error correction

**Setting.** Suppose we have access to three qubits, forming a single register $A$ with state space $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^8$. Its classical (computational) basis states $|000\rangle, \ldots, |111\rangle$ are the eight standard basis vectors of $\mathbb{C}^8$.

Consider the channel $\mathcal{E} : \mathbb{C}^{8\times 8} \to \mathbb{C}^{8\times 8}$,

$$\begin{aligned}\mathcal{E}(\rho) = {} & p_0\, (I\otimes I\otimes I)\,\rho\,(I\otimes I\otimes I)^\dagger + p_1\,(Z\otimes I\otimes I)\,\rho\,(Z\otimes I\otimes I)^\dagger \\ & + p_2\,(I\otimes Z\otimes I)\,\rho\,(I\otimes Z\otimes I)^\dagger + p_3\,(I\otimes I\otimes Z)\,\rho\,(I\otimes I\otimes Z)^\dagger,\end{aligned}$$

where $p_0, p_1, p_2, p_3 \geq 0$ and $\sum_i p_i = 1$. That is, independently of the register's state, exactly one of four things happens: with probability $p_0$ nothing happens; with probability $p_1$ (respectively $p_2$, $p_3$) a phase-flip error $Z$ strikes the first (respectively second, third) qubit, leaving the other two untouched.

Each of the four operators $I\otimes I\otimes I$, $Z\otimes I\otimes I$, $I\otimes Z\otimes I$, $I\otimes I\otimes Z$ is unitary, being a tensor product of unitaries. So $\mathcal{E}$ has Kraus operators $\sqrt{p_i}\,U_i$ with each $U_i$ unitary, and completeness holds automatically:

$$\sum_{i=0}^{3} \big(\sqrt{p_i}\,U_i\big)^\dagger \big(\sqrt{p_i}\,U_i\big) = \sum_{i=0}^{3} p_i\, U_i^\dagger U_i = \sum_{i=0}^{3} p_i\, I = I,$$

using $\sum_i p_i = 1$.

**The channel is not reversible.** Recall from Lecture 15 that a channel is reversible if and only if it acts by conjugation with a single unitary; such a channel necessarily maps every pure state to a pure state. Hence, to show $\mathcal{E}$ is *not* reversible, it suffices to exhibit one pure state whose image under $\mathcal{E}$ is not pure. That is,

there is at least one pure state $|\psi\rangle$ such that $\mathcal{E}(|\psi\rangle\langle\psi|)$ is mixed $\Rightarrow$ $\mathcal{E}$ is not reversible.

Recall the Hadamard basis $|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ of $\mathbb{C}^2$, an orthonormal basis with $\langle + | - \rangle = 0$. Since $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$,

$$Z|+\rangle = \frac{Z|0\rangle + Z|1\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle, \qquad Z|-\rangle = \frac{Z|0\rangle - Z|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle.$$

Take the pure state $|\psi\rangle = |+++\rangle \in \mathbb{C}^8$. Then

$$\begin{aligned}(Z \otimes I \otimes I)|+++\rangle &= |-++\rangle,\\ (I \otimes Z \otimes I)|+++\rangle &= |+-+\rangle,\\ (I \otimes I \otimes Z)|+++\rangle &= |++-\rangle,\end{aligned}$$

and hence,

$$\begin{aligned}\mathcal{E}(|+++\rangle\langle+++|) = \; & p_0|+++\rangle\langle+++|\\ & + p_1|-++\rangle\langle-++|\\ & + p_2|+-+\rangle\langle+-+|\\ & + p_3|++-\rangle\langle++-|.\end{aligned}$$

Since $\{|+\rangle, |-\rangle\}$ is an orthonormal basis of $\mathbb{C}^2$, the four kets $|+++\rangle$, $|-++\rangle$, $|+-+\rangle$, $|++-\rangle$ are mutually orthogonal unit vectors in $\mathbb{C}^8$. So the right-hand side above is already a spectral decomposition of $\mathcal{E}(|+++\rangle\langle+++|)$, with eigenvalues $p_0, p_1, p_2, p_3$. The rank is the number of non-zero $p_i$. This is a pure state only in the degenerate case where exactly one $p_i = 1$ and the rest vanish; whenever at least two of the $p_i$ are nonzero $\mathcal{E}(|+++\rangle\langle+++|)$ is a mixed state. Hence $\mathcal{E}$ is not reversible.

**Restricting to a subspace.** This means that if we allow *all* possible pure states of the register $A$ as inputs to $\mathcal{E}$, then, since $\mathcal{E}$ is not reversible, we cannot undo the effect of $\mathcal{E}$: once an error occurs, no quantum operation can recover the pre-error state with certainty for every possible input. But what if we restrict the possible inputs to a well-designed subspace of $\mathbb{C}^8$ instead? Can we undo the effect of $\mathcal{E}$ with the knowledge that $|\psi\rangle$ belongs to a specific subspace of $\mathbb{C}^8$?

In particular, suppose we allow only pure states of the form

$$|\psi\rangle = \alpha|+++\rangle + \beta|---\rangle, \qquad \alpha, \beta \in \mathbb{C}, \;\; |\alpha|^2 + |\beta|^2 = 1,$$

that is, we only ever prepare the register $A$ in a state belonging to the 2-dimensional subspace

$$S_0 := \text{span}\{|+++\rangle, |---\rangle\} \subset \mathbb{C}^8.$$

**The four possible outcomes lie in pairwise orthogonal subspaces.** If the operator $Z \otimes I \otimes I$ acts on $|\psi\rangle$, we have

$$(Z \otimes I \otimes I)|\psi\rangle = \alpha|-++\rangle + \beta|+--\rangle \;\in\; S_1 := \text{span}\{|-++\rangle, |+--\rangle\}.$$

If $I \otimes Z \otimes I$ acts on $|\psi\rangle$, then the output lies in the subspace spanned by $\{|+-+\rangle, |-+-\rangle\}$:

$$(I \otimes Z \otimes I)|\psi\rangle = \alpha|+-+\rangle + \beta|-+-\rangle \;\in\; S_2 := \text{span}\{|+-+\rangle, |-+-\rangle\}.$$

If $I \otimes I \otimes Z$ acts on $|\psi\rangle$, then the output lies in the subspace spanned by $\{|++-\rangle, |--+\rangle\}$:

$$(I \otimes I \otimes Z)|\psi\rangle = \alpha|++-\rangle + \beta|--+\rangle \;\in\; S_3 := \text{span}\{|++-\rangle, |--+\rangle\}.$$

**CLAIM.** *The subspaces $S_0, S_1, S_2, S_3 \subset \mathbb{C}^8$ are pairwise orthogonal.*

*Proof.* Since $\{|+\rangle, |-\rangle\}$ is an orthonormal basis of $\mathbb{C}^2$, the eight vectors $|s_1 s_2 s_3\rangle$, $s_1, s_2, s_3 \in \{+, -\}$, form an orthonormal basis of $\mathbb{C}^8 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Each $S_i$ ($i = 0, 1, 2, 3$) is spanned by exactly two of these eight orthonormal basis vectors, and the four pairs of sign patterns

$$\{+++, ---\}, \quad \{-++, +--\}, \quad \{+-+, -+-\}, \quad \{++-, --+\}$$

are disjoint and together exhaust all $2^3 = 8$ sign patterns. Hence any vector in $S_i$ is a linear combination of basis vectors none of which appears in the orthonormal basis expansion of any vector in $S_j$ for $j \neq i$, so $S_i \perp S_j$. ■

Pairwise orthogonality of $S_0, S_1, S_2, S_3$ is sufficient to correct these errors: a projective measurement with respect to the four orthogonal subspaces $\{S_0, S_1, S_2, S_3\}$ can determine which of the four events (no error / $Z$ on qubit 1 / qubit 2 / qubit 3) occurred without disturbing the state. That is, the post-measurement state and the pre-measurement state are identical and the classical outcome of the measurement tells us exactly which subspace the state lies in. Once we know the subspace, we know which one of the four unitary operator acted on the state $|\psi\rangle$. We can undo the effect of this unitary error by applying its inverse as a gate (controlled by the classical outcome of the measurement).

Thus error correction is indeed possible if the states are restricted to a good choice of subspace of the ambient Hilbert space.

# *Lecture 18*

These notes are based on Chapters 2 and 3 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*.

## §18.1. Prerequisites

This lecture introduces the *stabilizer framework* for quantum error correction using examples. We first get to know two prerequisites:

- a special case of measurement where the measurement does not change the state of the register, and
- the commuting/anti-commuting properties of tensor products of Pauli matrices.

**Measuring an observable.** Consider a register $A$ with state space $\mathbb{C}^d$, and let $|\psi\rangle$ be the pure state residing in $A$. We measure an observable $M \in \mathbb{C}^{d\times d}$, that is, $M = M^\dagger$. Let

$$M = \sum_\ell \lambda_\ell P_\ell$$

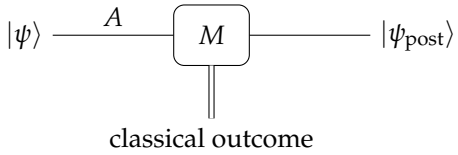
be the spectral decomposition of $M$, where $\lambda_\ell$ are the distinct eigenvalues of $M$ and $P_\ell$ is the orthogonal projection onto the $\ell$-th eigenspace. Note that for any Hermitian matrix eigenvectors corresponding to distinct eigenvalues are orthogonal to each other. We denote the subspace consisting of all eigenvectors with eigenvalue $\lambda_\ell$ along with the all-zero vector (an eigenvector is non-zero by definition, but a subspace must contain the all-zero vector) as

$$S_\ell = \big\{|\varphi\rangle \in \mathbb{C}^d : M|\varphi\rangle = \lambda_\ell|\varphi\rangle\big\}.$$

We define $P_\ell$ to be the operator that projects onto this subspace, i.e., $P_\ell$ and $S_\ell$ satisfy

$$S_\ell = \big\{|\varphi\rangle \in \mathbb{C}^d : P_\ell|\varphi\rangle = |\varphi\rangle\big\}.$$

Recall from Lecture 11 that measuring $M$ produces the classical outcome $\lambda_\ell$ with probability $\|P_\ell|\psi\rangle\|^2 = \langle\psi|P_\ell|\psi\rangle$, and the post-measurement state is then $P_\ell|\psi\rangle / \|P_\ell|\psi\rangle\|$.




We will repeatedly use the following special case of measurement.

**CLAIM.** *If $|\psi\rangle$ is an eigenvector of $M$, say $M|\psi\rangle = \lambda_k|\psi\rangle$, then measuring $M$*

*(1) leaves the state unchanged: $|\psi_{\text{post}}\rangle = |\psi\rangle$; and*

*(2) produces, with probability 1, the classical outcome $\lambda_k$, the eigenvalue corresponding to the eigenvector $|\psi\rangle$.*

*Proof.* Since $|\psi\rangle \in S_k$, we have $P_k|\psi\rangle = |\psi\rangle$. Eigenspaces of a Hermitian matrix corresponding to distinct eigenvalues are mutually orthogonal, so $P_\ell P_k = 0$ for $\ell \neq k$, and hence

$$P_\ell|\psi\rangle = P_\ell P_k|\psi\rangle = 0 \quad \text{for all } \ell \neq k.$$

Thus the outcome $\lambda_\ell$, $\ell \neq k$, occurs with probability $\|P_\ell|\psi\rangle\|^2 = 0$, while $\lambda_k$ occurs with probability $\|P_k|\psi\rangle\|^2 = \||\psi\rangle\|^2 = 1$. The post-measurement state is $P_k|\psi\rangle / \|P_k|\psi\rangle\| = |\psi\rangle$. ∎

**About Pauli matrices.** The Pauli matrices are

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The three non-identity Paulis $X, Y, Z$ *anticommute* with each other:

$$XY = -YX, \qquad YZ = -ZY, \qquad XZ = -ZX.$$

Indeed, direct multiplication gives

$$XY = iZ = -YX, \qquad YZ = iX = -ZY, \qquad ZX = iY = -XZ.$$

Of course, $I$ commutes with every matrix, and every matrix commutes with itself. Also, the Paulis are Hermitian, unitary and self-inverse: $P^\dagger = P$ and $P^2 = I$ for every $P \in \{I, X, Y, Z\}$ (and unitarity then follows from $P^\dagger P = P^2 = I$).

Consider the set

$$\widehat{\mathsf{P}}_n := \{Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n \,:\, Q_i \in \{I, X, Y, Z\}\} \subset \mathbb{C}^{2^n \times 2^n}.$$

We call the elements of $\widehat{\mathsf{P}}_n$ the *n-qubit Paulis*. There are $4^n$ of them. We borrow this notation from Gottesman's book. In his book, Gottesman reserves the notation $\mathsf{P}_n$ (without the hat) for the set

$$\mathsf{P}_n := \{\gamma\, Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n \,:\, Q_i \in \{I, X, Y, Z\},\, \gamma \in \{\pm 1, \pm i\}\}.$$

This distinction is important since $\mathsf{P}_n$ is closed under matrix products and inverse, i.e., if $A, B \in \mathsf{P}_n$ then $AB \in \mathsf{P}_n$ and $A^{-1}, B^{-1} \in \mathsf{P}_n$. On the other hand, $\widehat{\mathsf{P}}_n$ is closed under matrix inverse but not under matrix products; consider for example the case $n = 1$, $X, Z \in \widehat{\mathsf{P}}_1$ but $XZ = -iY \notin \widehat{\mathsf{P}}_1$. At this point we are not interested in closure under matrix multiplication, so we continue to use the Pauli matrices in $\widehat{\mathsf{P}}_n$.

*Shorthand notation.* We will often omit the tensor product symbols, writing for instance $XXI$ for $X \otimes X \otimes I$. Although this is confusing in a general situation, the context will probably help us in deciphering this notation, i.e., read $XXI$ as $X \otimes X \otimes I$ rather than read it as $X \times X \times I = I$. Another shorthand notation for $XXI$ is $X_1X_2$, that is, the operator $X$ appears as a factor in the first and second positions of the Kronecker product.

**CLAIM.** *The n-qubit Paulis have the following properties.*

*(1) Every operator in $\widehat{\mathsf{P}}_n$ is Hermitian and unitary, and is the inverse of itself.*

*(2) If $P, Q \in \widehat{\mathsf{P}}_n$, then either $PQ = QP$ or $PQ = -QP$.*

These facts were stated without proof during the lecture (the proof is by induction on $n$). A direct proof is as follows.

*Proof.* Write $P = P_1 \otimes \cdots \otimes P_n$ and $Q = Q_1 \otimes \cdots \otimes Q_n$ with $P_i, Q_i \in \{I, X, Y, Z\}$.

(1) Using $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$ and $(A \otimes B)(C \otimes D) = AC \otimes BD$,

$$P^\dagger = P_1^\dagger \otimes \cdots \otimes P_n^\dagger = P_1 \otimes \cdots \otimes P_n = P,$$

$$P^2 = P_1^2 \otimes \cdots \otimes P_n^2 = I \otimes \cdots \otimes I = I_{2^n}.$$

So $P$ is Hermitian and self-inverse, and $P^\dagger P = P^2 = I_{2^n}$ shows that $P$ is unitary.

(2) For each $i$, the single-qubit Paulis $P_i$ and $Q_i$ either commute (if $P_i = Q_i$, or if one of them is $I$) or anticommute (if they are distinct and both non-identity). So $P_iQ_i = \varepsilon_i\, Q_iP_i$ with $\varepsilon_i \in \{+1, -1\}$. Therefore

$$PQ = (P_1Q_1) \otimes \cdots \otimes (P_nQ_n) = (\varepsilon_1 Q_1P_1) \otimes \cdots \otimes (\varepsilon_n Q_nP_n) = \Big(\prod_{i=1}^n \varepsilon_i\Big)\, QP,$$

and $\prod_i \varepsilon_i \in \{+1, -1\}$. ∎

The proof of (2) shows more: $P$ and $Q$ anticommute if and only if the number of positions $i$ at which $P_i$ and $Q_i$ are distinct and both non-identity is odd. That is,

$$PQ = (-1)^c QP,$$

where $c$ is the number of Kronecker factor locations $i$ such that $P_i$ and $Q_i$ anticommute.

EXAMPLE. *Let $n = 2$ and consider $X \otimes X,\ Z \otimes Z \in \widehat{\mathsf{P}}_2$. Then*

$$(X \otimes X)(Z \otimes Z) = XZ \otimes XZ = (-ZX) \otimes (-ZX) = ZX \otimes ZX = (Z \otimes Z)(X \otimes X).$$

*So $X \otimes X$ and $Z \otimes Z$ commute, even though $X$ and $Z$ anticommute: the two minus signs cancel.*

EXAMPLE. *Consider the two Paulis $XXI$ and $IXX$. Both Paulis consist of $X$ and $I$ only in their Kronecker factors. Thus, in each of the three Kronecker factor locations we have commutativity only. Hence, overall, these two 3-qubit Paulis commute.*

*Similarly, any two $n$-qubit Paulis whose factors are all either $I$ or one and the same $P \in \{X, Y, Z\}$ always commute with each other, such as $YYI$ and $IYI$, or $ZZZ$ and $IIZ$.*

The stabilizer framework for designing quantum error correcting codes was introduced by Gottesman in his PhD thesis. The Pauli matrices play a central role in this framework:

- the error operators $E_0, E_1, \ldots$ that will be corrected by these codes will be $n$-qubit Paulis,
- the decoder will use Paulis as observables $M_1, M_2, \ldots$ to diagnose which error event occurred in the channel, and
- the code (a subspace of the state space) is determined as the common $+1$-eigenspace of the Paulis $M_1, M_2, \ldots$.

## §18.2. The three-qubit phase-flip code revisited

This code is called the phase-flip code since it corrects phase-flip errors $Z$ occurring on at most one of the three qubits. We relook at this code from the perspective of Paulis and the stabilizer formalism.

**Setting.** We return to the example of Lecture 17. A register of three qubits, with state space $\mathbb{C}^8$, passes through the channel

$$\mathcal{E}(\rho) = \sum_{i=0}^{3} p_i \, E_i \, \rho \, E_i^\dagger,$$

where the four possible errors are

$$E_0 = III, \qquad E_1 = ZII, \qquad E_2 = IZI, \qquad E_3 = IIZ,$$

all of which lie in $\widehat{\mathsf{P}}_3$. The Kraus operators of this channel are

$$\sqrt{p_0}E_0, \ldots, \sqrt{p_3}E_3.$$

We interpret this channel as randomly applying one of the 4 possible unitaries $E_0, \ldots, E_3$, with probabilities $p_0, \ldots, p_3$, respectively. Thus, if $\rho$ is the pure state $|\psi\rangle\langle\psi|$, then we see one of the following four states in the channel output

$$E_0|\psi\rangle, \ldots, E_3|\psi\rangle$$

with probabilities $p_0, \ldots, p_3$, respectively.

Since we know the characterization of the channel $\mathcal{E}$, we know that $\mathcal{E}$ acts irreversibly and hence it will not be wise to allow an arbitrary pure state $|\psi\rangle$ at the channel input. It will be pragmatic to be more conservative and restrict ourselves to a well-designed choice of a subspace $\mathcal{C}$ of the state space $\mathbb{C}^8$. In the case of the phase-flip code we choose $\mathcal{C}$ to be the 2-dimensional subspace spanned by $|+++\rangle$ and $|---\rangle$, i.e.,

$$\mathcal{C} = \text{span}(|+++\rangle, |---\rangle).$$

We only allow pure states $|\psi\rangle$ that belong to this subspace. The subspace $\mathcal{C}$ is called a *code*, *codespace* or *quantum error correcting code*. The states lying in the code $\mathcal{C}$ are called *codewords*. In the case of the phase-flip code, codewords are states of the form

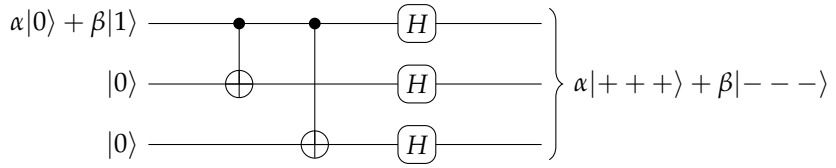
$$|\psi\rangle = \alpha|+++\rangle + \beta|---\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

Note that here $\mathcal{C}$ has dimension equal to 2. This is enough space to carry information about only one qubit since the state space of a qubit is $\mathbb{C}^2$ which is 2-dimensional. Thus, we can *encode* a 'message' qubit $\alpha|0\rangle + \beta|1\rangle$ into a codeword $|\psi\rangle \in \mathcal{C}$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|+++\rangle + \beta|---\rangle.$$

This process is called *encoding* and can be implemented using a unitary map (as shown below). The encoder 'spreads' the quantum information of 1 qubit over 3 qubits (hence, using $3\times$ more quantum resources to store this quantum information). We say that this code uses 3 physical qubits to encode 1 logical qubit. In general, the symbol $n$ is used to denote the number of physical qubits and $k$ denotes the number of logical qubits; $n = 3$ and $k = 1$ in this specific example.

**Encoding circuit.** The message qubit $\alpha|0\rangle + \beta|1\rangle$ is placed on qubit 1, and qubits 2 and 3 are ancillary qubits initialized to $|0\rangle$. The encoding can be implemented using two CNOT gates followed by three Hadamard gates, as shown below. Recall from Lecture 10 that $\text{CNOT}_{i,j}$ denotes the CNOT gate with qubit $i$ as the control and qubit $j$ as the target.




We track the state through the circuit. Before any gate is applied, the three-qubit state is

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle = \alpha|000\rangle + \beta|100\rangle.$$

The gate $\text{CNOT}_{1,2}$ flips qubit 2 exactly when qubit 1 is $|1\rangle$, so by linearity

$$\text{CNOT}_{1,2}\big(\alpha|000\rangle + \beta|100\rangle\big) = \alpha|000\rangle + \beta|110\rangle.$$

Similarly, $\text{CNOT}_{1,3}$ flips qubit 3 exactly when qubit 1 is $|1\rangle$:

$$\text{CNOT}_{1,3}\big(\alpha|000\rangle + \beta|110\rangle\big) = \alpha|000\rangle + \beta|111\rangle.$$

Finally, a Hadamard gate is applied to each qubit, i.e., the gate $H \otimes H \otimes H$. Using $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$,

$$(H \otimes H \otimes H)|000\rangle = H|0\rangle \otimes H|0\rangle \otimes H|0\rangle = |+++\rangle,$$

$$(H \otimes H \otimes H)|111\rangle = H|1\rangle \otimes H|1\rangle \otimes H|1\rangle = |---\rangle.$$

Hence, by linearity,

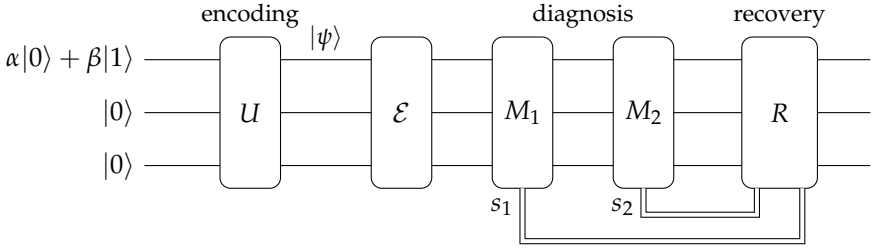
$$(H \otimes H \otimes H)\big(\alpha|000\rangle + \beta|111\rangle\big) = \alpha|+++\rangle + \beta|---\rangle,$$

which is the desired codeword. The encoding unitary is therefore

$$U = (H \otimes H \otimes H)\,\mathrm{CNOT}_{1,3}\,\mathrm{CNOT}_{1,2},$$

a product of unitaries, and hence unitary.

The overall error-correction procedure is shown below. A single-qubit state $\alpha|0\rangle + \beta|1\rangle$, together with two ancillary qubits in state $|0\rangle$, is mapped by a unitary *encoding* $U$ to the codeword $|\psi\rangle$. The codeword passes through the channel $\mathcal{E}$. We then perform a *diagnosis*, also called *syndrome measurement*: two observables $M_1$ and $M_2$ are measured in turn, giving classical outcomes $s_1, s_2 \in \{+1, -1\}$. The pair $(s_1, s_2)$ is called the *syndrome*. Finally, a *recovery* operation, classically controlled by the syndrome, is applied. The syndrome $(s_1, s_2)$ can take four possible values $(\pm 1, \pm 1)$, and identifies which of the four unitary errors $E_0, \ldots, E_3$ occurred in the channel. Once this information is extracted during diagnosis, the inverse unitary is applied in recovery. The observables $M_1$ and $M_2$ are chosen such that irrespective of which of the four errors $E_i$ occurs, the channel output $E_i|\psi\rangle$ is an eigenvector of both $M_1$ and $M_2$, and hence, these two measurements do not modify the state.




**Diagnosis.** Assume that the channel introduced one of the four errors. Then the state before diagnosis is

$$E_i|\psi\rangle \quad \text{for some } i \in \{0, 1, 2, 3\},$$

where we do not know $i$. For the diagnosis, we measure the following two observables:

$$M_1 = XXI = X \otimes X \otimes I,$$

$$M_2 = IXX = I \otimes X \otimes X.$$

**Why use $M_1$ and $M_2$?** Because every codeword $|\psi\rangle$ is a $+1$-eigenvector of both $M_1$ and $M_2$. Indeed, since $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$,

$$\begin{aligned} M_1|\psi\rangle &= (XXI)\big(\alpha|+++\rangle + \beta|---\rangle\big) \\ &= \alpha\,(X|+\rangle)(X|+\rangle)|+\rangle + \beta\,(X|-\rangle)(X|-\rangle)|-\rangle \\ &= \alpha|+++\rangle + \beta\,(-1)(-1)|---\rangle \\ &= |\psi\rangle, \end{aligned}$$

and similarly

$$M_2|\psi\rangle = \alpha|+++\rangle + \beta|---\rangle = |\psi\rangle.$$

We say that $M_1$ and $M_2$ *stabilize* every codeword $|\psi\rangle$, or $M_1, M_2$ stabilize the code $\mathcal{C}$.

We can replace $M_1$ or $M_2$ with $XIX$. This will also give us a valid choice of diagnosis observables, but the association of the syndromes with errors, i.e., $(s_1, s_2) \leftrightarrow E_i$, will change (it will still be one-to-one allowing us to perform a successful recovery).

**Examples.** Suppose the channel introduced the error $E_0 = I \otimes I \otimes I$. The state before diagnosis is $E_0|\psi\rangle = |\psi\rangle$, which is a $+1$-eigenvector of both $M_1$ and $M_2$. By the Claim on measuring an observable in §18.1, the measurements do not change the state, and the syndrome is $(s_1, s_2) = (+1, +1)$.

Now consider $E_1 = ZII$. Before diagnosis the state is $E_1|\psi\rangle$. For the first measurement, in the first position $X$ and $Z$ anticommute, while in the other two positions the factors commute, so $M_1 E_1 = -E_1 M_1$. Hence

$$M_1\big(E_1|\psi\rangle\big) = -E_1 M_1|\psi\rangle = -E_1|\psi\rangle,$$

where the last step uses $M_1|\psi\rangle = |\psi\rangle$. So $E_1|\psi\rangle$ is a $-1$-eigenvector of $M_1$: measuring $M_1$ yields $s_1 = -1$ and leaves $E_1|\psi\rangle$ unchanged. On the other hand, $M_2 = IXX$ and $E_1 = ZII$ commute (in every position one of the two factors is $I$), so $M_2(E_1|\psi\rangle) = E_1 M_2|\psi\rangle = E_1|\psi\rangle$, and measuring $M_2$ yields $s_2 = +1$, again without disturbing the state. The syndrome is $(-1, +1)$.

**In general.** The same argument works for every Pauli error $E_j$ and every Pauli observable $M_i$ that stabilizes all codewords $|\psi\rangle \in \mathcal{C}$.

**CLAIM.** *Let $M_i, E_j \in \widehat{\mathsf{P}}_n$, and let $|\psi\rangle \in \mathcal{C}$ be a codeword. Let $M_i$ stabilize $\mathcal{C}$, i.e., every vector in $\mathcal{C}$ is a $+1$-eigenvector of $M_i$. Then $M_i E_j = \pm E_j M_i$. Suppose the error $E_j$ occurred in the channel and the state $E_j|\psi\rangle$ is measured via the observable $M_i$. We have:*

*(1) the post-measurement state equals the pre-measurement state $E_j|\psi\rangle$;*

*(2) if $M_i$ and $E_j$ commute, the classical outcome is $+1$;*
*if $M_i$ and $E_j$ anticommute, the classical outcome is $-1$.*

*Proof.* By the Claim about $n$-qubit Paulis in §18.1, $M_i E_j = \varepsilon\, E_j M_i$ for some $\varepsilon \in \{+1, -1\}$, with $\varepsilon = +1$ exactly when $M_i$ and $E_j$ commute. Since $M_i|\psi\rangle = |\psi\rangle$,

$$M_i\big(E_j|\psi\rangle\big) = \varepsilon\, E_j M_i|\psi\rangle = \varepsilon\, E_j|\psi\rangle.$$

Moreover, $E_j|\psi\rangle \neq 0$ because $E_j$ is unitary. So $E_j|\psi\rangle$ is an eigenvector of $M_i$ with eigenvalue $\varepsilon$, and the Claim on measuring an observable (§18.1) gives both statements. ∎

Since the first measurement does not disturb the state, the second observable $M_2$ is also measured on the same state $E_j|\psi\rangle$, and thus, we obtain two measurements on the same state.

**Diagnosis / syndrome calculation.** Using the claim, the syndrome for each of the four errors is obtained by checking whether the error commutes $(+1)$ or anticommutes $(-1)$ with each observable. We have the *syndrome table*:

| Error | $M_1 = XXI$ | $M_2 = IXX$ |
|---|---|---|
| $III$ | $+1$ | $+1$ |
| $ZII$ | $-1$ | $+1$ |
| $IZI$ | $-1$ | $-1$ |
| $IIZ$ | $+1$ | $-1$ |

For example, $IZI$ anticommutes with $XXI$ (one conflicting position, namely the second) and with $IXX$ (again the second position), so its syndrome is $(-1, -1)$.

The four syndromes are distinct, so the syndrome identifies which error $E_j$ occurred. The recovery then applies $E_j$ once more; since $E_j$ is self-inverse,

$$E_j\big(E_j|\psi\rangle\big) = E_j^2|\psi\rangle = |\psi\rangle,$$

and the codeword is restored exactly. That is, the recovery operation $R$ applies

| Syndrome $(s_1, s_2)$ | Gate applied |
|---|---|
| $(+1, +1)$ | $III$ |
| $(-1, +1)$ | $ZII$ |
| $(-1, -1)$ | $IZI$ |
| $(+1, -1)$ | $IIZ$ |

REMARK. *In code design, there is a tension or trade-off between the number or diversity of error operators that can be corrected and the amount of physical resources required to correct these errors. The ability to correct a larger number of (linearly independent) error operators generally requires a larger number of physical qubits (to encode the quantum information into).*

REMARK. *The phase-flip code can be used to correct the errors $ZZZ, IZZ, ZIZ, ZZI$ (can you find the syndrome table for this collection of errors?). We chose to correct $III, ZII, IZI, IIZ$ instead of $ZZZ, IZZ, ZIZ, ZZI$ (both have the same number of linearly independent error operators), since in channel models of interest to us the errors $III, ZII, IZI, IIZ$ have a greater probability of occurring than $ZZZ, IZZ, ZIZ, ZZI$, i.e., it is more likely to experience zero or one phase flip than to experience two or three phase flips.*

## §18.3. The Steane code

The 3-qubit phase-flip code is not a truly quantum code. It corrects only one type of Pauli error — the $Z$ error occurring in at most one of the three physical qubits. It is reasonable to expect a quantum code to correct all Pauli errors: $X, Y$ and $Z$ errors. We will now look at the Steane code that encodes $k = 1$ logical qubit into $n = 7$ physical qubits. This code corrects one Pauli error in any of its physical qubits.

The shortest code that encodes one logical qubit and can correct any single Pauli error is of length $n = 5$ (i.e., number of physical qubits). The Steane code uses 7 physical qubits, and hence, is less efficient. On the positive side[1], the Steane code has a rich structure that allows us to describe the error correction easily.

For the Steane code, the state space of the seven physical qubits is $(\mathbb{C}^2)^{\otimes 7} = \mathbb{C}^{128}$, and the code $\mathcal{C}$ is a 2-dimensional subspace of $\mathbb{C}^{128}$. We will use six observables $M_1, \ldots, M_6 \in \widehat{\mathsf{P}}_7$, built from the following *seed matrix*:

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The seed matrix contains all the non-zero binary strings of length 3 as its columns; no two columns are identical. In classical coding theory this is the parity check matrix of the Hamming code.

Each row of the seed matrix gives two observables: one obtained by placing $X$ at the positions of the 1s and $I$ elsewhere, and one obtained by placing $Z$ at the positions of the 1s and $I$ elsewhere:

$$\begin{aligned} M_1 &= I\,I\,I\,X\,X\,X\,X, \\ M_2 &= I\,X\,X\,I\,I\,X\,X, \\ M_3 &= X\,I\,X\,I\,X\,I\,X, \\ M_4 &= I\,I\,I\,Z\,Z\,Z\,Z, \\ M_5 &= I\,Z\,Z\,I\,I\,Z\,Z, \\ M_6 &= Z\,I\,Z\,I\,Z\,I\,Z. \end{aligned}$$

FACT. There exists a 2-dimensional subspace $\mathcal{C}$ of $\mathbb{C}^{128}$ that is stabilized by $M_1, \ldots, M_6$ (we did not prove this during the lecture). A logical qubit $\alpha|0\rangle + \beta|1\rangle$ is mapped into $\mathcal{C}$ using a unitary gate. The Steane code is this subspace $\mathcal{C}$ and the pure states of $\mathcal{C}$ are the codewords.

We consider 22 possible error operators: no error, one $X$ error in any of the physical qubits, similarly a single $Y$ error, and a single $Z$ error. For diagnosis we do a sequence of 6 measurements using the observables $M_1, \ldots, M_6$ yielding a syndrome $(s_1, \ldots, s_6)$ with each $s_i \in \{+1, -1\}$. The Steane code is designed in such a way that $(s_1, \ldots, s_6)$ uniquely

[1]The Steane code also has good fault-tolerant properties, such as the transversal implementation of all logical Clifford gates, see Chapter 11 of Gottesman's book.

determines which of the 22 errors we are interested in occurred. Listing all the 22 errors and their syndromes will give us a syndrome table with 22 rows.

EXAMPLE. *Suppose the channel applies an X error to the fourth qubit, i.e., the error* $E = IIIXIII$. *The syndrome is obtained, as in §18.2, by checking commutation of E with each* $M_i$*:*

| | $M_1$ | $M_2$ | $M_3$ | $M_4$ | $M_5$ | $M_6$ |
|---|---|---|---|---|---|---|
| $IIIXIII$ | $+1$ | $+1$ | $+1$ | $-1$ | $+1$ | $+1$ |

*Only* $M_4$ *has a Z in position* 4*, so E anticommutes with* $M_4$ *and commutes with all the others.*

More generally, for any $X$ error, the error operator and the observables $M_1, M_2, M_3$ commute since $M_1, M_2, M_3$ are composed of Kronecker factors $I$ and $X$.

We will pursue the Steane code further in Lecture 19 and observe that syndrome measurement can indeed distinguish between the 22 errors we are interested in.

# *Lecture 19*

These notes continue Lecture 18 with the discussion on the Steane code. We then discuss the 9-qubit Shor code. Both these codes are instances of stabilizer codes (as is the 3-qubit phase-flip code from Lecture 18).

## §19.1. The Steane code

The Steane code encodes $k = 1$ logical qubit into $n = 7$ physical qubits. The state space of the seven physical qubits is $(\mathbb{C}^2)^{\otimes 7} = \mathbb{C}^{128}$, and the code $\mathcal{C}$ is a 2-dimensional subspace of $\mathbb{C}^{128}$.

**Encoding.** Pick any orthonormal basis of $\mathcal{C}$ and call its elements $|\bar{0}\rangle, |\bar{1}\rangle$ (also written $|0_L\rangle, |1_L\rangle$, for 'logical'). Encoding is the map

$$\alpha|0\rangle + \beta|1\rangle \;\longmapsto\; \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle, \qquad \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2, \quad \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \in \mathcal{C} \subset \mathbb{C}^{128},$$

implemented by appending 6 ancillary qubits in the state $|0\cdots 0\rangle$ and applying a unitary gate on the composite system of 7 qubits:

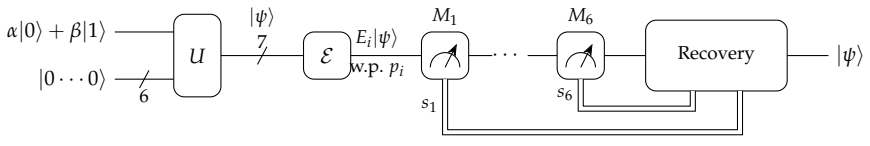
$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes |000000\rangle \;\xrightarrow{\text{unitary gate}}\; \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle.$$

We have the freedom to choose any orthonormal basis $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ of the code $\mathcal{C}$ to apply the above unitary encoding. However, certain choices of the bases are mathematically more structured and natural to use. This is indeed the case with a subclass of stabilizer codes called the *CSS codes* (named after Calderbank, Shor and Steane) to which the Steane code belongs. Every CSS code has a natural choice of logical basis that can be expressed in terms of the codewords of a pair of classical error correcting codes[1]. For the Steane code the natural basis is

$$\begin{aligned}|\bar{0}\rangle = \tfrac{1}{\sqrt{8}}\Big(&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\Big),\\ |\bar{1}\rangle = X^{\otimes 7}|\bar{0}\rangle.&\end{aligned}$$

The standard basis vectors appearing in the linear expansion of $|\bar{0}\rangle$ are the codewords of the dual of the (classical) Hamming code.

**Error correction.** The overall procedure is shown below. The codeword $|\psi\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \in \mathcal{C}$ passes through the channel $\mathcal{E}$; we then measure the six observables $M_1, \ldots, M_6$ of Lecture 18 in turn, obtaining the syndrome $s = (s_1, \ldots, s_6)$, and a recovery operation controlled by $s$ restores $|\psi\rangle$.




[1]This basis is useful in identifying logical operations on the codewords, see Chapters 5 and 11 of Gottesman's book.

*Assumption.* The channel $\mathcal{E}$ introduces Pauli errors: $|\psi\rangle \mapsto E_i|\psi\rangle$ with probability $p_i$, where $E_i \in \widehat{\mathsf{P}}_7$.

We will first see that the code can correct the following set of 22 errors: no error (i.e., the error operator is $E = I^{\otimes 7}$), an $X$ error on any one of the 7 qubits, a $Y$ error on one of the 7 qubits, or a single $Z$ error. That is, the Steane code can correct all one-qubit Pauli errors. We will denote these 22 error operators as

$$I, X_j, Y_j \text{ or } Z_j, \text{ for } j = 1, \ldots, 7,$$

where $X_j$ is the 7-qubit Pauli with $X$ on the $j^{\text{th}}$ qubit and identity elsewhere. We can verify this directly by inspecting the measurement syndrome for each of these 22 error operators. Recall from Lecture 18 the six observables measured for diagnosis:

$$\begin{aligned} M_1 &= I\,I\,I\,X\,X\,X\,X, \quad & M_4 &= I\,I\,I\,Z\,Z\,Z\,Z, \\ M_2 &= I\,X\,X\,I\,I\,X\,X, \quad & M_5 &= I\,Z\,Z\,I\,I\,Z\,Z, \\ M_3 &= X\,I\,X\,I\,X\,I\,X, \quad & M_6 &= Z\,I\,Z\,I\,Z\,I\,Z. \end{aligned}$$

Note that among $M_1, M_2, M_3$ the 'signature' formed by $I$ and $X$ is distinct across the 7 qubit locations. Similar observation holds for $M_4, M_5, M_6$. This signature comes from the seed matrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

whose columns are precisely the seven distinct non-zero binary strings of length 3. Let's now calculate the syndromes for each of the 22 errors we are interested in. We will see that these 22 syndromes are distinct and hence they help the decoder identify the error and apply its inverse for successful recovery.

Recall that for stabilizer codes with Pauli error $E$ and the stabilizing measurement observable $M_i$ the outcome of measuring $M_i$ is

- $s_i = +1$ if $M_i$ and $E$ commute,
- $s_i = -1$, otherwise (that is, $M_i$ and $E$ anticommute).

Further, measurement does not change the quantum state. Hence, all six measurements are performed on the same state and each measurement outcome provides us some information about the error operator $E$.

1. *No error.* In this case the error operator is $E = I^{\otimes 7}$ and the channel output is $E|\psi\rangle = |\psi\rangle \in \mathcal{C}$. Since the code $\mathcal{C}$ is stabilized by $M_1, \ldots, M_6$ we have

   $$M_i E|\psi\rangle = M_i|\psi\rangle = |\psi\rangle = E|\psi\rangle$$

   and thus, each measurement leaves the state unaffected and outputs $s_i = +1$ as the classical outcome. Thus, the syndrome for no error is $(+1, \ldots, +1)$.

2. *Single X error.* Assume that the error occurred at qubit $j$, i.e., $E = X_j$. Note that $X_j$ commutes with $M_1, M_2, M_3$ since these are all $X$-type Paulis (they are Kronecker products of $X$ and $I$ only). Thus, $(s_1, s_2, s_3) = (+1, +1, +1)$. However, $X_j$ anticommutes with at least one of $M_4, M_5, M_6$ so that $(s_4, s_5, s_6) \neq (+1, +1, +1)$. This is the identifying feature of $X$-type errors. Among $M_4, M_5, M_6$, we see that $X_j$ anticommutes with $M_i$ if and only if $M_i$ has $Z$ as a factor in the $j^{\text{th}}$ factor of its Kronecker product. Thus, $(s_4, s_5, s_6)$ is precisely the 'signature' available in the $j^{\text{th}}$ column of the seed matrix with 1 replaced by $-1$ and 0 replaced with $+1$. Since the columns of the seed matrix are distinct, the second part of the syndrome $(s_4, s_5, s_6)$ identifies the location of the single $X$ error.

3. *Single Z error.* Assume that the error occurred at qubit $j$, i.e., $E = Z_j$. Now $Z_j$ commutes with $M_4, M_5, M_6$ since these are all $Z$-type Paulis (Kronecker products of $Z$ and $I$ only). Thus, $(s_4, s_5, s_6) = (+1, +1, +1)$. However, $Z_j$ anticommutes with at least one of $M_1, M_2, M_3$ so that $(s_1, s_2, s_3) \neq (+1, +1, +1)$. This is the identifying feature of $Z$-type errors. Among $M_1, M_2, M_3$, we see that $Z_j$ anticommutes with $M_i$ if and only if $M_i$ has $X$ as a factor in the $j^{\text{th}}$ factor of its Kronecker product. Thus, $(s_1, s_2, s_3)$ is precisely the 'signature' available in the $j^{\text{th}}$ column of the seed matrix with 1 replaced by $-1$ and 0 replaced with $+1$. Since the columns of the seed matrix are distinct, the first part of the syndrome $(s_1, s_2, s_3)$ identifies the location of the single $Z$ error.

4. *Single Y error.* Assume that the error occurred at qubit $j$, i.e., $E = Y_j$. Since $Y$ anticommutes with both $X$ and $Z$ (and commutes with $I$), $Y_j$ anticommutes with $M_i$ if and only if $M_i$ has a non-identity factor ($X$ or $Z$) in the $j^{\text{th}}$ factor of its Kronecker product, for each $i = 1, \ldots, 6$. Hence, both halves of the syndrome carry the signature of the $j^{\text{th}}$ column of the seed matrix: $(s_1, s_2, s_3) = (s_4, s_5, s_6) \neq (+1, +1, +1)$. This is the identifying feature of $Y$-type errors, and it is consistent with $Y_j \sim X_j Z_j$ up to a global phase (see below): the syndrome of $Y_j$ is the combination of the syndromes of $X_j$ and $Z_j$. As before, since the columns of the seed matrix are distinct, the syndrome identifies the location $j$ of the single $Y$ error.

We record this observation as

**CLAIM.** *The Steane code can correct any single Pauli error on any physical qubit; that is, it corrects the* 22 *errors* $I^{\otimes 7}$, $X_j$, $Y_j$, $Z_j$ $(j = 1, \ldots, 7)$.

While this is a good result, we see that we can probably correct more errors (in addition to the 22 listed above) since we have not exhausted all the possibilities of the syndrome $(s_1, \ldots, s_6)$. The 22 errors have accounted for only 22 of the 64 possible syndromes.

We will now see that the Steane code can correct the following 64 possible errors

- an $X$ error on at most one physical qubit ($1 + 7 = 8$ possibilities), and independently of this,
- a $Z$ error on at the most one of the qubits (again 8 possibilities),

totalling $8 \times 8 = 64$ possibilities. In other words, the errors are

$$I^{\otimes 7}, X_i, Z_j \text{ and } X_i Z_j \text{ for all } i, j = 1, \ldots, 7.$$

Before we study the syndromes of these 64 errors, let us observe that this set includes $Y$ errors on any single qubit. This follows from

$$Y_j = i\, X_j Z_j = e^{i\pi/2} X_j Z_j, \text{ i.e., } Y_j = X_j Z_j \text{ up to global phase.}$$

Since the channel was assumed to introduce a Pauli gate (at random) as an error, and since any two gates differing by a global phase are equivalent, we see that correcting the error $X_j Z_j$ is the same as correcting the error $Y_j$.

The correction process for correcting these 64 errors is similar to correcting the 22 error from earlier. We correct $X$-type and $Z$-type errors independently (even if they both occur and even if they occur on the same qubit). To decode the $X$-type error we make use of $(s_4, s_5, s_6)$ and to decode the $Z$-type error using $(s_1, s_2, s_3)$.

Assume the error $X_i Z_j$ occurred (where $i$ and $j$ can be equal). Among $M_1, M_2, M_3$, $X_i Z_j$ anticommutes with $M_k$ if and only if $M_k$ contains an $X$ in its $j^{\text{th}}$ Kronecker factor. Hence, as before, $(s_1, s_2, s_3)$ identifies the location $j$ of the $Z$ error. If there was no $Z$ error then $s_1 = s_2 = s_3 = +1$. Similarly, $(s_4, s_5, s_6)$ identifies the location $i$ of $X$ error and $s_4 = s_5 = s_6 = +1$ if there was no $X$-type error.

This exhausts all the 64 possibilities of the syndrome.

## §19.2. Remarks on stabilizer codes

The canonical decoding architecture for stabilizer codes measures $r$ Pauli observables $M_1, \ldots, M_r \in \widehat{\mathsf{P}}_n$ and uses the syndrome $(s_1, \ldots, s_r)$ for recovery.

We would like each of these measurements to *not* change the quantum state being measured. This can indeed happen only when the quantum state is a common eigenvector of $M_1, \ldots, M_r$. Further, when there is no error, i.e., $E = I^{\otimes n}$, we would like to have the all-$+1$ syndrome $s_1 = \cdots = s_r = +1$. This is the condition

$$M_1|\psi\rangle = \cdots = M_r|\psi\rangle = |\psi\rangle \text{ for all } |\psi\rangle \in \mathcal{C}.$$

Hence, we choose $\mathcal{C}$ to be the common $+1$-eigenspace of $M_1, \ldots, M_r$. The existence of such a non-trivial subspace is possible only when the Paulis $M_1, \ldots, M_r$ commute with each other; this is tied with the matrix theoretic fact that diagonalizable matrices that pairwise commute with each other can be simultaneously diagonalized (see a related question in Homework 9). Thus, we assume that $M_1, \ldots, M_r$ commute with each other.

We would like the classical information made available by each measurement to be *informative*, i.e., we would like to perform a measurement $M_i$ only if its outcome $s_i$ is not a pre-determined function of the measurement outcomes $(s_j : j \neq i)$. This will minimize the number of measurements required for decoding and it also provides a tight mathematical structure to analyze the diagnosis step. We can ensure that there is no redundancy in the syndrome components $s_1, \ldots, s_r$ when we have

$$M_i \neq \gamma \prod_{j:j\neq i} M_j^{a_j}$$

for every $\gamma \in \mathbb{C}$ with $|\gamma| = 1$ and every choice of integers $\{a_j\}$ (see a related question in Homework 9).

Apart from the above two conditions there is yet another condition for existence of a non-trivial subspace $\mathcal{C}$ (this is the condition that the multiplicative group generated by $M_1, \ldots, M_r$ should not include $-I$). Under these conditions we have

$$k = n - r$$

where $k$ is the number of logical qubits which determines the dimension of $\mathcal{C}$ as $2^k$. Hence, increasing the number of non-redundant measurements reduces the number of logical qubits of stabilizer codes. We will look at these results in greater details in later lectures.

In the Steane code $n = 7$, $r = 6$, so $k = 1$; in the phase-flip code of Lecture 18, $n = 3$, $r = 2$, so $k = 1$. An extreme case is $r = n$, where $k = 0$ and the code is a single state up to a global phase (dimension of $\mathcal{C}$ is $2^k = 2^0 = 1$).

**DEFINITION.** *A* stabilizer state *is a common $+1$-eigenvector of $n$ pairwise commuting, independent (in terms of matrix product) Paulis $M_1, \ldots, M_n \in \widehat{\mathsf{P}}_n$.*

EXAMPLE. *Let $n = 2$, $M_1 = X \otimes X$, $M_2 = Z \otimes Z$. These commute (Lecture 18). The state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is a common $+1$-eigenvector:*

$$(X \otimes X)\,\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|11\rangle + |00\rangle}{\sqrt{2}}, \qquad (Z \otimes Z)\,\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

*So the EPR state is a stabilizer state.*

## §19.3. The Shor code

The Shor code has $k = 1$ logical qubit and $n = 9$ physical qubits: the message qubit is joined by 8 ancillary qubits in state $|0\cdots0\rangle$, a unitary $U$ maps it to $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \in \mathbb{C}^{512}$,

and the circuit is the same as before, but with 8 observables $M_1, \ldots, M_8$ and syndrome $s = (s_1, \ldots, s_8)$. As before, the channel may apply an $X$ error on any qubit and an independent $Z$ error on any qubit. This set of errors includes a $Y$ on a single qubit (this is when $X$ and $Z$ occur on the same qubit).

**The code.** An orthonormal basis of the code is

$$|\bar{0}\rangle = \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^{\otimes 3}, \qquad |\bar{1}\rangle = \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)^{\otimes 3}.$$

The observables, written as three blocks of three qubits each (block 1 contains first three qubits, block 2 contains the next set of 3 qubits, etc.), are

$$M_1 = XXX\ XXX\ III, \quad M_3 = ZZI\ III\ III, \quad M_5 = III\ ZZI\ III, \quad M_7 = III\ III\ ZZI,$$
$$M_2 = III\ XXX\ XXX, \quad M_4 = IZZ\ III\ III, \quad M_6 = III\ IZZ\ III, \quad M_8 = III\ III\ IZZ.$$

All 8 commute pairwise (the $X$-type and $Z$-type ones overlap in an even number of positions), and they are independent, so $k = n - r = 9 - 8 = 1$.

**Syndromes.** To analyse the syndromes, we split the syndrome $(s_1, \ldots, s_8)$ into four sections of two values each: $(s_1, s_2), \ldots, (s_7, s_8)$.

The section $(s_3, s_4)$ carries information about $X$ error when it occurs in qubits in block 1 (i.e., qubits 1, 2 or 3). To see why, recall that $M_3 = ZZI\ III\ III$ and $M_4 = IZZ\ III\ III$ are the only observables that have $Z$ factors in block 1. An $X$ error on qubit $q \in \{1, 2, 3\}$ commutes with $M_1, M_2$ (these only have $X$ and $I$ factors) and with $M_5, \ldots, M_8$ (these have identity factors in block 1), so $s_1 = s_2 = s_5 = \cdots = s_8 = +1$. It anticommutes with $M_3$ or $M_4$ exactly when that observable has a $Z$ in position $q$:

| Error | $M_3 = ZZI\ III\ III$ | $M_4 = IZZ\ III\ III$ |
|---|---|---|
| $X_1$ | $-1$ | $+1$ |
| $X_2$ | $-1$ | $-1$ |
| $X_3$ | $+1$ | $-1$ |

Thus $(s_3, s_4)$ equals $(+1, +1)$ if there is no $X$ error in block 1 and is one of three distinct non-trivial values otherwise, which tells us the location of the $X$ error within block 1. The same argument applies to the sections $(s_5, s_6)$ and $(s_7, s_8)$ for blocks 2 and 3, respectively. Note that the syndrome values $s_3, \ldots, s_8$ are 'transparent' to any $Z$ error occurring independently of these $X$ errors, since the presence of any $Z$ component will not affect the values $s_3, \ldots, s_8$. Hence, we conclude that the Shor code can correct any single $X$ error (independently of any $Z$ errors occurring).

Similarly, the section $(s_1, s_2)$ carries information about $Z$ errors. Here $M_1 = XXX\ XXX\ III$ and $M_2 = III\ XXX\ XXX$ are the only observables with $X$ factors. A $Z$ error on any qubit commutes with $M_3, \ldots, M_8$ (these only have $Z$ and $I$ factors), so $s_3 = \cdots = s_8 = +1$. It anticommutes with $M_1$ exactly when the single $Z$ error occurs in block 1 (qubits 1–3) or block 2 (qubits 4–6). Similarly, the $Z$ error anticommutes with $M_2$ if it occurs either in block 2 or block 3.

| Error | $M_1 = XXX\ XXX\ III$ | $M_2 = III\ XXX\ XXX$ |
|---|---|---|
| $Z$ in block 1 (qubit 1, 2 or 3) | $-1$ | $+1$ |
| $Z$ in block 2 (qubit 4, 5 or 6) | $-1$ | $-1$ |
| $Z$ in block 3 (qubit 7, 8 or 9) | $+1$ | $-1$ |

Thus $(s_1, s_2)$ equals $(+1, +1)$ if there is no $Z$ error and is one of three distinct non-trivial values otherwise, which identifies the *block* in which the $Z$ error occurred. Note, however, that the section $(s_1, s_2)$ does not tell us which of the three qubits of that block was hit. This is unlike the decoding of $X$ errors above, which pins down the exact qubit. Fortunately, any $Z$ error in block 1 (similarly for block 2 or block 3) affects a codeword the same way and hence their effect can be undone using the same recovery.

**CLAIM.** *For any codeword $|\psi\rangle \in \mathcal{C}$, $Z_1|\psi\rangle = Z_2|\psi\rangle = Z_3|\psi\rangle$ (and likewise in the other blocks).*

*Proof.* It suffices to check this for $|\bar{0}\rangle$ and $|\bar{1}\rangle$, since then $Z_1(\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle) = Z_2(\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle)$ by linearity. For $j \in \{1,2,3\}$, $Z_j|000\rangle = |000\rangle$ and $Z_j|111\rangle = -|111\rangle$, so

$$Z_j \frac{|000\rangle \pm |111\rangle}{\sqrt{2}} = \frac{|000\rangle \mp |111\rangle}{\sqrt{2}} \qquad (j = 1,2,3),$$

independent of $j$. Hence

$$Z_1|\bar{0}\rangle = \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right) = Z_2|\bar{0}\rangle = Z_3|\bar{0}\rangle,$$

and likewise $Z_1|\bar{1}\rangle = Z_2|\bar{1}\rangle = Z_3|\bar{1}\rangle$. ■

So any $Z$ error in the first three qubits affects $|\psi\rangle \in \mathcal{C}$ in the same way, and they have the same recovery (apply, say, $Z_1$). If $Z_1$ was the error introduced in the channel, the decoder recognizes that one of the $Z_1, Z_2$ or $Z_3$ occurred. It can arbitrarily pick one of these three unitary operators for recovery. Even if the decoder picks $Z_2$ for recovery there is no actual harm since $Z_1$ and $Z_2$ act on all codewords the same way. Therefore the Shor code corrects any single Pauli error on any physical qubit.

The Shor code is an example of a *degenerate code*: there are two correctable errors (which are not scalar multiples of each other) that affect the codewords the same way. Hence, the decoder is not required to distinguish between these two errors.

# *Homework 9*

1. **Spectrum of Paulis.** You must show that every non-identity $n$-qubit Pauli has exactly two eigenvalues $+1$ and $-1$, each with multiplicity $2^{n-1}$.

   HINT. Each non-identity $P \in \widehat{\mathsf{P}}_n$ is unitary and Hermitian and has zero trace. In the complex plane where do the eigenvalues of unitary operators lie? What about the eigenvalues of Hermitian operators? If the trace is zero what happens to the eigenvalues?

2. **Non-commuting Paulis do not have common eigenvectors.** Suppose $P, Q \in \widehat{\mathsf{P}}_n$ and $P$ and $Q$ do not commute, which means that $PQ = -QP$. You must show that there is no *non-zero* $|\psi\rangle$ such that $|\psi\rangle$ is an eigenvector of $P$ (with some eigenvalue) and $|\psi\rangle$ is an eigenvector of $Q$ (with eigenvalue not necessarily the same as that of $P$).

   HINT. One solution is to use proof by contradiction. Suppose $|\psi\rangle \neq 0$ is indeed a common eigenvector of $P$ and $Q$ (with possibly different eigenvalues), compare $PQ|\psi\rangle$ and $QP|\psi\rangle$. What contradiction do you reach?

3. **The optimal single error correcting quantum code.** The shortest quantum error correcting code that can correct a single Pauli error (an $X$, $Y$ or $Z$ error) uses $n = 5$ physical qubits and encodes $k = 1$ logical qubit. If you are curious, you can look up the code's logical orthonormal basis $|\bar{0}\rangle, |\bar{1}\rangle \in \mathbb{C}^{2^5}$ in this code's page in **Error Correction Zoo**.

   This code has been designed to be decoded using the following set of $r = n - k = 4$ measurement observables

   $$\begin{aligned} M_1 &= XZZXI \\ M_2 &= IXZZX \\ M_3 &= XIXZZ \\ M_4 &= ZXIXZ \end{aligned}$$

   *Questions*

   (a) Do $M_1, \ldots, M_4$ commute pairwise?

   (b) Find the syndromes for each of the possible 16 errors: no error, single $X$ error, single $Y$ error, single $Z$ error. Are these syndromes distinct?

4. **A simplified version of the quantum Hamming bound.** The quantum Hamming bound limits how many logical qubits a *non-degenerate* code can protect against a given set of errors (we didn't define degeneracy and non-degeneracy in the lectures, but we will come to that soon). In this question we will look at a simplified version of this bound. For this simplification we will make some assumptions (beyond non-degeneracy) that are not necessary to prove the quantum Hamming bound.

   *Assumptions.* Suppose we encode $k$ logical qubits into $n$ physical qubits with $n > k$. Assume that we decode the code in two steps

   - syndrome measurement as observables using $r$ pairwise commuting, non-identity Pauli measurement observables $M_1, \ldots, M_r$, and
   - recovery unitary (which is decided by the syndrome value).

This is a major assumption since, in principle, one is free to design a decoding algorithm and a decoder circuit and it is possible to perform decoding (which is a CPTP map) which need not follow the above two steps. For this question we will enforce this assumption (the real proof of the quantum Hamming bound does not use this assumption, see Chapter 7 of Gottesman's book). Further, as done in Lecture 19, let us assume that the number $r$ of measurements we make satisfies

$$r = n - k.$$

The quantum Hamming bound applies only to non-degenerate codes; while we don't want to formally define non-degeneracy right now, you can assume that this means that the Pauli errors we want to correct have distinct syndromes. Now to the question itself.

*Questions.*

Let all the above assumptions hold ($r = n - k$, syndrome measurement + recovery steps, distinct syndromes for each of the Pauli errors we want to correct).

(a) Since each $M_i$ is a Pauli, what are the possible classical outcomes of this measurement? How many different values can the syndrome $(s_1, \ldots, s_{n-k})$ potentially take?

HINT. What are the possible eigenvalues of Paulis?

(b) Suppose we want to encode $k$ logical qubits into $n$ physical qubits. Suppose we wish to correct a single Pauli error, i.e., the errors we want to correct are: no error, one $X$ error, one $Y$ error, or one $Z$ error. Show that

$$k \leq n - \log_2(1 + 3n)$$

HINT. How many Pauli errors do we wish to correct? How many different values can the syndrome vector $(s_1, \ldots, s_{n-k})$ take? We want distinct syndromes for each correctable Pauli error — use the pigeonhole principle.

(c) Generalize the quantum Hamming bound to correcting up to $t$ Pauli errors (where $t$ is some design constant): that is we want to correct every Pauli error $P_1 \otimes \cdots \otimes P_n$ such that the number of non-identity $2 \times 2$ Paulis $P_i$ is at most $t$. Show that

$$k \leq n - \log_2 \left( 1 + \sum_{w=1}^{t} \binom{n}{w} 3^w \right).$$

HINT. How many distinct Pauli errors do we wish to correct?

(d) Do any of the codes we know so far satisfy this bound with equality: Steane code, Shor code, the 5-qubit code?

REMARK. Non-degenerate codes that satisfy the quantum Hamming bound with equality are called *perfect codes*.

5. **Redundant measurements in diagnosis.** Consider the Steane code as treated during Lecture 19. We used $M_1, \ldots, M_6$ (first three are $X$ type, rest are $Z$ type). These 6 observable Paulis are not dependent, i.e., it is not possible to express any $M_i$ as a product of powers of the rest of the $M_j$'s (up to global phase), i.e.,

$$M_i \neq \gamma \prod_{j:\neq i} M_j^{a_j}$$

for any $|\gamma| = 1$ and any integers $\{a_j : j \neq i\}$. This is the key mathematical property that ensures that with each measurement we get some information that is not already obtained from the other measurements.

In this question we will break this assumption by introducing a seventh redundant observable $M_7$ that depends on $M_1, \ldots, M_6$. Say

$$M_7 = M_1 M_2 = I \otimes X \otimes X \otimes X \otimes X \otimes I \otimes I.$$

Now the modified syndrome contains 7 components $(s_1, \ldots, s_6, s_7)$ instead of the original 6. You must show that $s_7$ is redundant.

*Question.* Show that the value $s_7$ is a deterministic function of $s_1, \ldots, s_6$. In particular, show that

$$s_7 = s_1 s_2$$

for any Pauli error $E$ introduced by the channel.

HINT. Instead of checking this brute force for all the Pauli errors, we can quickly make use of the eigen property of the observables $M_j$ and noisy codewords $E|\psi\rangle$. Is $E|\psi\rangle$ an eigenvector of $M_7$? What is its eigenvalue?

6. Verify that every codeword $|\psi\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ in the Shor code is a $+1$-eigenvector of each of the observables $M_1, \ldots, M_8$ listed in Lecture 19, i.e.,

$$M_j|\psi\rangle = |\psi\rangle \text{ for all } j = 1, \ldots, 8.$$

7. **Alternative argument for degeneracy in the Shor code.** Use the same notation as in Lecture 19. Let $|\psi\rangle$ be an arbitrary codeword from the Shor code.

   (a) Is it true that $M_3|\psi\rangle = M_4|\psi\rangle$? Does this mean that $Z_1|\psi\rangle = Z_3|\psi\rangle$?

   (b) Using a similar argument prove that $Z_2|\psi\rangle = Z_1|\psi\rangle$.

8. **A correctable set of errors for the Shor code.** In addition to

   - an $X$ error on at most one qubit, and independently of this,
   - a $Z$ error on at most one qubit

   what other errors can the Shor code correct?

   HINT. Can the Shor code correct some patterns of two $X$ errors?

9. **A generalization of the Shor code.** Consider encoding one logical qubit into 25 physical qubits using the logical basis

$$|\bar{0}\rangle = \left(\frac{|00000\rangle + |11111\rangle}{\sqrt{2}}\right)^{\otimes 5}$$
$$|\bar{1}\rangle = \left(\frac{|00000\rangle - |11111\rangle}{\sqrt{2}}\right)^{\otimes 5}$$

   (a) Can you find 24 observable Paulis $M_1, \ldots, M_{24}$ (in the same pattern as the 9-qubit Shor code) such that $M_j|\psi\rangle = |\psi\rangle$ for all codewords $|\psi\rangle$?

   (b) Argue that this code can independently correct at most two $X$ errors and at most two $Z$ errors.

   (c) Does this code correct at most two $Y$ errors as well?

10. **A code for correcting a single unitary error.** Consider encoding one logical qubit into three physical qubits to protect against the following four errors where $U \in \mathbb{C}^{2\times 2}$ is a unitary matrix and $I$ is the $2 \times 2$ identity matrix:

$$III, UII, IUI, IIU$$

For any $2 \times 2$ unitary matrix $U$, the following facts are known from linear algebra

- $U$ has a spectral decomposition $U = \lambda_1|\phi_1\rangle\langle\phi_1| + \lambda_2|\phi_2\rangle\langle\phi_2|$,
- $|\lambda_1| = |\lambda_2| = 1$ because $U$ is unitary, and $\langle\phi_1 \,|\, \phi_2\rangle = 0$, $\|\phi_1\| = \|\phi_2\| = 1$.

For this question assume that $\lambda_1 = -\lambda_2$. We make no other assumptions about $U$.

(a) Identify two pure states $|a\rangle, |b\rangle \in \mathbb{C}^2$ such that

$$\langle a \,|\, b\rangle = 0, \;\; \langle a|U|a\rangle = 0, \;\; \langle b|U|b\rangle = 0.$$

(b) Argue that the following encoding of a logical qubit protects against the four errors $III, UII, IUI, IIU$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|aaa\rangle + \beta|bbb\rangle,$$

where $|aaa\rangle = |a\rangle \otimes |a\rangle \otimes |a\rangle$ and $|bbb\rangle = |b\rangle \otimes |b\rangle \otimes |b\rangle$.

# *Lecture 20*

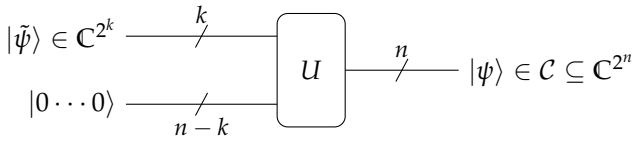
These notes are based on Chapter 2 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. In Lectures 17–19 we studied three specific codes: the 3-qubit phase-flip code, the Steane code and the Shor code. We now give the general definitions: what a quantum error correcting code is, and what it means for a code to correct a quantum channel or a collection of errors. We then ask whether a code that corrects a collection of errors also corrects linear combinations of these errors.

## §20.1. Quantum error correcting codes

**DEFINITION.** *A* quantum error correcting code*, or simply a* code*, $\mathcal{C}$ over $n$ physical qubits is a subspace of $\mathbb{C}^{2^n}$. If $K = \dim(\mathcal{C})$, we say that $\mathcal{C}$ is an $((n, K))$ code. The pure states in $\mathcal{C}$ (i.e., the unit vectors in $\mathcal{C}$) are called* codewords*.*

For example, the phase-flip code of Lecture 18 is a $((3,2))$ code, the Steane code is a $((7,2))$ code and the Shor code is a $((9,2))$ code.

**Encoding logical qubits.** Often $K$ is a power of 2, i.e., $K = 2^k$ for some integer $k \geq 0$. In this case $\mathcal{C}$ is an $((n, 2^k))$ code, and it can be used to encode $k$ *logical qubits*. The state space of $k$ logical qubits is $\mathbb{C}^{2^k}$, and encoding is an isometry (a linear map that preserves inner products) between $\mathbb{C}^{2^k}$ and $\mathcal{C} \subseteq \mathbb{C}^{2^n}$. This is done by appending $n-k$ ancillary qubits in the state $|0\cdots0\rangle$ and then applying a unitary gate $U$ on all $n$ qubits:




To construct $U$, identify any orthonormal basis of $\mathcal{C}$ and label its $2^k$ elements by the binary strings of length $k$:

$$|\overline{0\cdots0}\rangle,\ |\overline{10\cdots0}\rangle,\ \ldots,\ |\overline{1\cdots1}\rangle\ \in \mathcal{C},$$

that is, $|\bar{x}\rangle$ for $x \in \{0,1\}^k$. On the input side, identify the orthonormal set of $2^k$ vectors in $\mathbb{C}^{2^n}$

$$|0\cdots0\rangle \otimes |0\cdots0\rangle, \quad |10\cdots0\rangle \otimes |0\cdots0\rangle, \quad \ldots, \quad |1\cdots1\rangle \otimes |0\cdots0\rangle,$$

that is, $|x\rangle \otimes |0\cdots0\rangle$ for $x \in \{0,1\}^k$, where the first factor is a state of the $k$ logical qubits and the second factor is the state of the $n-k$ ancillary qubits. Recall from Lecture 15 the fact that there exists a unitary that maps one orthonormal set of vectors to another orthonormal set of the same size. Hence, there exists a unitary $U \in \mathbb{C}^{2^n \times 2^n}$ with

$$U\big(|x\rangle \otimes |0\cdots0\rangle\big) = |\bar{x}\rangle \quad \text{for every } x \in \{0,1\}^k.$$

There is more than one choice of such a unitary $U$ when $n > k$; and $n > k$ is the interesting case where you can afford to correct some errors. By linearity, if the $k$ logical qubits are in the state

$$|\tilde{\psi}\rangle = \sum_{x\in\{0,1\}^k} \alpha_x |x\rangle = \alpha_{0\cdots0}|0\cdots0\rangle + \alpha_{10\cdots0}|10\cdots0\rangle + \cdots,$$

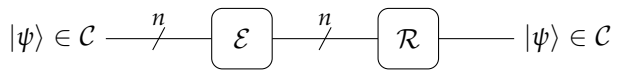
then the corresponding codeword is

$$\begin{aligned} U\big(|\tilde{\psi}\rangle \otimes |0\cdots0\rangle\big) &= \sum_{x\in\{0,1\}^k} \alpha_x |\bar{x}\rangle \\ &= \alpha_{0\cdots0}|\overline{0\cdots0}\rangle + \alpha_{10\cdots0}|\overline{10\cdots0}\rangle + \cdots. \end{aligned}$$

Since $U$ is unitary and the ancillary state $|0\cdots0\rangle$ is a unit vector, the map $|\tilde{\psi}\rangle \mapsto U(|\tilde{\psi}\rangle \otimes |0\cdots0\rangle)$ preserves inner products, and its image is all of $\mathcal{C}$ (every vector of $\mathcal{C}$ is a linear combination of the basis vectors $|\bar{x}\rangle$). The encoders of Lecture 19 for the Steane and the Shor codes are the case $k = 1$, with $|\bar{0}\rangle, |\bar{1}\rangle$.

## §20.2. Correcting a channel

A codeword $|\psi\rangle \in \mathcal{C}$ is sent through a channel $\mathcal{E}$ acting on the $n$ physical qubits, and a decoding operation $\mathcal{R}$ (that is intended to reverse the effect of the channel $\mathcal{E}$) is then applied to the channel output; that is, the aim of applying the CPTP map $\mathcal{R}$ is to get back $|\psi\rangle$:




**DEFINITION.** *Let $\mathcal{E} : \mathbb{C}^{2^n\times 2^n} \to \mathbb{C}^{2^n\times 2^n}$ be a quantum channel. We say that a code $\mathcal{C}$* corrects *the quantum channel $\mathcal{E}$ if there exists a CPTP map $\mathcal{R} : \mathbb{C}^{2^n\times 2^n} \to \mathbb{C}^{2^n\times 2^n}$ such that*

$$\mathcal{R}\big(\mathcal{E}(|\psi\rangle\langle\psi|)\big) = |\psi\rangle\langle\psi|, \quad \textit{i.e.,} \quad \mathcal{R}\circ\mathcal{E}\big(|\psi\rangle\langle\psi|\big) = |\psi\rangle\langle\psi|,$$

*for all $|\psi\rangle \in \mathcal{C}$.*

Note that a single recovery $\mathcal{R}$ must work for every codeword, since the codeword sent through the channel is unknown to the decoder (of course, the decoder knows that $|\psi\rangle \in \mathcal{C}$). Further, since $\mathcal{R}$ is a CPTP map, it is a quantum channel and hence physically realizable (Lecture 14).

**Towards a criterion for correcting the channel.** We would like to identify a necessary and sufficient criterion for a code to correct a quantum channel which can later be used to design quantum error correcting codes. We now move in this direction.

Suppose

$$\mathcal{E}(N) = \sum_j E_j N E_j^\dagger, \qquad \sum_j E_j^\dagger E_j = I,$$

is a Kraus form of $\mathcal{E}$. Suppose $\mathcal{C}$ corrects $\mathcal{E}$ with the recovery $\mathcal{R}$, and fix a codeword $|\psi\rangle \in \mathcal{C}$. We have

$$\begin{aligned}
|\psi\rangle\langle\psi| &= \mathcal{R}\Big[\sum_j E_j|\psi\rangle\langle\psi|E_j^\dagger\Big] \\
&= \sum_j \mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) \\
&= \sum_{j:\, E_j|\psi\rangle\neq 0} \mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) \\
&= \sum_{j:\, E_j|\psi\rangle\neq 0} \|E_j|\psi\rangle\|^2\, \mathcal{R}\Big(\frac{E_j|\psi\rangle\langle\psi|E_j^\dagger}{\|E_j|\psi\rangle\|\,\|E_j|\psi\rangle\|}\Big).
\end{aligned}$$

The second equality uses the linearity of $\mathcal{R}$, and the third drops the terms with $E_j|\psi\rangle = 0$, which contribute $\mathcal{R}(0) = 0$. For each $j$ with $E_j|\psi\rangle \neq 0$, define

$$p_j := \|E_j|\psi\rangle\|^2 > 0 \qquad \text{and} \qquad \sigma_j := \frac{E_j|\psi\rangle\langle\psi|E_j^\dagger}{\|E_j|\psi\rangle\|^2}.$$

Here $\sigma_j$ is a density operator: it is the density operator of the pure state $E_j|\psi\rangle/\|E_j|\psi\rangle\|$. Further, by completeness,

$$\sum_j \|E_j|\psi\rangle\|^2 = \sum_j \langle\psi|E_j^\dagger E_j|\psi\rangle = \langle\psi\,|\,\psi\rangle = 1,$$

so $\{p_j\}$ is a probability distribution. (This is the ensemble at the output of a channel with a pure state input, see Lecture 16.) Since $\mathcal{R}$ is CPTP, $\rho_j := \mathcal{R}(\sigma_j)$ is also a density operator. Therefore

$$|\psi\rangle\langle\psi| = \sum_{j:\, p_j \neq 0} p_j \rho_j,$$

where each $\rho_j$ is a density operator.

**CLAIM.** *Let $|\psi\rangle$ be a unit vector, let $\rho_1, \ldots, \rho_m$ be density operators and let $p_1, \ldots, p_m > 0$ with $\sum_j p_j = 1$. If $|\psi\rangle\langle\psi| = \sum_j p_j \rho_j$, then $\rho_j = |\psi\rangle\langle\psi|$ for every $j$.*

*Proof.* This proof was not done during the lecture. Let $\rho_j = \sum_k \lambda_{jk} |v_{jk}\rangle\langle v_{jk}|$ be a spectral decomposition, with $\lambda_{jk} \geq 0$ since $\rho_j \geq 0$. Then

$$|\psi\rangle\langle\psi| = \sum_{j,k} |a_{jk}\rangle\langle a_{jk}|, \qquad |a_{jk}\rangle := \sqrt{p_j \lambda_{jk}}\, |v_{jk}\rangle.$$

By the proportionality claim of Lecture 15 (§15.2), $|a_{jk}\rangle = \alpha_{jk}|\psi\rangle$ for some scalars $\alpha_{jk} \in \mathbb{C}$. Hence, for each $j$,

$$p_j \rho_j = \sum_k |a_{jk}\rangle\langle a_{jk}| = \Big(\sum_k |\alpha_{jk}|^2\Big) |\psi\rangle\langle\psi|,$$

i.e., $\rho_j = c_j |\psi\rangle\langle\psi|$ for the constant $c_j := \sum_k |\alpha_{jk}|^2 / p_j$. Taking the trace on both sides, $1 = \mathrm{Tr}(\rho_j) = c_j \langle\psi \,|\, \psi\rangle = c_j$. ∎

Applying the claim, $\mathcal{R}(\sigma_j) = |\psi\rangle\langle\psi|$, that is,

$$\mathcal{R}\Big(\frac{E_j|\psi\rangle\langle\psi|E_j^\dagger}{\||E_j|\psi\rangle\|^2}\Big) = |\psi\rangle\langle\psi|$$

for every $j$ with $E_j|\psi\rangle \neq 0$. Using the linearity of $\mathcal{R}$,

$$\mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) = \||E_j|\psi\rangle\|^2\, |\psi\rangle\langle\psi|,$$

which also holds trivially when $E_j|\psi\rangle = 0$ (both sides are 0). Or equivalently,

$$\mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) \propto |\psi\rangle\langle\psi|,$$

where the proportionality constant is allowed to be 0. That is, the recovery must map *every* member of the ensemble produced by the channel back to the codeword $|\psi\rangle$. The converse also holds, and we have the following equivalent condition.

**THEOREM.** *Let $\{E_j\}$ be the Kraus operators of a quantum channel $\mathcal{E}$. A code $\mathcal{C}$ corrects $\mathcal{E}$ if and only if there exists a CPTP map $\mathcal{R}$ such that*

$$\mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) \propto |\psi\rangle\langle\psi|$$

*for all $j = 1, 2, \ldots$ and all $|\psi\rangle \in \mathcal{C}$.*

*Proof.* ($\Rightarrow$) was shown above. ($\Leftarrow$) This direction was not done during the lecture. Fix $|\psi\rangle \in \mathcal{C}$ and write $\mathcal{R}(E_j|\psi\rangle\langle\psi|E_j^\dagger) = c_j|\psi\rangle\langle\psi|$ for some constants $c_j \in \mathbb{C}$ (which may depend on $|\psi\rangle$). By linearity of $\mathcal{R}$,

$$\mathcal{R} \circ \mathcal{E}\big(|\psi\rangle\langle\psi|\big) = \sum_j \mathcal{R}\big(E_j|\psi\rangle\langle\psi|E_j^\dagger\big) = \Big(\sum_j c_j\Big) |\psi\rangle\langle\psi|.$$

The composition $\mathcal{R} \circ \mathcal{E}$ is trace preserving, so taking the trace of both sides gives $1 = \sum_j c_j$. Hence $\mathcal{R} \circ \mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. ∎

## §20.3. Correcting a collection of errors

The condition in the theorem refers to each Kraus operator $E_j$ separately, and not to the channel $\mathcal{E}$ as a whole.

We will now provide a definition of when a code $\mathcal{C}$ corrects a set of errors $S_e$. Here, $S_e$ is a collection of operators of size $2^n \times 2^n$. The operators in the set $S_e$ need not satisfy the completeness condition, and in fact, the set $S_e$ need not even be finite. $S_e$ can simply be any set of operators. We would like to see if the code can correct *any* error in $S_e$ using a common decoding circuit.

What does it mean for an error from $S_e$ to occur? Let $|\psi\rangle \in \mathcal{C}$ be a codeword stored in a register, and say this register is exposed to some error $E \in S_e$. What we mean is that the state of the register is changed to

$$|\psi\rangle \mapsto \frac{E|\psi\rangle}{\|E|\psi\rangle\|},$$

assuming that $E|\psi\rangle \neq 0$. If $E|\psi\rangle = 0$, this event occurs with zero probability and hence we need not consider correcting this error. We would like to promise the existence of a decoding circuit or CPTP map $\mathcal{R}$ that reverses the effect of any of these errors. This is the motivation for the following definition.

**DEFINITION.** *Suppose $S_e \subseteq \mathbb{C}^{2^n \times 2^n}$. We say that a code $\mathcal{C}$* corrects the collection of errors *$S_e$ if there exists a CPTP map $\mathcal{R}$ such that*

$$\mathcal{R}\big(E|\psi\rangle\langle\psi|E^\dagger\big) \propto |\psi\rangle\langle\psi|$$

*for all $E \in S_e$ and all $|\psi\rangle \in \mathcal{C}$.*

Again, the same decoder $\mathcal{R}$ must work for every error $E \in S_e$ and every codeword $|\psi\rangle \in \mathcal{C}$. This constraint ensures that the decoder can do its job without knowing which error (from among $S_e$) occurred and which codeword $|\psi\rangle$ (from among $\mathcal{C}$) was exposed to the error.

For example, the phase-flip code of Lecture 18 corrects $S_e = \{III, ZII, IZI, IIZ\}$: the recovery measures $M_1 = XXI$ and $M_2 = IXX$ and applies the error identified by the syndrome, so that $\mathcal{R}(E|\psi\rangle\langle\psi|E^\dagger) = |\psi\rangle\langle\psi|$ for every $E \in S_e$.

REMARK (1). *The definition of 'correcting a set of errors' includes the definition of 'correcting a channel' as a special case. Suppose $\mathcal{E}$ is a channel with Kraus operators $\{E_j\}$. Then, use $S_e = \{E_j\}$. With this choice of $S_e$, we immediately see that the two definitions coincide, i.e., the following two statements are equivalent:*

- *$\mathcal{C}$ corrects the quantum channel $\mathcal{E}$ with Kraus operators $\{E_j\}$,*
- *$\mathcal{C}$ corrects the set of errors $S_e = \{E_j\}$.*

REMARK (2). *As we will soon see, if a code can correct a channel $\mathcal{E}$ with Kraus operators $\{E_j\}$, it can correct even the linear combinations of these Kraus operators. So, sometimes, we will work in a situation where we have identified an error set $S_e$ that is larger than $\{E_j\}$, that is, $\{E_j\} \subset S_e$. For such situations, we have: if $\{E_j\} \subset S_e$, then*

$$\mathcal{C} \text{ corrects } S_e \implies \mathcal{C} \text{ corrects the channel } \mathcal{E}.$$

*Indeed, the recovery $\mathcal{R}$ that corrects $S_e$ satisfies $\mathcal{R}(E_j|\psi\rangle\langle\psi|E_j^\dagger) \propto |\psi\rangle\langle\psi|$ for every $j$ and every $|\psi\rangle \in \mathcal{C}$ (since $E_j \in S_e$), and the theorem above applies.*

REMARK (3). *Suppose a code $\mathcal{C}$ corrects a set of errors $S_e$, and let $E_0 \in S_e$. Then the code $\mathcal{C}$ corrects*

$$S_e \cup \big\{\alpha_0 E_0 : \alpha_0 \in \mathbb{C}\big\}.$$

*Proof.* We know that $\mathcal{C}$ corrects $S_e$. This implies that there exists a CPTP map $\mathcal{R}$ such that

$$\mathcal{R}\big(E|\psi\rangle\langle\psi|E^\dagger\big) \propto |\psi\rangle\langle\psi| \quad \text{for all } |\psi\rangle \in \mathcal{C} \text{ and all } E \in S_e.$$

In particular, $\mathcal{R}(E_0|\psi\rangle\langle\psi|E_0^\dagger) \propto |\psi\rangle\langle\psi|$ since $E_0 \in S_e$. Using $(\alpha_0 E_0)^\dagger = \alpha_0^* E_0^\dagger$ and the linearity of $\mathcal{R}$,

$$\mathcal{R}\big(\alpha_0 E_0|\psi\rangle\langle\psi|\alpha_0^* E_0^\dagger\big) = |\alpha_0|^2\,\mathcal{R}\big(E_0|\psi\rangle\langle\psi|E_0^\dagger\big) \propto |\psi\rangle\langle\psi|.$$

So the same $\mathcal{R}$ corrects every error in $S_e \cup \{\alpha_0 E_0 : \alpha_0 \in \mathbb{C}\}$. ■

The above remark is also evident from the following argument. If the error $E_0$ occurs, then the codeword is modified as

$$|\psi\rangle \mapsto \frac{E_0|\psi\rangle}{\|E_0|\psi\rangle\|}.$$

We have been promised that the decoder $\mathcal{R}$ maps this pure state back to $|\psi\rangle$. If instead of $E_0$, say the error $\alpha_0 E_0$ occurred (for $\alpha_0 \neq 0$) then the codeword is modified as

$$|\psi\rangle \mapsto \frac{\alpha_0 E_0|\psi\rangle}{\|\alpha_0 E_0|\psi\rangle\|} = \frac{\alpha_0}{|\alpha_0|} \cdot \frac{E_0|\psi\rangle}{\|E_0|\psi\rangle\|} = \frac{E_0|\psi\rangle}{\|E_0|\psi\rangle\|} \text{ up to global phase.}$$

We already know that when this state is fed into the decoder $\mathcal{R}$ we get $|\psi\rangle$ as the output of the decoder. Hence, clearly, the same decoder $\mathcal{R}$ can decode the error $\alpha_0 E_0$ as well.

Combining Remarks (2) and (3): the channel of Lecture 18, with Kraus operators $\sqrt{p_0}\,III$, $\sqrt{p_1}\,ZII$, $\sqrt{p_2}\,IZI$, $\sqrt{p_3}\,IIZ$, is corrected by the phase-flip code, since each Kraus operator is a scalar multiple of an error in $\{III, ZII, IZI, IIZ\}$.

## §20.4. Correcting linear combinations of errors

*Objective.* If $E_1$ and $E_2$ are correctable, can we correct $E_1 + E_2$ as well? More generally, can we correct $\alpha_1 E_1 + \alpha_2 E_2$ where $\alpha_1, \alpha_2 \in \mathbb{C}$? Remark (3) answers this for a single scalar multiple $\alpha_0 E_0$; here we ask about sums of different errors. The technique we will use to prove that the answer is yes involves the Stinespring dilation of the decoder. We will look at this in Lecture 21. Right now, we will see an example to convince ourselves that a linear combination of two correctable errors is indeed correctable.

EXAMPLE. *Consider the 3-qubit phase-flip code. We know that $\mathcal{C}$ can correct $\{I, Z_1, Z_2, Z_3\}$, where $I = I \otimes I \otimes I$ and $Z_1 = Z \otimes I \otimes I$, $Z_2 = I \otimes Z \otimes I$, $Z_3 = I \otimes I \otimes Z$. Let's see if $\mathcal{C}$ can correct*

$$E_\theta := \cos\theta\, I + i \sin\theta\, Z_1, \qquad \theta \in \mathbb{R}.$$

**What is this error?** Writing $c = \cos\theta$ and $s = \sin\theta$,

$$\begin{aligned}
E_\theta &= (\cos\theta\, I) \otimes I \otimes I + (i \sin\theta\, Z) \otimes I \otimes I \\
&= (\cos\theta\, I + i \sin\theta\, Z) \otimes I \otimes I \\
&= \left( \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} + \begin{bmatrix} is & 0 \\ 0 & -is \end{bmatrix} \right) \otimes I \otimes I \\
&= \begin{bmatrix} c + is & 0 \\ 0 & c - is \end{bmatrix} \otimes I \otimes I \\
&= \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix} \otimes I \otimes I.
\end{aligned}$$

So $E_\theta$ is a unitary that changes the relative phase between $|0\rangle$ and $|1\rangle$ of the first qubit by $2\theta$. As $\theta$ varies, this is a continuous family of errors. We will show that the 3-qubit code can correct all these errors (infinitely many of them!).

**The setting.** Recall the 3-qubit code from Lectures 17 and 18: the codewords are

$$|\psi\rangle = \alpha|+++\rangle + \beta|---\rangle.$$

We explored two decoding circuits for this code: one with a single projective measurement with 4 classical outcomes, and one with two measurements (each with two classical outcomes). We will consider the first decoder now (although the argument holds for the second decoder as well). Consider the four subspaces (corresponding to the four possible projection operators of the projective measurement)

$$S_0 := \mathcal{C} = \text{span}\{|+++\rangle, |---\rangle\}, \quad S_1 := \text{span}\{|-++\rangle, |+--\rangle\},$$
$$S_2 := \text{span}\{|+-+\rangle, |-+-\rangle\}, \qquad S_3 := \text{span}\{|++-\rangle, |--+\rangle\}$$

of $\mathbb{C}^8$. They are pairwise orthogonal, with $Z_\ell|\psi\rangle \in S_\ell$ for $\ell = 1, 2, 3$ (Lecture 17). Let $P_\ell$ be the orthogonal projection onto $S_\ell$. Since the four 2-dimensional subspaces are pairwise orthogonal and $4 \times 2 = 8$, we have $P_0 + P_1 + P_2 + P_3 = I$ and $P_\ell P_m = 0$ for $\ell \neq m$, so $\{P_0, P_1, P_2, P_3\}$ is a projective measurement (Lecture 11). How do we correct? Use a measurement with the four projections $P_0, P_1, P_2, P_3$ followed by a recovery gate controlled by the outcome. Labelling the four classical outcomes $0, 1, 2, 3$, we apply the recovery as follows:

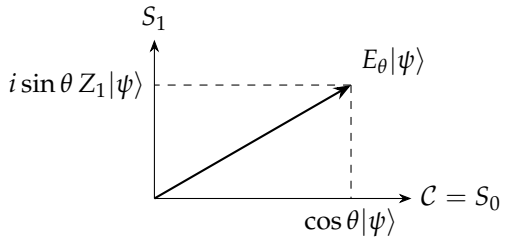
$$\begin{aligned}
0 &\to \text{ apply unitary } I \\
1 &\to \text{ apply unitary } (Z \otimes I \otimes I)^{-1} = Z \otimes I \otimes I \\
2 &\to \text{ apply unitary } (I \otimes Z \otimes I)^{-1} = I \otimes Z \otimes I \\
3 &\to \text{ apply unitary } (I \otimes I \otimes Z)^{-1} = I \otimes I \otimes Z.
\end{aligned}$$

We will now see that this *same* decoder (call it $\mathcal{R}$) corrects the error $E_\theta$ as well.

**Diagnosis.** If $E_\theta$ is the error, the output of the channel is

$$E_\theta|\psi\rangle = (\cos\theta\, I + i \sin\theta\, Z_1)|\psi\rangle = \underbrace{\cos\theta|\psi\rangle}_{\in \mathcal{C}} + \underbrace{i \sin\theta\, Z_1|\psi\rangle}_{\in S_1}.$$

Since $\mathcal{C}$ and $S_1$ are orthogonal subspaces, these two components are perpendicular:




(This is only a schematic picture of complex vectors.)

We now apply the projective measurement (with 4 classical outcomes) on $E_\theta|\psi\rangle$. Measuring with $\{P_0, P_1, P_2, P_3\}$ yields the probability of the outcomes as $\|P_\ell E_\theta|\psi\rangle\|^2$ (Lecture 11) computed as follows

$$\begin{aligned}
P_0\big(\cos\theta|\psi\rangle + i\sin\theta\, Z_1|\psi\rangle\big) &= \cos\theta|\psi\rangle, && \text{probability } \cos^2\theta, \\
P_1\big(\cos\theta|\psi\rangle + i\sin\theta\, Z_1|\psi\rangle\big) &= i\sin\theta\, Z_1|\psi\rangle, && \text{probability } \sin^2\theta, \\
P_2\big(\cos\theta|\psi\rangle + i\sin\theta\, Z_1|\psi\rangle\big) &= 0, && \text{probability } 0, \\
P_3\big(\cos\theta|\psi\rangle + i\sin\theta\, Z_1|\psi\rangle\big) &= 0, && \text{probability } 0,
\end{aligned}$$

where we used $\||\psi\rangle\| = \|Z_1|\psi\rangle\| = 1$. The outcome of the projective measurement is therefore:

- with probability $\cos^2\theta$, the post-measurement state is

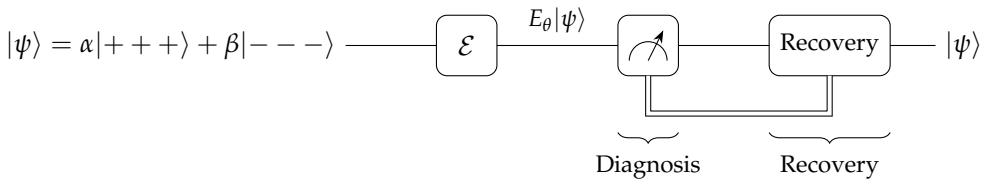
$$\frac{\cos\theta|\psi\rangle}{\|\cos\theta|\psi\rangle\|} = \pm|\psi\rangle = |\psi\rangle \text{ up to global phase;}$$

- with probability $\sin^2\theta$, the post-measurement state is

$$\frac{i\sin\theta\, Z_1|\psi\rangle}{\|i\sin\theta\, Z_1|\psi\rangle\|} = \pm i\, Z_1|\psi\rangle = Z_1|\psi\rangle \text{ up to global phase.}$$

Thus the measurement turns the continuous error $E_\theta$ into either no error (with probability $\cos^2\theta$) or the Pauli error $Z_1$ (with probability $\sin^2\theta$), and the classical outcome tells us which one of these two occurred during the measurement.

**Recovery.** The full procedure is shown below.




The recovery applies the same gates as in Lectures 17 and 18:

| Probability | Outcome $\ell$ | Gate applied |
|---|---|---|
| $\cos^2\theta$ | 0 | $I$ |
| $\sin^2\theta$ | 1 | $Z_1$ |
| 0 | 2 | $Z_2$ |
| 0 | 3 | $Z_3$ |

With outcome 0 the state is already $|\psi\rangle$, and with outcome 1 the gate $Z_1$ maps $Z_1|\psi\rangle$ to $Z_1^2|\psi\rangle = |\psi\rangle$. Hence the codeword is recovered in both cases.

We can also check this directly against the definition of §20.3. The recovery is a measurement with classical control, so it is the CPTP map (Lecture 13)

$$\mathcal{R}(\rho) = \sum_{\ell=0}^{3} U_\ell P_\ell\, \rho\, P_\ell U_\ell^\dagger, \qquad U_0 = I,\ U_1 = Z_1,\ U_2 = Z_2,\ U_3 = Z_3.$$

From the computation above, $U_0P_0E_\theta|\psi\rangle = \cos\theta|\psi\rangle$, $U_1P_1E_\theta|\psi\rangle = Z_1(i\sin\theta\, Z_1|\psi\rangle) = i\sin\theta|\psi\rangle$, and the other two terms vanish. Therefore

$$\mathcal{R}\big(E_\theta|\psi\rangle\langle\psi|E_\theta^\dagger\big) = \cos^2\theta\,|\psi\rangle\langle\psi| + \sin^2\theta\,|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|.$$

Since the same $\mathcal{R}$ also corrects $I, Z_1, Z_2, Z_3$, the phase-flip code corrects $\{I, Z_1, Z_2, Z_3, E_\theta\}$ for every $\theta \in \mathbb{R}$, even though $E_\theta = \cos\theta\, I + i\sin\theta\, Z_1$ is a linear combination of $I$ and $Z_1$ that is not, in general, a scalar multiple of either.

REMARK. *This example illustrates a general principle, the linearity of quantum error correction (Chapter 2 of Gottesman's book): if a code corrects a collection of errors $S_e$, then it also corrects every linear combination of the errors in $S_e$, using the same recovery (we prove this in Lecture 21).*

## §20.5. Summary

We now list the important points from this lecture.

1. *Occurrence/application of an error.* If $E \in \mathbb{C}^{2^n \times 2^n}$ is any operator and $|\psi\rangle \in \mathcal{C}$ is any codeword, when we say that an *error $E$ occurs* or *error $E$ is applied on* $|\psi\rangle$ we mean that the state $|\psi\rangle$ is transformed as
$$|\psi\rangle \mapsto \frac{E|\psi\rangle}{\|E|\psi\rangle\|}.$$
The errors $E$ and $\alpha E$ (for any non-zero scalar $\alpha$) have the same effect on $|\psi\rangle$ (since global phase can be ignored).

2. *Effect of a quantum channel.* A quantum channel $\mathcal{E}$, with Kraus operators $\{E_j\}$ has the following effect on the codeword $|\psi\rangle$: it creates an ensemble
$$\left\{ \left( \|E_j|\psi\rangle\|^2, \frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|} \right) \right\}_{j:\, E_j|\psi\rangle \neq 0}$$
that is, it applies one of the Kraus operators $E_j$ at random to produce
$$|\psi\rangle \mapsto \frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|}, \text{ with probability } \|E_j|\psi\rangle\|^2.$$

3. *Definition: correcting a set $S_e$ of errors.* We say that a code $\mathcal{C}$ corrects $S_e$ if there is a CPTP map $\mathcal{R}$ that undoes the effect of any of the errors $E \in S_e$ for all codewords $|\psi\rangle \in \mathcal{C}$, i.e.,
$$\mathcal{R}\left(E|\psi\rangle\langle\psi|E^\dagger\right) \propto |\psi\rangle\langle\psi| \text{ for all } E \in S_e, |\psi\rangle \in \mathcal{C}.$$
The trace-preserving property of $\mathcal{R}$ implies that, whenever $E|\psi\rangle \neq 0$, this proportionality condition is the same as the condition
$$\mathcal{R}\left(\frac{E|\psi\rangle\langle\psi|E^\dagger}{\|E|\psi\rangle\|^2}\right) = |\psi\rangle\langle\psi|.$$

4. *Definition: correcting a channel $\mathcal{E}$.* A code $\mathcal{C}$ corrects a quantum channel $\mathcal{E}$ if there exists a CPTP map $\mathcal{R}$ such that $\mathcal{R} \circ \mathcal{E}$ acts as the identity super-operator whenever the channel input is a codeword $|\psi\rangle \in \mathcal{C}$, that is, $\mathcal{R}$ reverses $\mathcal{E}$ for all codewords.

   We saw that $\mathcal{C}$ corrects the channel $\mathcal{E}$ if and only if $\mathcal{C}$ corrects the set of Kraus operators $\{E_j\}$ of this channel, that is, with $S_e = \{E_j\}$, $\mathcal{C}$ corrects the error set $S_e$.

5. A code can correct an infinitely large set of errors. We saw two pieces of evidence of this:

   - A correctable set $S_e$ of errors can be enlarged by appending any scalar multiple of any error $E_0 \in S_e$.
   - The 3-qubit phase-flip code that we know to correct $\{I, Z_1, Z_2, Z_3\}$ can correct (without any modifications to the decoder circuit),
   $$\{I, Z_1, Z_2, Z_3\} \cup \{E_\theta : 0 \leq \theta < 2\pi\}.$$
   There are even more errors that this code can correct (such as linear combinations of $I$ and $Z_2$, and so on).

# *Lecture 21*

These notes are based on Chapter 2 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. In Lecture 20 we saw an example in which the 3-qubit phase-flip code corrects a linear combination of two errors that it is known to correct, and we stated that this is an instance of a general principle. In this lecture we prove this principle—known as *linearity of error correction* or *discretization of errors*—using the Stinespring dilation of the decoder (Lecture 15). This is achieved as a byproduct of our journey towards the main goal: is there a usable set of conditions that allow us to determine if a quantum error correcting code $C$ corrects a set of errors $S_e$. This set of conditions is called the *Knill–Laflamme* criteria. We will prove Knill–Laflamme in the next lecture.

## §21.1. Recap

Throughout, $\mathcal{C}$ is an $((n, 2^k))$ code, i.e., a $2^k$-dimensional subspace of $\mathbb{C}^{2^n}$. The codewords are the pure states $|\psi\rangle \in \mathcal{C}$, i.e., the vectors $|\psi\rangle \in \mathcal{C}$ with $\||\psi\rangle\| = 1$.

**Errors.** An *error*, or *error operator*, is any operator $E \in \mathbb{C}^{2^n \times 2^n}$. Note that, in general, $E$ need not have any further structure—it need not be unitary or Hermitian, or the set of errors $S_e$ need not satisfy completeness condition. When the error $E$ acts on a state $|\psi\rangle$, the state changes as

$$|\psi\rangle \mapsto \frac{E|\psi\rangle}{\|E|\psi\rangle\|},$$

assuming $E|\psi\rangle \neq 0$.

**Channels.** A quantum channel $\mathcal{E}$ with Kraus operators $\{E_j\}$ acts on a pure state as

$$\mathcal{E}\left(|\psi\rangle\langle\psi|\right) = \sum_j E_j|\psi\rangle\langle\psi|E_j^\dagger,$$

which is the density operator of the ensemble

$$\left\{ \left( \|E_j|\psi\rangle\|^2,\ \frac{E_j|\psi\rangle}{\|E_j|\psi\rangle\|} \right) \right\}_{j:\, E_j|\psi\rangle \neq 0}.$$

That is, the channel applies the error $E_j$ on the state $|\psi\rangle$ with probability $\|E_j|\psi\rangle\|^2$ (Lectures 16 and 20).

**Correcting a collection of errors.** Let $S_e \subseteq \mathbb{C}^{2^n \times 2^n}$ be a collection of errors. The code $\mathcal{C}$ corrects $S_e$ if there exists a CPTP map $\mathcal{R}$ such that

$$\mathcal{R}\left( \frac{E|\psi\rangle\langle\psi|E^\dagger}{\|E|\psi\rangle\|^2} \right) = |\psi\rangle\langle\psi| \quad \text{for all } |\psi\rangle \in \mathcal{C} \text{ and all } E \in S_e \text{ with } E|\psi\rangle \neq 0. \tag{$*$}$$

As we saw in Lecture 20, this is the same as requiring that there exists a CPTP map $\mathcal{R}$ such that

$$\mathcal{R}\left(E|\psi\rangle\langle\psi|E^\dagger\right) \propto |\psi\rangle\langle\psi| \quad \text{for all } E \in S_e \text{ and all } |\psi\rangle \in \mathcal{C}. \tag{$**$}$$

(Condition $(*)$ implies $(**)$ by linearity of $\mathcal{R}$, with proportionality constant $\|E|\psi\rangle\|^2$, which is 0 when $E|\psi\rangle = 0$. Conversely, if $E|\psi\rangle \neq 0$ and $\mathcal{R}(E|\psi\rangle\langle\psi|E^\dagger) = c|\psi\rangle\langle\psi|$, then taking traces and using that $\mathcal{R}$ is trace preserving gives $c = \|E|\psi\rangle\|^2$, which is $(*)$.)

## §21.2. Using the Stinespring dilation

*Basic question.* When does $\mathcal{C}$ correct $S_e$? By definition, $\mathcal{C}$ corrects $S_e$ if and only if there exists a CPTP map $\mathcal{R}$ for which $(*)$ holds. We need a mathematically workable equivalent condition, for instance, something that a computer program can check: we feed the computer program an orthonormal basis for $\mathcal{C}$ (to describe the quantum code) and the set of errors $S_e$, and the program tells us if $\mathcal{C}$ can indeed correct $S_e$. A solution can be found via two possible routes:

- use the Kraus form of the CPTP map $\mathcal{R}$ (as done in Nielsen and Chuang), or
- use the Stinespring dilation version of $\mathcal{R}$ (Gottesman's book).

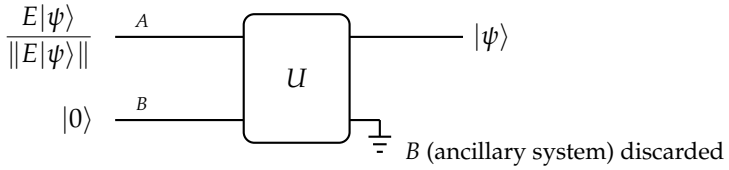
We will take the Stinespring option.

**The decoder as a unitary.** The decoder $\mathcal{R}$ maps $\mathbb{C}^{2^n \times 2^n}$ to itself, so by Lecture 15 (the case $d_1 = d_2 = d$, with $d = 2^n$) it has a Stinespring representation: there is an ancillary system $B$ and a unitary $U$ acting on the composite register $AB$, where $A$ is the register of $n$ qubits holding the code, such that

$$\mathcal{R}(\rho) = \mathrm{Tr}_B\left[U(\rho \otimes |0\rangle\langle 0|)U^\dagger\right] \quad \text{for all } \rho \in \mathbb{C}^{2^n \times 2^n}.$$

The RHS above is the Stinespring form of the decoder $\mathcal{R}$.

Now suppose the code $\mathcal{C}$ corrects $S_e$. We know that for any $|\psi\rangle \in \mathcal{C}$ and any error $E \in S_e$, the noisy version of $|\psi\rangle$, which is $E|\psi\rangle / \|E|\psi\rangle\|$, is correctable by $\mathcal{R}$. Pictorially, for an error $E \in S_e$ and a codeword $|\psi\rangle \in \mathcal{C}$ with $E|\psi\rangle \neq 0$, condition $(*)$ says:




Now,

$$|\Phi\rangle := U\left(\frac{E|\psi\rangle}{\|E|\psi\rangle\|} \otimes |0\rangle\right)$$

is a pure state on the composite register $AB$ (it is a unit vector, since $U$ is unitary). Further, tracing out $B$ gives the pure state $|\psi\rangle\langle\psi|$ on $A$. By Lecture 9 (Schmidt decomposition), a pure state on $AB$ whose reduced state on $A$ is pure has Schmidt rank $r = 1$, and hence it is a product state: $|\Phi\rangle = |a\rangle \otimes |b\rangle$ for unit vectors $|a\rangle, |b\rangle$. Its reduced state on $A$ is $|a\rangle\langle a|$, and this must equal $|\psi\rangle\langle\psi|$; hence $|a\rangle = e^{i\theta}|\psi\rangle$ for some $\theta \in \mathbb{R}$. Absorbing the phase into the second factor,

$$U\left(\frac{E|\psi\rangle}{\|E|\psi\rangle\|} \otimes |0\rangle\right) = |\psi\rangle \otimes |\text{something}\rangle,$$

where $|\text{something}\rangle = e^{i\theta}|b\rangle$ is a unit vector of $B$ that may depend on $E$ and $|\psi\rangle$. Multiplying both sides by $\|E|\psi\rangle\|$ removes the normalization:

$$U\big(E|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |v(E, |\psi\rangle)\rangle,$$

where

$$|v(E, |\psi\rangle)\rangle := \|E|\psi\rangle\| \, |\text{something}\rangle.$$

This holds also when $E|\psi\rangle = 0$, with $|v(E, |\psi\rangle)\rangle := 0$.

REMARK. *The notation $|v(E, |\psi\rangle)\rangle$ means that $|v\rangle$ is a vector (living in the Hilbert space of the register B) and that the value of this vector might depend on both E and $|\psi\rangle$ (for a fixed unitary gate U). Think of $|v\rangle$ as a vector-valued function with the arguments of the function being E and $|\psi\rangle$, and the notation $|v(E, |\psi\rangle)\rangle$ simply reflects this dependence.*

We have proved the ($\Rightarrow$) direction of the following theorem.

**THEOREM** (weak form). *A code $\mathcal{C}$ corrects $S_e$ if and only if there exist an ancillary system $B$ and a unitary $U$ on $AB$ such that*

$$U\left(\frac{E|\psi\rangle}{\|E|\psi\rangle\|}\otimes|0\rangle\right) = |\psi\rangle\otimes|\mathit{something}\rangle,$$

*or equivalently,*

$$U\big(E|\psi\rangle\otimes|0\rangle\big) = |\psi\rangle\otimes|v(E,|\psi\rangle)\rangle, \qquad (***)$$

*for all $E\in S_e$ and all $|\psi\rangle\in\mathcal{C}$ (and for a fixed $U$), where the first form is required only when $E|\psi\rangle\neq 0$. Here $|v(E,|\psi\rangle)\rangle$ is some vector of $B$ that may depend on $E$ and $|\psi\rangle$.*

*Proof.* ($\Rightarrow$) was shown above.

($\Leftarrow$) this was mentioned briefly during the lecture. This result follows immediately from the first equation stated in the theorem. Given the erroneous codeword $E|\psi\rangle/\|E|\psi\rangle\|$ as the input to the Stinespring circuit yields a product state on $AB$, and with $B$ traced out, we immediately obtain the pure state $|\psi\rangle$. Hence, the decoder is successful in correcting the error. ■

REMARK. *In ($***$), the vector $|\psi\rangle$ was intended to be a pure state of $\mathcal{C}$, that is, unit norm vector of the subspace $\mathcal{C}$. But the equation extends to all vectors (irrespective of their norm) by linearity (linearity of $E$, Kronecker product and $U$). Thus, we can assume that the statement of the theorem holds for every $|\psi\rangle\in\mathcal{C}$ whatever be its norm.*

We next prove the strong version of the above theorem, which says that $|v\rangle$ does not depend on $|\psi\rangle$. This is what one should expect from the product form at the unitary gate's output, let's see why. Suppose $|v\rangle$ depended on $|\psi\rangle$, that is, for some suitable fixed error $E$, varying $|\psi\rangle$ changes the value of $|v\rangle$. This would then mean that there is correlation in the quantum information $|\psi\rangle$ and $|v\rangle$ at the output of the unitary, hinting at entanglement. Such a correlation or entanglement can not exist exactly because $A$ and $B$ are in a product state. We will now prove this rigorously.

**The ancilla vector does not depend on the codeword.** We now show that $|v(E,|\psi\rangle)\rangle$ does not depend on $|\psi\rangle$ at all. We will assume that $k\geq 1$, i.e., $2^k\geq 2$, which is the practically relevant case.

Assume $\mathcal{C}$ corrects $S_e$, and let $U$ be as in ($***$). Fix $E\in S_e$. Pick any orthonormal basis $\{|\phi_1\rangle,|\phi_2\rangle,\ldots,|\phi_{2^k}\rangle\}$ of $\mathcal{C}$. Using ($***$) with $|\phi_1\rangle$, $|\phi_2\rangle$ and $|\phi_1\rangle+|\phi_2\rangle$,

$$\begin{aligned}
U\big(E|\phi_1\rangle\otimes|0\rangle\big) &= |\phi_1\rangle\otimes|v(E,|\phi_1\rangle)\rangle,\\
U\big(E|\phi_2\rangle\otimes|0\rangle\big) &= |\phi_2\rangle\otimes|v(E,|\phi_2\rangle)\rangle,\\
U\big(E(|\phi_1\rangle+|\phi_2\rangle)\otimes|0\rangle\big) &= \big(|\phi_1\rangle+|\phi_2\rangle\big)\otimes|v(E,|\phi_1\rangle+|\phi_2\rangle)\rangle.
\end{aligned}$$

Here $|v(E,|\phi_1\rangle)\rangle$ is a vector-valued function of $E$ and $|\phi_1\rangle$, and $|v(E,|\phi_1\rangle+|\phi_2\rangle)\rangle$ is some vector that depends on $E$ and $|\phi_1\rangle+|\phi_2\rangle$. On the other hand, the map $|\chi\rangle\mapsto U(E|\chi\rangle\otimes|0\rangle)$ is linear, so by linearity the left-hand side of the third equation is the sum of the left-hand sides of the first two. Therefore

$$\begin{aligned}
\big(|\phi_1\rangle+|\phi_2\rangle\big)\otimes|v(E,|\phi_1\rangle+|\phi_2\rangle)\rangle &= U\big(E|\phi_1\rangle\otimes|0\rangle\big)+U\big(E|\phi_2\rangle\otimes|0\rangle\big)\\
&= |\phi_1\rangle\otimes|v(E,|\phi_1\rangle)\rangle+|\phi_2\rangle\otimes|v(E,|\phi_2\rangle)\rangle.
\end{aligned}$$

Premultiplying both sides by $\langle\phi_1|\otimes I$ and using $\langle\phi_1\,|\,\phi_1\rangle=1$, $\langle\phi_1\,|\,\phi_2\rangle=0$,

$$|v(E,|\phi_1\rangle+|\phi_2\rangle)\rangle = |v(E,|\phi_1\rangle)\rangle.$$

Premultiplying both sides by $\langle\phi_2| \otimes I$ instead,

$$|v(E, |\phi_1\rangle + |\phi_2\rangle)\rangle = |v(E, |\phi_2\rangle)\rangle.$$

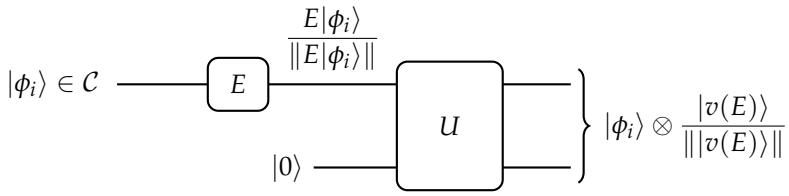
Hence

$$|v(E, |\phi_1\rangle)\rangle = |v(E, |\phi_2\rangle)\rangle.$$

In the same way (using $|\phi_i\rangle + |\phi_j\rangle$ in place of $|\phi_1\rangle + |\phi_2\rangle$), for all $E \in S_e$ and all $i, j = 1, \ldots, 2^k$,

$$|v(E, |\phi_i\rangle)\rangle = |v(E, |\phi_j\rangle)\rangle.$$

Call this common vector $|v(E)\rangle$. Pictorially, for a fixed error $E$ (with $E|\phi_i\rangle \neq 0$), the state of the ancilla at the output does not depend on $i$:




So far we have

$$U\big(E|\phi_i\rangle \otimes |0\rangle\big) = |\phi_i\rangle \otimes |v(E)\rangle \quad \text{for all } i = 1, \ldots, 2^k \text{ and all } E \in S_e.$$

This only covers the cases where the codeword $|\psi\rangle$ is one of the orthonormal basis vectors $|\phi_i\rangle$. We use linearity to generalize to every $|\psi\rangle \in \mathcal{C}$ (including vectors with norm other than 1). Now pick any $|\psi\rangle \in \mathcal{C}$ and expand it in the basis: $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle$. Then

$$\begin{aligned} U\big(E|\psi\rangle \otimes |0\rangle\big) &= U\Big(E\Big(\sum_i \alpha_i |\phi_i\rangle\Big) \otimes |0\rangle\Big) \\ &= \sum_i \alpha_i \, U\big(E|\phi_i\rangle \otimes |0\rangle\big) \\ &= \sum_i \alpha_i |\phi_i\rangle \otimes |v(E)\rangle \\ &= |\psi\rangle \otimes |v(E)\rangle. \end{aligned}$$

This proves the ($\Rightarrow$) direction of the following stronger form of the theorem; the proof for the ($\Leftarrow$) direction is exactly same as the the ($\Leftarrow$) direction proof of the weak form of the theorem.

**THEOREM** (strong form). *A code $\mathcal{C}$ corrects $S_e$ if and only if there exist an ancillary system $B$ and a unitary $U$ on $AB$ such that, for all $E \in S_e$ and all $|\psi\rangle \in \mathcal{C}$,*

$$U\big(E|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |v(E)\rangle,$$

*where the vector $|v(E)\rangle$ of $B$ does not change if we change $|\psi\rangle$.*

In words: the decoder's unitary moves all of the effect of the error $E$ into the ancillary system (which is going to be traced out), and the ancilla's final state $|v(E)\rangle$ carries information only about the error $E$, and none about the codeword $|\psi\rangle$. So the state $|v(E)\rangle$ that is being discarded does not contain any useful information related to $|\psi\rangle$, and is therefore, irrelevant to us.

REMARK. *Under some restrictions on the set $S_e$ and the code $C$, it is possible to perform a measurement on $|v(E)\rangle$ to precisely identify the error operator $E$. This was the situation with two of the quantum code examples from the previous lectures (Steane code and the 3-qubit phase-flip code). Thus, $|v(E)\rangle$ can act as a syndrome.*

## §21.3. Corollaries

**Linearity of error correction.** We can now prove the claim made at the end of Lecture 20.

**COROLLARY.** *Suppose $\mathcal{C}$ corrects $S_e$, and let $E_1, E_2 \in S_e$. Then $\mathcal{C}$ corrects*

$$S_e \cup \{\alpha_1 E_1 + \alpha_2 E_2 : \alpha_1, \alpha_2 \in \mathbb{C}\}.$$

*Proof.* Since $\mathcal{C}$ corrects $S_e$, by the strong form of the theorem there exist an ancilla and a unitary $U$ such that

$$U\big(E_1|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |v(E_1)\rangle$$

and

$$U\big(E_2|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |v(E_2)\rangle$$

for all $|\psi\rangle \in \mathcal{C}$ (and similarly for every other error in $S_e$). Multiplying the first equation by $\alpha_1$ and the second by $\alpha_2$, and using the linearity of $U$ and of the tensor product,

$$U\big(\alpha_1 E_1|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes \alpha_1|v(E_1)\rangle$$

and

$$U\big(\alpha_2 E_2|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes \alpha_2|v(E_2)\rangle.$$

Adding these two equations,

$$U\big((\alpha_1 E_1 + \alpha_2 E_2)|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes \big(\alpha_1|v(E_1)\rangle + \alpha_2|v(E_2)\rangle\big).$$

Thus the same $U$ satisfies $(***)$ for every error in $S_e \cup \{\alpha_1 E_1 + \alpha_2 E_2 : \alpha_1, \alpha_2 \in \mathbb{C}\}$, and the weak/strong form of the theorem shows that $\mathcal{C}$ corrects this larger set. ∎

So the linear combinations are corrected by the *same* decoder, as we observed for the phase-flip code in Lecture 20.

REMARK. *Incidentally, the above proof shows the linearity of the ancilla register too: tracking the same steps in the proof we immediately see that*

$$|v(\alpha_1 E_1 + \alpha_2 E_2)\rangle = \alpha_1|v(E_1)\rangle + \alpha_2|v(E_2)\rangle,$$

*that is $|v\rangle$ is a linear function of $E$.*

**COROLLARY.** *The following are equivalent:*

*(i) $\mathcal{C}$ corrects $S_e$;*

*(ii) $\mathcal{C}$ corrects* $\mathrm{span}(S_e)$*;*

*(iii) $\mathcal{C}$ corrects a basis of* $\mathrm{span}(S_e)$.

*Proof.* The proofs were mentioned orally during the lecture. First note that if $\mathcal{C}$ corrects a set $S$, then it corrects every subset $S' \subseteq S$, using the same decoder.

(i)⇒(ii): Let $U$ be as in the strong form of the theorem. Every $F \in \mathrm{span}(S_e)$ is a finite linear combination $F = \sum_a \alpha_a E_a$ with $E_a \in S_e$, and exactly as in the previous proof,

$$U\big(F|\psi\rangle \otimes |0\rangle\big) = \sum_a \alpha_a |\psi\rangle \otimes |v(E_a)\rangle = |\psi\rangle \otimes \Big(\sum_a \alpha_a |v(E_a)\rangle\Big)$$

for all $|\psi\rangle \in \mathcal{C}$. By the weak/strong form of the theorem, $\mathcal{C}$ corrects $\mathrm{span}(S_e)$.

(ii)⇒(iii) and (ii)⇒(i): $S_e$ and any basis of $\mathrm{span}(S_e)$ are subsets of $\mathrm{span}(S_e)$.

(iii)⇒(ii): if $\mathcal{C}$ corrects a basis of $\mathrm{span}(S_e)$, by linearity of error correction, $\mathcal{C}$ corrects every linear combination of this basis, which is precisely $\mathrm{span}(S_e)$. ∎

REMARK. *Here, by* span *we mean all possible (finite) linear combinations* $\sum_a \alpha_a E_a$ *of operators* $E_a \in S_e$*; we are not referring to row or column spans of individual matrices* $E_a$*. We think of* $E_a \in S_e$ *as 'vectors' in the vector space* $\mathbb{C}^{2^n \times 2^n}$ *and consider the linear combinations of such 'vectors'.*

For example, the phase-flip code of Lecture 18 corrects the set $\{I, Z_1, Z_2, Z_3\}$. Hence, it corrects all of span$\{I, Z_1, Z_2, Z_3\}$,

$$\{\alpha_0 I + \alpha_1 Z_1 + \alpha_2 Z_2 + \alpha_3 Z_3 : \alpha_0, \ldots, \alpha_3 \in \mathbb{C}\}$$

which contains the errors of Lecture 20,

$$E_\theta = \cos\theta\, I + i \sin\theta\, Z_1, \qquad \theta \in \mathbb{R}.$$

Since span$(S_e)$ is a subspace of $\mathbb{C}^{2^n \times 2^n}$, which has dimension $4^n$, any basis of span$(S_e)$ has at most $4^n$ elements. Hence, without loss of generality, we can assume that

(1) $|S_e|$ is finite, and

(2) $S_e$ contains linearly independent operators (that is, no operator in $S_e$ is a linear combination of other operators in $S_e$).

## §21.4. The Knill–Laflamme conditions

With some more effort we can transform the strong form of the theorem into a set of conditions that involves only the errors and the orthonormal basis of code, and not the unitary operator used in the Stinespring version. This is the essence of the corollary below. The converse of the following corollary holds true as well, but the proof is slightly more involved. The forward and reverse directions of this corollary, put together, is known as the Knill–Laflamme criterion. We will prove this in the next lecture, first the forward direction (the below corollary) and then the reverse.

**COROLLARY.** *Without loss of generality let* $S_e = \{E_1, \ldots, E_m\}$ *be finite, and let* $\{|\phi_1\rangle, \ldots, |\phi_{2^k}\rangle\}$ *be an orthonormal basis of* $\mathcal{C}$*.*

$$\mathcal{C} \text{ corrects } S_e \Rightarrow \langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \delta_{i,j}\, \gamma_{a,b}$$

*for all* $i, j = 1, \ldots, 2^k$ *and all* $a, b = 1, \ldots, m$*, where* $\Gamma = [\gamma_{a,b}]$ *is some* $|S_e| \times |S_e|$ *matrix (that does not depend on* $i, j$*).*

Note that, with the indexing of the errors (using $a, b$) and the orthonormal basis of code (using $i, j$) as done in the statement of the corollary, we might expect

$$\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle$$

to depend on $a, b, i, j$ in an arbitrary manner. However, when $\mathcal{C}$ corrects $S_e$, we see a 'product' structure with two factors: the first $\delta_{i,j}$ depends only on the codewords $|\phi_i\rangle$ and $|\phi_j\rangle$, and the second $\gamma_{a,b}$ depends only on the errors $E_a$ and $E_b$. This reflects the product form of the decoder output (before tracing out $B$), where the state of the first register depends only on the codeword and the second register depends only on the error.

Also, note that $\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle$ is the inner product between (the unnormalized versions of) two erroneous codewords: $E_a|\phi_i\rangle$ and $E_b|\phi_j\rangle$ (with possibly different codewords, and possibly different errors).

# *Lecture 22*

These notes are based on Chapter 2 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. In Lecture 21 we used the Stinespring dilation of the decoder to obtain the strong form of the error-correction theorem, and we stated (without proof) a necessary condition for a code to correct a set of errors. In this lecture we prove this condition, prove its converse, and thereby obtain the *Knill–Laflamme conditions*: a necessary and sufficient condition for a code $\mathcal{C}$ to correct a set of errors $S_e$, expressed purely in terms of the errors and an orthonormal basis of $\mathcal{C}$. The major advantage of the Knill–Laflamme conditions over the earlier strong theorem is that they give us a set of concrete conditions that completely bypass the question of the existence of a suitable unitary gate ($U$) and an appropriate ancillary system ($B$). Finally, we begin the study of codes that correct errors on up to $t$ qubits.

## §22.1. Recap

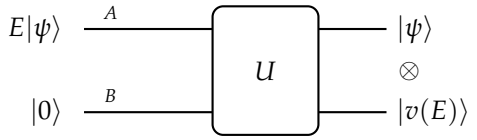
Throughout, $\mathcal{C}$ is an $((n, 2^k))$ code, i.e., a $2^k$-dimensional subspace of $\mathbb{C}^{2^n}$, and $S_e \subseteq \mathbb{C}^{2^n \times 2^n}$ is a collection of errors. As we saw in Lecture 21, we may assume without loss of generality that $S_e = \{E_1, \dots, E_m\}$ is finite. The register holding the codeword (or its noisy version) is $A$.

**THEOREM** (strong form, Lecture 21)**.** *$\mathcal{C}$ corrects $S_e$ if and only if there exist an ancillary system $B$ and a unitary $U$ on $AB$ such that*

$$U\big(E|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |v(E)\rangle \quad \textit{for all } E \in S_e \textit{ and all } |\psi\rangle \in \mathcal{C}, \tag{22.1}$$

*where the vector $|v(E)\rangle$ of $B$ depends on $E$ but not on $|\psi\rangle$.*

Pictorially, the decoder's unitary takes the erroneous codeword to a product state, whose first factor is the codeword and whose second factor depends only on the error:




## §22.2. The Knill–Laflamme conditions

Let $\{|\phi_1\rangle, \dots, |\phi_{2^k}\rangle\}$ be an orthonormal basis of $\mathcal{C}$.

**The forward direction.** We first prove the corollary stated at the end of Lecture 21.

**COROLLARY.** *If $\mathcal{C}$ corrects $S_e = \{E_1, \dots, E_m\}$, then*

$$\langle\phi_i|E_a^\dagger E_b|\phi_j\rangle = \delta_{i,j}\,\gamma_{a,b} \quad \textit{for all } i, j \in \{1, \dots, 2^k\} \textit{ and all } a, b \in \{1, \dots, m\},$$

*where the constants $\gamma_{a,b} \in \mathbb{C}$ do not depend on $i, j$.*

REMARK. *We use the notation $\gamma_{a,b}$ and $\gamma(E_a^\dagger E_b)$ interchangeably (see the remark after the proof).*

*Proof.* Assume $\mathcal{C}$ corrects $S_e$. By the strong form of the theorem, (22.1) holds; in particular,

$$E_a|\phi_i\rangle \otimes |0\rangle \xrightarrow{U} |\phi_i\rangle \otimes |v(E_a)\rangle$$

and

$$E_b|\phi_j\rangle \otimes |0\rangle \xrightarrow{U} |\phi_j\rangle \otimes |v(E_b)\rangle.$$

A unitary preserves inner products. Therefore the inner product of the two left-hand sides equals the inner product of the two right-hand sides:

$$\langle \phi_i|E_a^\dagger E_b|\phi_j\rangle \cdot \langle 0\,|\,0\rangle = \langle \phi_i\,|\,\phi_j\rangle \cdot \langle v(E_a)\,|\,v(E_b)\rangle.$$

Since $\langle 0\,|\,0\rangle = 1$ and $\langle \phi_i\,|\,\phi_j\rangle = \delta_{i,j}$, the claim holds with

$$\gamma_{a,b} := \langle v(E_a)\,|\,v(E_b)\rangle,$$

which depends only on the errors $E_a, E_b$ and not on $i, j$. ■

Since $\langle \phi_i\,|\,\phi_j\rangle = \delta_{i,j}$, the condition can be written in any of the following equivalent ways:

$$\langle \phi_i|E_a^\dagger E_b|\phi_j\rangle = \delta_{i,j}\cdot\gamma_{a,b} = \langle \phi_i\,|\,\phi_j\rangle\cdot\gamma_{a,b} = \langle \phi_i\,|\,\phi_j\rangle\cdot\gamma(E_a^\dagger E_b).$$

REMARK. *The last notation, $\gamma(E_a^\dagger E_b)$, emphasizes that the constant depends only on the operator $E_a^\dagger E_b$. Indeed, setting $i = j = 1$ in the condition gives*

$$\gamma_{a,b} = \langle \phi_1|E_a^\dagger E_b|\phi_1\rangle,$$

*which is a function of the operator $E_a^\dagger E_b$ alone: if two pairs of errors satisfy $E_a^\dagger E_b = E_c^\dagger E_d$, then $\gamma_{a,b} = \gamma_{c,d}$.*

**The converse.** We are now given a code $\mathcal{C}$ with orthonormal basis $\{|\phi_1\rangle, \ldots, |\phi_{2^k}\rangle\}$ and a set of errors $S_e = \{E_1, \ldots, E_m\}$ such that

$$\langle \phi_i|E_a^\dagger E_b|\phi_j\rangle = \langle \phi_i\,|\,\phi_j\rangle\cdot\gamma_{a,b} \quad \text{for all } i,j \text{ and all } a,b. \tag{22.2}$$

We want to show that $\mathcal{C}$ corrects $S_e$. By the strong form of the theorem, it is enough to construct an ancilla $B$ and a unitary $U$ satisfying (22.1). We will need the following fact from linear algebra.

**LEMMA** (key linear algebra fact)**.** *Let $|a_1\rangle, |a_2\rangle, \ldots, |a_L\rangle \in \mathbb{C}^d$ and $|b_1\rangle, |b_2\rangle, \ldots, |b_L\rangle \in \mathbb{C}^d$. If*

$$\langle a_i\,|\,a_j\rangle = \langle b_i\,|\,b_j\rangle \quad \textit{for all } i,j \in \{1,\ldots,L\},$$

*then there exists a unitary $U \in \mathbb{C}^{d\times d}$ such that*

$$U|a_i\rangle = |b_i\rangle \quad \textit{for all } i \in \{1,\ldots,L\}.$$

A proof of this fact is given in the Appendix (§22.4). This lemma replaces the requirement of the existence of a unitary operator with the equality of certain inner products. In our proof of the converse, the Knill–Laflamme conditions will precisely provide the 'equality of inner products' condition and guarantee the existence of a unitary for the Stinespring representation of the decoder.

**THEOREM** (converse)**.** *If* (22.2) *holds, then $\mathcal{C}$ corrects $S_e$.*

*Proof.* We will identify an ancillary system and a unitary (with the help of the above lemma). We will rely on some reverse engineering to characterize the unitary operator.

First, the ancillary system. Pick $B$ to be a register with the same Hilbert space as $A$, i.e., $n$ qubits, and let $|0\rangle \in \mathbb{C}^{2^n}$ denote its all-zero state $|0\cdots 0\rangle$. It is possible to pick an ancillary system with a smaller Hilbert space (dimension at least $\operatorname{rank}(\Gamma)$ is necessary, and dimension $\operatorname{rank}(\Gamma)$ suffices, where $\Gamma = [\gamma_{a,b}]$ is the $m \times m$ matrix of the constants in (22.2);

see the Appendix), but here, for the sake of providing a simple proof, we will use $\mathbb{C}^{2^n}$ for $B$.

We want the unitary $U$ to clean up the noise from the register $A$, i.e., we require the unitary action to have the following form on all possible erroneous basis codewords:

$$\begin{aligned}
E_1|\phi_1\rangle \otimes |0\rangle &\longmapsto |\phi_1\rangle \otimes _____ \\
&\vdots \\
E_a|\phi_i\rangle \otimes |0\rangle &\longmapsto |\phi_i\rangle \otimes _____ \\
&\vdots \\
E_b|\phi_j\rangle \otimes |0\rangle &\longmapsto |\phi_j\rangle \otimes _____ \\
&\vdots \\
E_m|\phi_{2^k}\rangle \otimes |0\rangle &\longmapsto |\phi_{2^k}\rangle \otimes _____
\end{aligned}$$

Consider $E_a|\phi_i\rangle \otimes |0\rangle$. The effect of the error operator $E_a$ has to be pushed to the second factor of the Kronecker product, so the vector filling the blank can depend on $E_a$ but not on the index $i$ of the basis codeword. Further, it must be chosen so that inner products on the input side equal the corresponding inner products on the output side. We will choose this vector to be $E_a|\phi_1\rangle$ no matter what the index $i$ is. This will play the role of $|v(E_a)\rangle$. Thus, we have

$$\begin{aligned}
E_1|\phi_1\rangle \otimes |0\rangle &\longmapsto |\phi_1\rangle \otimes E_1|\phi_1\rangle \\
&\vdots \\
E_a|\phi_i\rangle \otimes |0\rangle &\longmapsto |\phi_i\rangle \otimes E_a|\phi_1\rangle \\
&\vdots \\
E_b|\phi_j\rangle \otimes |0\rangle &\longmapsto |\phi_j\rangle \otimes E_b|\phi_1\rangle \\
&\vdots \\
E_m|\phi_{2^k}\rangle \otimes |0\rangle &\longmapsto |\phi_{2^k}\rangle \otimes E_m|\phi_1\rangle
\end{aligned}$$

for all $a \in \{1, \ldots, m\}$ and $i \in \{1, \ldots, 2^k\}$.

By the key linear algebra fact, such a unitary exists if the inner products on the input and the output sides agree. We check this for any two input vectors, $E_a|\phi_i\rangle \otimes |0\rangle$ and $E_b|\phi_j\rangle \otimes |0\rangle$. On the input side, using (22.2),

$$\begin{aligned}
\text{LHS} &= \big(E_a|\phi_i\rangle \otimes |0\rangle\big)^\dagger \big(E_b|\phi_j\rangle \otimes |0\rangle\big) \\
&= \langle\phi_i|E_a^\dagger E_b|\phi_j\rangle \cdot \langle 0 \,|\, 0\rangle \\
&= \langle\phi_i \,|\, \phi_j\rangle \cdot \gamma_{a,b} \cdot 1.
\end{aligned}$$

On the output side, using (22.2) with $i = j = 1$, i.e., $\langle\phi_1|E_a^\dagger E_b|\phi_1\rangle = \langle\phi_1 \,|\, \phi_1\rangle \cdot \gamma_{a,b} = \gamma_{a,b}$,

$$\begin{aligned}
\text{RHS} &= \big(|\phi_i\rangle \otimes E_a|\phi_1\rangle\big)^\dagger \big(|\phi_j\rangle \otimes E_b|\phi_1\rangle\big) \\
&= \langle\phi_i \,|\, \phi_j\rangle \cdot \langle\phi_1|E_a^\dagger E_b|\phi_1\rangle \\
&= \langle\phi_i \,|\, \phi_j\rangle \cdot \langle\phi_1 \,|\, \phi_1\rangle \cdot \gamma_{a,b} \\
&= \langle\phi_i \,|\, \phi_j\rangle \cdot \gamma_{a,b}.
\end{aligned}$$

So LHS = RHS for all $a, b, i, j$, and by the key linear algebra fact there is a unitary $U$ on $AB$ with

$$U\big(E_a|\phi_i\rangle \otimes |0\rangle\big) = |\phi_i\rangle \otimes |v(E_a)\rangle, \qquad \text{where } |v(E_a)\rangle := E_a|\phi_1\rangle,$$

for all $a$ and $i$. Exactly as in Lecture 21, linearity extends this from the basis vectors to every $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle \in \mathcal{C}$:

$$\begin{aligned} U\big(E_a|\psi\rangle \otimes |0\rangle\big) &= \sum_i \alpha_i \, U\big(E_a|\phi_i\rangle \otimes |0\rangle\big) \\ &= \sum_i \alpha_i |\phi_i\rangle \otimes |v(E_a)\rangle \\ &= |\psi\rangle \otimes |v(E_a)\rangle. \end{aligned}$$

This is (22.1), so by the strong form of the theorem, $\mathcal{C}$ corrects $S_e$. ■

Putting the two directions together, we obtain the main result.

**THEOREM** (Knill–Laflamme conditions)**.** *Let $\{|\phi_1\rangle, \dots, |\phi_{2^k}\rangle\}$ be an orthonormal basis of $\mathcal{C}$. Then $\mathcal{C}$ corrects $S_e = \{E_1, \dots, E_m\}$ if and only if*

$$\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \langle \phi_i \,|\, \phi_j \rangle \cdot \gamma\big(E_a^\dagger E_b\big) \quad \textit{for all } i, j \textit{ and all } a, b,$$

*where $\gamma(E_a^\dagger E_b) \in \mathbb{C}$ is a constant that depends only on $E_a^\dagger E_b$.*

This is exactly the kind of condition we were looking for in Lecture 21: a computer program given an orthonormal basis of $\mathcal{C}$ and the errors $E_1, \dots, E_m$ can check it by computing the finitely many numbers $\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle$. No decoder (Kraus operators or Stinespring unitary) needs to be found.

REMARK. *Such a naive computer-based verification becomes computationally costly even for moderate values of $n$. When the codewords $|\phi_i\rangle$ and the errors are given explicitly as vectors of length $2^n$ and $2^n \times 2^n$ matrices, even storing them, let alone computing the LHS of a single condition, incurs complexity exponential in $n$, no matter what $k$ is. Thus, it is important to design structured codes $\mathcal{C}$ for which we can give theoretical guarantees for error correction without relying on such computer verification.*

**A basis-free version.** There are several equivalent versions of the Knill–Laflamme conditions. Here we state another version that does not depend on the choice of the orthonormal basis of the code space.

**THEOREM** (Knill–Laflamme conditions)**.** *$\mathcal{C}$ corrects $S_e = \{E_1, \dots, E_m\}$ if and only if*

$$\langle \psi | E_a^\dagger E_b | \phi \rangle = \langle \psi \,|\, \phi \rangle \cdot \gamma\big(E_a^\dagger E_b\big) \quad \textit{for all } |\psi\rangle, |\phi\rangle \in \mathcal{C} \textit{ and all } a, b \in \{1, \dots, m\},$$

*where $\gamma(E_a^\dagger E_b) \in \mathbb{C}$ is a constant that depends only on $E_a^\dagger E_b$.*

*Proof.* The proof was discussed verbally during the lecture; here we give the details. By the previous theorem, it is enough to show that the condition above is equivalent to the condition for the orthonormal basis $\{|\phi_i\rangle\}$.

($\Leftarrow$) Take $|\psi\rangle = |\phi_i\rangle$ and $|\phi\rangle = |\phi_j\rangle$.

($\Rightarrow$) Expand $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle$ and $|\phi\rangle = \sum_j \beta_j |\phi_j\rangle$, so that $\langle\psi| = \sum_i \alpha_i^* \langle\phi_i|$. Then

$$\begin{aligned} \langle \psi | E_a^\dagger E_b | \phi \rangle &= \sum_{i,j} \alpha_i^* \beta_j \langle \phi_i | E_a^\dagger E_b | \phi_j \rangle \\ &= \sum_{i,j} \alpha_i^* \beta_j \, \delta_{i,j} \, \gamma\big(E_a^\dagger E_b\big) \\ &= \gamma\big(E_a^\dagger E_b\big) \sum_i \alpha_i^* \beta_i \\ &= \langle \psi \,|\, \phi \rangle \cdot \gamma\big(E_a^\dagger E_b\big). \end{aligned}$$

■

## §22.3. $t$-qubit error correction

We now turn to codes that correct all errors acting on at most $t$ of the $n$ qubits. We first collect some facts about Paulis and their weights.

**Preliminaries.** Recall the single-qubit Paulis $I, X, Y, Z$, with $Y = iXZ$, i.e., $-iY = XZ$ (Lecture 18). The product of any two Paulis is another Pauli times a scalar $\mu \in \{+1, -1, +i, -i\}$. Indeed, $IP = PI = P$ and $PP = I$ for every $P \in \{I, X, Y, Z\}$, and the remaining products are (Lecture 18)

$$XY = iZ = -YX, \qquad YZ = iX = -ZY, \qquad ZX = iY = -XZ.$$

**Products of n-qubit Paulis.** Let $P = P_1 \otimes P_2 \otimes \cdots \otimes P_n$ and $Q = Q_1 \otimes Q_2 \otimes \cdots \otimes Q_n$ be in $\widehat{\mathsf{P}}_n$. By the mixed-product property of the Kronecker product,

$$PQ = P_1Q_1 \otimes P_2Q_2 \otimes \cdots \otimes P_nQ_n.$$

By the preliminaries, $P_iQ_i = \mu_i V_i$ for some $V_i \in \{I, X, Y, Z\}$ and $\mu_i \in \{\pm 1, \pm i\}$. Pulling the scalars out of the Kronecker product,

$$PQ = \mu_1 V_1 \otimes \mu_2 V_2 \otimes \cdots \otimes \mu_n V_n = \Big(\prod_{i=1}^{n} \mu_i\Big)\big(V_1 \otimes V_2 \otimes \cdots \otimes V_n\big),$$

and $\prod_i \mu_i \in \{\pm 1, \pm i\}$, since this set is closed under multiplication. So the product of two $n$-qubit Paulis is again an $n$-qubit Pauli up to a scalar factor:

$$PQ = \mu\, V, \qquad V \in \widehat{\mathsf{P}}_n,\ \mu \in \{\pm 1, \pm i\}.$$

**Weight of a Pauli.** The *weight* of $P = P_1 \otimes \cdots \otimes P_n \in \widehat{\mathsf{P}}_n$ is the number of qubits on which $P$ acts non-trivially:

$$\mathrm{wt}(P) = \mathrm{wt}(P_1 \otimes \cdots \otimes P_n) := \big|\{i : P_i \neq I\}\big|.$$

For instance, $\mathrm{wt}(XIZ) = 2$ and $\mathrm{wt}(III) = 0$. Even when a global phase $\mu \in \{\pm 1, \pm i\}$ is present, i.e., for $\mu V$ with $V \in \widehat{\mathsf{P}}_n$ (an element of Gottesman's $\mathsf{P}_n$, Lecture 18), we define the weight similarly, as the number of qubits on which $\mu V$ acts non-trivially; the phase plays no role:

$$\mathrm{wt}(\mu V) := \mathrm{wt}(V).$$

For instance, $\mathrm{wt}(-i\,XIZ) = \mathrm{wt}(XIZ) = 2$.

**Claim.** *For all $P, Q \in \widehat{\mathsf{P}}_n$, $\mathrm{wt}(PQ) \leq \mathrm{wt}(P) + \mathrm{wt}(Q)$.*

*Proof.* Write $PQ = \mu V$ as above, with $V_i \propto P_iQ_i$. The number of identity factors in $P$ is $n - \mathrm{wt}(P)$, and the number of identity factors in $Q$ is $n - \mathrm{wt}(Q)$. At every position $i$ with $P_i = Q_i = I$ we have $V_i = I$. Among the $n - \mathrm{wt}(P)$ positions where $P_i = I$, at most $\mathrm{wt}(Q)$ have $Q_i \neq I$. Hence

$$\#\{i : V_i = I\} \ \geq\ \big(n - \mathrm{wt}(P)\big) - \mathrm{wt}(Q),$$

and therefore

$$\mathrm{wt}(PQ) = n - \#\{i : V_i = I\} \ \leq\ \mathrm{wt}(P) + \mathrm{wt}(Q).$$

■

**Claim.** *If $V \in \widehat{\mathsf{P}}_n$ has $\mathrm{wt}(V) \leq 2t$, then there exist $P, Q \in \widehat{\mathsf{P}}_n$ such that*

$$V = PQ, \qquad \mathrm{wt}(P) \leq t \quad \textit{and} \quad \mathrm{wt}(Q) \leq t.$$

*Proof.* Let $J := \{i : V_i \neq I\}$, so $|J| = \mathrm{wt}(V) \leq 2t$. Split $J$ into two disjoint sets $J_1, J_2$ with $|J_1| \leq t$ and $|J_2| \leq t$. Define $P$ to agree with $V$ on $J_1$ and $Q$ to agree with $V$ on $J_2$, with identity factors elsewhere:

$$P_i := \begin{cases} V_i, & i \in J_1, \\ I, & \text{otherwise}, \end{cases} \qquad Q_i := \begin{cases} V_i, & i \in J_2, \\ I, & \text{otherwise}. \end{cases}$$

Then $\mathrm{wt}(P) = |J_1| \leq t$ and $\mathrm{wt}(Q) = |J_2| \leq t$. At each position at most one of $P_i, Q_i$ is not the identity, so $P_i Q_i = V_i$ for every $i$, and hence $V = PQ$.

For example, with $t = 2$ and $V = V_1 \otimes V_2 \otimes V_3 \otimes V_4 \otimes I \otimes \cdots \otimes I$ of weight 4 (with $V_1, \ldots, V_4 \neq I$),

$$P = V_1 \otimes V_2 \otimes I \otimes I \otimes I \otimes \cdots \otimes I,$$
$$Q = I \otimes I \otimes V_3 \otimes V_4 \otimes I \otimes \cdots \otimes I.$$

■

## §22.4. Appendix

**Proof of the key linear algebra fact.** We restate the fact: if $|a_1\rangle, \ldots, |a_L\rangle \in \mathbb{C}^d$ and $|b_1\rangle, \ldots, |b_L\rangle \in \mathbb{C}^d$ satisfy $\langle a_i \,|\, a_j \rangle = \langle b_i \,|\, b_j \rangle$ for all $i, j \in \{1, \ldots, L\}$, then there exists a unitary $U \in \mathbb{C}^{d \times d}$ such that $U|a_i\rangle = |b_i\rangle$ for all $i$.

*Proof.* Collect the vectors as the columns of two $d \times L$ matrices (not to be confused with the registers $A$ and $B$ of §22.2):

$$A := \big[\, |a_1\rangle \; |a_2\rangle \; \cdots \; |a_L\rangle \,\big], \qquad B := \big[\, |b_1\rangle \; |b_2\rangle \; \cdots \; |b_L\rangle \,\big].$$

The $(i, j)$-th entry of $A^\dagger A$ is the $i$-th row of $A^\dagger$, which is $\langle a_i|$, times the $j$-th column of $A$, which is $|a_j\rangle$:

$$\big(A^\dagger A\big)_{i,j} = \langle a_i \,|\, a_j \rangle, \qquad \text{and similarly} \qquad \big(B^\dagger B\big)_{i,j} = \langle b_i \,|\, b_j \rangle.$$

So the conditions in the lemma are precisely the same as saying

$$A^\dagger A = B^\dagger B.$$

Rename $C := A^\dagger$ and $D := B^\dagger$. Since $(A^\dagger)^\dagger = A$ and $(B^\dagger)^\dagger = B$, the above equation reads

$$CC^\dagger = DD^\dagger.$$

Both $C$ and $D$ are $L \times d$ matrices; in particular, they have the same number of columns. By fact (2) of Lecture 8 (if $MM^\dagger = NN^\dagger$ and $M$ and $N$ have the same number of columns, then $N = MW$ for some unitary $W$), there is a unitary $V \in \mathbb{C}^{d \times d}$ such that

$$CV = D.$$

Taking the conjugate transpose of both sides,

$$V^\dagger C^\dagger = D^\dagger, \qquad \text{i.e.,} \qquad V^\dagger A = B.$$

Hence

$$UA = B, \qquad \text{where } U := V^\dagger,$$

which is a unitary matrix (since $V$ is unitary, $U^\dagger U = VV^\dagger = I_d$). Comparing the $i$-th columns of $UA$ and $B$, and noting that the $i$-th column of $UA$ is $U$ times the $i$-th column of $A$, we obtain

$$U|a_i\rangle = |b_i\rangle \quad \text{for all } i \in \{1, \ldots, L\}.$$

■

**Dimension of the ancillary system.** In the proof of the converse we took the ancilla $B$ to be $n$ qubits, i.e., $\mathbb{C}^{2^n}$. Here we determine how small $B$ can be. Assume the Knill–Laflamme conditions (22.2) hold, and collect the constants into the $m \times m$ matrix

$$\Gamma := \big[\gamma_{a,b}\big]_{a,b=1}^{m} \in \mathbb{C}^{m\times m}, \qquad r := \operatorname{rank}(\Gamma).$$

**CLAIM.** *(a)* $\Gamma$ *is a positive operator, i.e.,* $\Gamma \geq 0$.

*(b) (Necessity) If an ancillary system* $B$ *and a unitary* $U$ *on* $AB$ *satisfy* (22.1)*, then* $\dim B \geq r$.

*(c) (Sufficiency) There exist an ancillary system* $B$ *with* $\dim B = r$ *and a unitary* $U$ *on* $AB$ *satisfying* (22.1)*. The same holds for any* $\dim B \geq r$.

*Proof.* (a) Let $F$ be the $2^n \times m$ matrix whose $a$-th column is $E_a|\phi_1\rangle$:

$$F := \big[\, E_1|\phi_1\rangle \;\; E_2|\phi_1\rangle \;\; \cdots \;\; E_m|\phi_1\rangle \,\big] \in \mathbb{C}^{2^n\times m}.$$

The $(a,b)$-th entry of $F^\dagger F$ is the $a$-th row of $F^\dagger$, which is $\langle\phi_1|E_a^\dagger$, times the $b$-th column of $F$, which is $E_b|\phi_1\rangle$. Setting $i = j = 1$ in (22.2),

$$\big(F^\dagger F\big)_{a,b} = \langle\phi_1|E_a^\dagger E_b|\phi_1\rangle = \langle\phi_1 \,|\, \phi_1\rangle \cdot \gamma_{a,b} = \gamma_{a,b},$$

so the entries of $\Gamma$ are the inner products between the vectors $E_a|\phi_1\rangle$ and $E_b|\phi_1\rangle$, and

$$\Gamma = F^\dagger F.$$

Hence $\Gamma \geq 0$ by fact (1) of Lecture 8 (a matrix is positive if and only if it is of the form $NN^\dagger$; here $N = F^\dagger$).

(b) Suppose $B$ and $U$ satisfy (22.1). The proof of the forward direction (§22.2) shows that then

$$\gamma_{a,b} = \langle v(E_a) \,|\, v(E_b)\rangle \quad \text{for all } a, b.$$

Let $M$ be the $(\dim B) \times m$ matrix whose $a$-th column is $|v(E_a)\rangle$:

$$M := \big[\, |v(E_1)\rangle \; |v(E_2)\rangle \; \cdots \; |v(E_m)\rangle \,\big].$$

As in the previous subsection, the $(a,b)$-th entry of $M^\dagger M$ is $\langle v(E_a) \,|\, v(E_b)\rangle = \gamma_{a,b}$, so $\Gamma = M^\dagger M$. Therefore

$$r = \operatorname{rank}(\Gamma) = \operatorname{rank}\big(M^\dagger M\big) = \operatorname{rank}(M) \leq \text{number of rows of } M = \dim B.$$

Here we used the fact that $\operatorname{rank}(M^\dagger M) = \operatorname{rank}(M)$ for any matrix $M$.

(c) We use the following linear algebra fact (a refinement of fact (1) of Lecture 8): *if* $\Gamma \in \mathbb{C}^{m\times m}$ *is positive with* $\operatorname{rank}(\Gamma) = r$*, then* $\Gamma = C^\dagger C$ *for some matrix* $C \in \mathbb{C}^{r\times m}$*, i.e.,* $C$ *has exactly* $r$ *rows.*[1] Now let $|c_a\rangle \in \mathbb{C}^r$ denote the $a$-th column of $C$. The $(a,b)$-th entry of $C^\dagger C$ is $\langle c_a \,|\, c_b\rangle$, so

$$\langle c_a \,|\, c_b\rangle = \gamma_{a,b} \quad \text{for all } a, b.$$

Take $B$ to be a system with Hilbert space $\mathbb{C}^r$, let $|0\rangle$ be a fixed unit vector of $\mathbb{C}^r$ (say, its first standard basis vector), and choose $|v(E_a)\rangle$ to be the $a$-th column of $C$:

$$|v(E_a)\rangle := |c_a\rangle, \qquad a = 1, \ldots, m.$$

We now repeat the proof of the converse with this choice. We want a unitary $U$ on $AB$, whose state space is $\mathbb{C}^{2^n} \otimes \mathbb{C}^r$, such that

$$E_a|\phi_i\rangle \otimes |0\rangle \;\longmapsto\; |\phi_i\rangle \otimes |c_a\rangle \quad \text{for all } a \in \{1, \ldots, m\},\ i \in \{1, \ldots, 2^k\}.$$

[1] This can be proved using the spectral decomposition of $\Gamma$.

On the input side, exactly as before, by (22.2),

$$\big(E_a|\phi_i\rangle \otimes |0\rangle\big)^\dagger \big(E_b|\phi_j\rangle \otimes |0\rangle\big) = \langle\phi_i|E_a^\dagger E_b|\phi_j\rangle \cdot \langle 0\,|\,0\rangle = \langle\phi_i\,|\,\phi_j\rangle \cdot \gamma_{a,b}.$$

On the output side,

$$\big(|\phi_i\rangle \otimes |c_a\rangle\big)^\dagger \big(|\phi_j\rangle \otimes |c_b\rangle\big) = \langle\phi_i\,|\,\phi_j\rangle \cdot \langle c_a\,|\,c_b\rangle = \langle\phi_i\,|\,\phi_j\rangle \cdot \gamma_{a,b}.$$

The inner products agree, so by the key linear algebra fact there is a unitary $U$ on $AB$ with $U(E_a|\phi_i\rangle \otimes |0\rangle) = |\phi_i\rangle \otimes |v(E_a)\rangle$ for all $a, i$; by linearity, $U(E_a|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |v(E_a)\rangle$ for all $|\psi\rangle \in \mathcal{C}$, which is (22.1).

For an ancilla of any dimension $\geq r$, the above idea can be readily extended. ■

# *Homework 10*

1. **The Knill–Laflamme condition from Nielsen and Chuang.** As usual, let $S_e = \{E_1, \ldots, E_m\}$ and $\mathcal{C}$ be an $((n, 2^k))$ code with orthonormal basis $\{|\phi_1\rangle, \ldots, |\phi_{2^k}\rangle\}$. Recall the version of Knill–Laflamme we derived during the lectures:

   $$\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \langle \phi_i \,|\, \phi_j \rangle \, \gamma(E_a^\dagger E_b) \;\; \forall i, j, a, b.$$

   Let us now see how Knill–Laflamme is presented in Nielsen and Chuang. For this, define $P$ to be the (orthogonal) projection onto the code space $\mathcal{C}$. The Knill–Laflamme conditions are presented as

   $$P E_a^\dagger E_b P = \gamma(E_a^\dagger E_b)\, P \;\; \forall a, b.$$

   *Questions.*

   (a) Express the projection operator $P$ in terms of $\{|\phi_1\rangle, \ldots, |\phi_{2^k}\rangle\}$.

   (b) Show that the two versions of Knill–Laflamme presented above are equivalent. You must show that the first version implies the second and the second version implies the first.

2. **Short proof of linearity from Knill–Laflamme.** During the lectures we proved linearity of error correction using the Stinespring version of the error correctability conditions. We can derive a short proof of linearity based on Knill–Laflamme.

   Suppose $\mathcal{C}$ corrects $S_e = \{E_1, \ldots, E_m\}$. Let $F = \alpha_1 E_1 + \alpha_2 E_2$ for scalars $\alpha_1, \alpha_2$. Show that $\mathcal{C}$ corrects $\{E_1, \ldots, E_m, F\}$.

   HINT. Assume that Knill–Laflamme conditions hold for $S_e$ (either of the two versions we saw in Lecture 22). Now check Knill–Laflamme for $S_e \cup \{F\}$. For Knill–Laflamme to hold for this larger set of errors, you need to check if there exist *some* constants $\gamma(E_1^\dagger F), \ldots, \gamma(E_m^\dagger F), \gamma(F^\dagger F)$ so that

   $$\begin{aligned} \langle \psi | E_a^\dagger F | \phi \rangle &= \langle \psi \,|\, \phi \rangle \, \gamma(E_a^\dagger F) \;\; \forall a = 1, \ldots, m, \text{ and} \\ \langle \psi | F^\dagger F | \phi \rangle &= \langle \psi \,|\, \phi \rangle \, \gamma(F^\dagger F) \end{aligned}$$

   for all codewords $|\psi\rangle, |\phi\rangle \in \mathcal{C}$.

3. **Correcting errors beyond linear combinations.** We know that the ability to correct both $E_1$ and $E_2$ allows us to correct all linear combinations of these two errors. We might be able to correct more errors even beyond these linear combinations. This question shows one such example.

   Consider a 3-qubit code $\mathcal{C}$ that corrects the following errors

   $$E_1 = |0\rangle\langle 0| \otimes I \otimes I \text{ and } E_2 = |0\rangle\langle 1| \otimes I \otimes I.$$

   *Questions.*

   (a) Using only the linearity of error correction can we show that the code can correct

   $$S_e := \{|0\rangle\langle 0| \otimes I \otimes I, |0\rangle\langle 1| \otimes I \otimes I,\ |1\rangle\langle 0| \otimes I \otimes I,\ |1\rangle\langle 1| \otimes I \otimes I\}?$$

   (b) Use the Knill–Laflamme conditions to show that this code can correct $S_e$.
   HINT. Directly verify the criteria.

(c) Can this code correct $\{F \otimes I \otimes I : F \in \mathbb{C}^{2\times 2}\}$?

4. Suppose a code corrects $\{E_1, \ldots, E_m\}$. Recall that $\Gamma$ is the $m \times m$ matrix whose $(a,b)$-th entry is $\gamma_{a,b} = \gamma(E_a^\dagger E_b)$. Show that

   (a) $\gamma_{b,a} = \gamma_{a,b}^*$ for all $a, b$. That is, $\Gamma$ is a Hermitian matrix.

   (b) $\Gamma$ is a positive matrix.
   HINT. An operator $A$ is positive if and only if it can be expressed as $B^\dagger B$ for some suitable operator $B$.

   (c) $S_e$ is linearly dependent $\Rightarrow$ $\Gamma$ is not invertible.
   HINT. Assume that $\alpha_1 E_1 + \cdots + \alpha_m E_m = 0$ where at least one of $\alpha_1, \ldots, \alpha_m$ is non-zero. Show that either the columns or the rows of $\Gamma$ are linearly dependent.
   REMARK. The contrapositive of this statement is

   $$\Gamma \text{ is invertible } \Rightarrow \; S_e \text{ is linearly independent.}$$

   We use this fact in the definition of non-degeneracy (later in this homework).

5. For the following codes $\mathcal{C}$ and error sets $S_e$, manually verify the Knill–Laflamme conditions and find the matrix $\Gamma$. You can exploit the fact that $\Gamma$ is a Hermitian operator.

   (a) The 3-qubit phase-flip code and the error set $\{|0\rangle\langle 0| \otimes I \otimes I, I \otimes I \otimes I, I \otimes Z \otimes I\}$.
   REMARK. I did not include the error $I \otimes I \otimes Z$ so that you can complete the problem quickly.

   (b) The Shor code and the error set $\{I, X_1, Z_1\}$.

6. Recall that when we say that a code $\mathcal{C}$ corrects an error set $S_e$ we mean that there exists a common decoder (a quantum circuit at the decoder) that can reverse the effect of any of the errors in $S_e$. Now, using the same code but a different decoding circuit could allow us to decode a different set of errors $S_e'$. It is possible that $\mathcal{C}$ can correct $S_e$ and $\mathcal{C}$ can correct $S_e'$, but $\mathcal{C}$ cannot correct $S_e \cup S_e'$ (that is, there is no single common decoder that corrects all the errors in $S_e$ as well as $S_e'$).

   (a) We know that the 3-qubit phase-flip code can correct $S_e = \{I, Z_1, Z_2, Z_3\}$. Show that this code can correct $S_e' = \{ZZZ, IZZ, ZIZ, ZZI\}$.
   REMARK. You must design a decoding algorithm that corrects all errors in $S_e'$. Try modifying the decoding algorithm that corrects $S_e$ (syndrome measurement followed by a recovery gate) so that it can work with $S_e'$.

   (b) Show that this code cannot correct $S_e \cup S_e'$. That is, no matter what decoding algorithm you use it is impossible to correct every error in $S_e \cup S_e'$.
   HINT. Identify two errors $E_a, E_b \in S_e \cup S_e'$ and two orthogonal codewords $|\psi\rangle$ and $|\phi\rangle$ such that the erroneous versions are the same, i.e., $E_a|\psi\rangle = E_b|\phi\rangle$. Use this to show that Knill–Laflamme is not satisfied.
   REMARK. To show that Knill–Laflamme is not satisfied, we need to show that no matter how we choose the constants $\gamma_{a,b} = \gamma(E_a^\dagger E_b)$, the collection of constraints

   $$\langle\psi|E_a^\dagger E_b|\phi\rangle = \langle\psi\,|\,\phi\rangle\,\gamma_{a,b} \;\; \forall a, b, \text{ and } |\psi\rangle, |\phi\rangle \in \mathcal{C}$$

   can not be simultaneously satisfied. For instance, if we show that for some choice of $|\psi\rangle$ and $|\phi\rangle$, the LHS is non-zero while the RHS is zero no matter what $\gamma_{a,b}$ is, our claim is proved.
   REMARK. When $E_a|\psi\rangle = E_b|\phi\rangle$ there is no way for *any* decoder to distinguish which of the following events occurred

   - codeword is $|\psi\rangle$ and the error is $E_a$, or

- codeword is $|\phi\rangle$ and the error is $E_b$.

7. **The quantum Hamming bound.** We will show that if an $((n, 2^k))$ code $\mathcal{C}$ corrects $S_e$ then we can derive an upper bound on the number of logical qubits $k$. For this, we will use the same notation as introduced in the lectures, and three linear algebra facts.

   FACT 1. For any operator $A$, we have $\text{rank}(A) = \text{rank}(A^\dagger A)$.

   FACT 2. $\text{rank}(A)$ is less than or equal to the number of rows in $A$.

   FACT 3. The rank of a block diagonal matrix is the sum of the ranks of the diagonal blocks.

   We will start by assuming that $\mathcal{C}$ corrects $S_e = \{E_1, \ldots, E_m\}$.

   *Questions.*

   (a) Consider all possible $E_a|\phi_i\rangle$ for every choice of $a = 1, \ldots, m$ and $i = 1, \ldots, 2^k$. List them in the following order (from left to right) as the columns of a single matrix $A$.

   $$E_1|\phi_1\rangle,\ E_2|\phi_1\rangle,\ \ldots,\ E_m|\phi_1\rangle,$$
   $$E_1|\phi_2\rangle,\ E_2|\phi_2\rangle,\ \ldots,\ E_m|\phi_2\rangle,$$
   $$\vdots$$
   $$E_1|\phi_{2^k}\rangle,\ E_2|\phi_{2^k}\rangle,\ \ldots,\ E_m|\phi_{2^k}\rangle.$$

   That is, the first $m$ columns of $A$ correspond to $|\phi_1\rangle$, the next $m$ columns correspond to $|\phi_2\rangle$, and so on.

   Express the matrix $A^\dagger A$ in terms of the operator $\Gamma$ encountered in the Knill–Laflamme condition.

   (b) Find the relation between $\text{rank}(A)$ and $\text{rank}(\Gamma)$.

   (c) How many rows does $A$ have?

   (d) Derive an upper bound on $k$ based on all the observations you have made so far.

   (e) We now tune this bound for the *non-degenerate* setting. For this, we assume that the errors in $S_e$ are linearly independent.

   DEFINITION. We say that a code $\mathcal{C}$ for correcting a linearly independent set of errors $S_e$ is *non-degenerate* if it satisfies the Knill–Laflamme conditions (that is, $\mathcal{C}$ corrects $S_e$) and $\text{rank}(\Gamma) = |S_e|$. In the non-degenerate setting $\Gamma$ is invertible. On the other hand, *degeneracy* means $\text{rank}(\Gamma) < |S_e|$.

   REMARK. Non-degeneracy and degeneracy are defined for a pair $(\mathcal{C}, S_e)$ consisting of a code and a linearly independent set of errors. You cannot say that 'a code is non-degenerate' without associating an error set to it. A code that is degenerate with respect to one set of errors could be non-degenerate with respect to another set of errors.

   *Question.* Show that for any non-degenerate pair $(\mathcal{C}, S_e)$ we have

   $$\mathcal{C} \text{ corrects } S_e \ \Rightarrow\ k \leq n - \log_2 |S_e|.$$

   This is called the quantum Hamming bound.

   REMARK. This does not mean that $k = n - \log_2 |S_e|$ is possible. The inequality only says that $k$ will never exceed $n - \log_2 |S_e|$.

   (f) Specialize the quantum Hamming bound (assuming non-degeneracy) to the case where $\mathcal{C}$ corrects all $n$-qubit Paulis of weight at most $t$.

   REMARK. Codes which meet this last bound with equality are called *perfect codes*.

8. **Protecting mixed states from errors.**

   (a) Let us denote the quantum state to be encoded as $|\tilde{\psi}\rangle \in \mathbb{C}^{2^k}$ and the corresponding codeword to be $|\psi\rangle \in \mathbb{C}^{2^n}$. Is there a circuit that takes $|\psi\rangle$ as the input and delivers $|\tilde{\psi}\rangle$?
   REMARK. Recovering $|\psi\rangle$ from errors is equivalent to recovering $|\tilde{\psi}\rangle$ from errors.

   (b) Suppose the state to be encoded is an arbitrary state (pure or mixed) $\tilde{\rho} \in \mathcal{D}(\mathbb{C}^{2^k})$. This is encoded using the standard encoding circuit for an $((n, 2^k))$ quantum code $\mathcal{C}$; denote the resulting state by $\rho \in \mathcal{D}(\mathbb{C}^{2^n})$. Assume that $\mathcal{C}$ corrects the channel $\mathcal{E}$ (recall the definition of this statement from the lectures). You must show that it is possible to retrieve the state $\rho$ from $\mathcal{E}(\rho)$.

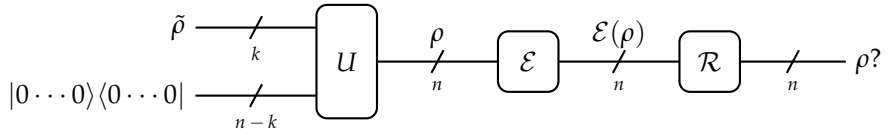


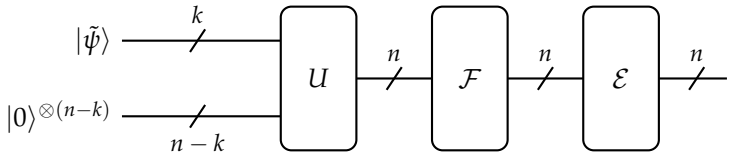

   *Figure.* The state $\tilde{\rho}$ of $k$ logical qubits is encoded (ancillas in $|0\cdots0\rangle$ followed by the encoding unitary $U$) into the $n$-qubit state $\rho$, which then passes through the channel $\mathcal{E}$. You must show that the decoder circuit (the CPTP map $\mathcal{R}$) outputs $\rho$ when its input is $\mathcal{E}(\rho)$.

   (c) Is it possible to retrieve $\tilde{\rho}$ from $\rho$?

9. Let $\mathcal{C}$ be an $((n, 2^k))$ code, and let $\mathcal{E}$ and $\mathcal{F}$ be quantum channels acting on $n$-qubit states. We make no other assumptions on $\mathcal{C}$, $\mathcal{E}$ and $\mathcal{F}$. We will use $\mathcal{E} \circ \mathcal{F}$ to denote the following channel

$$(\mathcal{E} \circ \mathcal{F})(\rho) = \mathcal{E}(\,\mathcal{F}(\rho)\,)$$

   where the state goes through $\mathcal{F}$ first and then through $\mathcal{E}$.



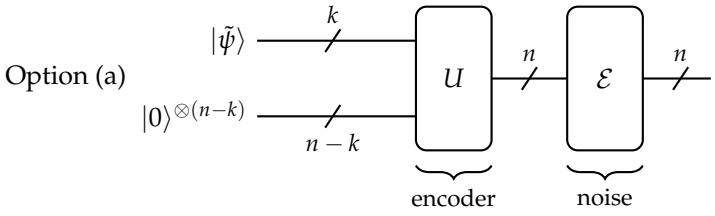

   You must either prove or disprove the following two statements.

   (a) Prove or disprove: $\mathcal{C}$ corrects $\mathcal{E} \circ \mathcal{F} \Rightarrow \mathcal{C}$ corrects $\mathcal{E}$

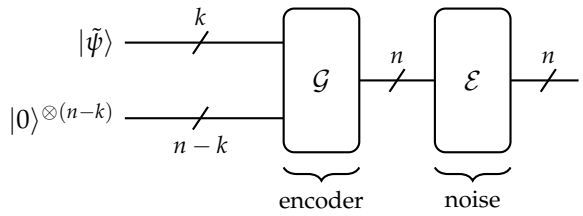
   (b) Prove or disprove: $\mathcal{C}$ corrects $\mathcal{E} \circ \mathcal{F} \Rightarrow \mathcal{C}$ corrects $\mathcal{F}$

10. Suppose we want to protect a $k$-qubit state $|\tilde{\psi}\rangle \in \mathbb{C}^{2^k}$ by mapping it to a state over $n$ qubits to protect against the quantum noise channel $\mathcal{E}$.

    In all our lectures, we used a unitary gate $U$ to encode $|\tilde{\psi}\rangle \otimes |0\cdots0\rangle$ where $|0\cdots0\rangle \in \mathbb{C}^{2^{n-k}}$. However, quantum mechanics allows us to use any CPTP map, that is, we could have chosen to use any CPTP map $\mathcal{G}$ as the encoder instead of restricting ourselves to unitary gates only. These are the two possibilities shown below.



Option (b)




We now ask if encoding using a general CPTP map $\mathcal{G}$ (which may or may not be a unitary gate) allows us to correct a wider class of channels than using a unitary operation $U$. Let's frame this question in another way:

*Question:* if a CPTP encoder $\mathcal{G}$ corrects $\mathcal{E}$ then is there a unitary gate $U$ that corrects $\mathcal{E}$?

Note that we do not have to use the same decoder for both the circuits, the choice of the decoder can depend on what encoder was used. If the answer to the above question is 'yes' then there is no harm in assuming that only unitary gates are used for encoding. Answer this question with a proof.

# *Lecture 23*

These notes are based on Chapter 2 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. In Lecture 22 we proved the Knill–Laflamme conditions and collected some facts about products and weights of $n$-qubit Paulis. In this lecture we use these facts to define $t$-error correcting codes, to translate the Knill–Laflamme conditions into a condition involving only the Paulis of weight at most $2t$, and to define the distance of a code.

Throughout, $\mathcal{C}$ is an $((n, 2^k))$ code with $k \geq 1$, and $\{|\phi_1\rangle, \ldots, |\phi_{2^k}\rangle\}$ is an orthonormal basis of $\mathcal{C}$.

## §23.1. $t$-error correction

**Paulis and their weights.** Recall the set of $n$-qubit Paulis (without phases, Lecture 18)

$$\widehat{\mathsf{P}}_n = \big\{E_1 \otimes E_2 \otimes \cdots \otimes E_n \ : \ E_i \in \{I, X, Y, Z\} \text{ for all } i\big\},$$

which has

$$|\widehat{\mathsf{P}}_n| = 4^n$$

elements, since each of the $n$ factors can be chosen in 4 ways. The weight of a Pauli (Lecture 22) is the number of qubits on which it acts non-trivially:

$$\mathrm{wt}(E_1 \otimes \cdots \otimes E_n) = \big|\{i : E_i \neq I\}\big|.$$

**The set of errors.** We will now focus on a particular choice of error set $S_e$: the collection of all Paulis of weight at most $t$, for some design parameter $t < n/2$. This problem is called *$t$-error correction*. The vast majority of the quantum error correction literature deals with $t$-error correction. Now, let us choose

$$S_e = \big\{E \in \widehat{\mathsf{P}}_n \ : \ \mathrm{wt}(E) \leq t\big\}. \tag{23.1}$$

To count its elements, note that a Pauli of weight exactly $w$ is specified by choosing the $w$ qubits on which it acts non-trivially, in $\binom{n}{w}$ ways, and then one of $X, Y, Z$ on each of these qubits, in $3^w$ ways. Hence

$$|S_e| = 1 + \binom{n}{1} \cdot 3 + \binom{n}{2} \cdot 3^2 + \cdots + \binom{n}{t} \cdot 3^t = \sum_{w=0}^{t} \binom{n}{w} 3^w.$$

If $t \geq n/2$, then only trivial codes (of dimension $2^k = 1$, i.e., $k = 0$) can correct $S_e$; see the Appendix.

Observe that $S_e$ is a linearly independent collection of operators. This follows from the facts that $S_e \subset \widehat{\mathsf{P}}_n$ and that $\widehat{\mathsf{P}}_n$ is a basis for $\mathbb{C}^{2^n \times 2^n}$, and in particular, $\widehat{\mathsf{P}}_n$ is a linearly independent set. Any subset of a linearly independent set is linearly independent.

Every operator in $\widehat{\mathsf{P}}_n$ is Hermitian; thus, every error $E_a \in S_e$ satisfies $E_a^\dagger = E_a$.

**DEFINITION.** *$\mathcal{C}$ is a* $t$-error correcting code *if $\mathcal{C}$ corrects the set $S_e$ in* (23.1).

Note that any $t$-error correcting code is automatically $(t-1)$-error correcting: if a code corrects all Paulis of weight up to $t$, it surely corrects all Paulis of weight up to $(t-1)$. However, a $(t-1)$-error correcting code need not be $t$-error correcting.

In some cases, a $t$-error correcting code corrects some errors with weight more than $t$. For instance, consider a 1-error correcting code that is not 2-error correcting. That is, the code corrects all errors of weight 0 and 1, but it cannot correct all weight-2 errors simultaneously. It is possible that such a code could correct some (not all) weight-2 errors in addition to all errors of weights 0 and 1.

**Examples.**

(1) The Steane code and the Shor code (Lectures 18 and 19) are both 1-error correcting codes: each of them corrects every single-qubit Pauli error in addition to the identity 'error'. Both these codes also correct some errors of weight 2:

- the Steane code can correct an $X$ and a $Z$ even if they appear on distinct qubits.
- the Shor code can correct two $X$'s if they appear on different 'blocks'; for instance, the error $X_1X_4$ is correctable.

Neither of them is a 2-error correcting code, since they cannot correct *all* Pauli errors of weight 2.

(2) The 3-qubit phase-flip code (Lectures 17 and 18) is *not* a 1-error correcting code. It corrects the phase-flip errors and the identity operator, i.e., the error set $\{I, Z_1, Z_2, Z_3\}$, but not the bit flip errors. Consider a bit flip on the first qubit. Since $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$, we have

$$\alpha|+++\rangle + \beta|---\rangle \xrightarrow{X_1} \alpha|+++\rangle - \beta|---\rangle,$$

which is a codeword too. On the other hand, the codeword $\alpha|+++\rangle - \beta|---\rangle$ is left unchanged by the error $I$:

$$\alpha|+++\rangle - \beta|---\rangle \xrightarrow{I} \alpha|+++\rangle - \beta|---\rangle.$$

If $\alpha, \beta \neq 0$, there is no way for any decoder to distinguish between these two cases and take a corrective action:

- the original codeword is $\alpha|+++\rangle + \beta|---\rangle$ and the error is $X_1$, versus
- the original codeword is $\alpha|+++\rangle - \beta|---\rangle$ and the error is $I$.

(3) Suppose $\mathcal{C}$ is 1-error correcting. Then $\mathcal{C}$ also corrects

$$N_1 \otimes I \otimes I \otimes \cdots \otimes I$$

for *any* $N_1 \in \mathbb{C}^{2\times 2}$, not only for $N_1 \in \{I, X, Y, Z\}$. Indeed, $\{I, X, Y, Z\}$ is a basis of $\mathbb{C}^{2\times 2}$ (the case $n = 1$ of the fact that $\widehat{\mathsf{P}}_n$ is a basis of $\mathbb{C}^{2^n\times 2^n}$), so $N_1 = c_0 I + c_1 X + c_2 Y + c_3 Z$ for some $c_0, \ldots, c_3 \in \mathbb{C}$, and expanding,

$$\begin{aligned} N_1 \otimes I \otimes \cdots \otimes I = {} & c_0\, I \otimes I \otimes \cdots \otimes I + c_1\, X \otimes I \otimes \cdots \otimes I \\ & + c_2\, Y \otimes I \otimes \cdots \otimes I + c_3\, Z \otimes I \otimes \cdots \otimes I, \end{aligned}$$

a linear combination of Paulis of weight at most 1, i.e., an element of the span of $S_e$. Similarly, $\mathcal{C}$ also corrects

$$I \otimes N_2 \otimes I \otimes \cdots \otimes I$$

for any $N_2 \in \mathbb{C}^{2\times 2}$, and so on for every qubit position. Since $\mathcal{C}$ corrects the span of $S_e$ (Lecture 21), $\mathcal{C}$ can also correct

$$\alpha_1\, N_1 \otimes I \otimes \cdots \otimes I + \alpha_2\, I \otimes N_2 \otimes I \otimes \cdots \otimes I$$

for any $\alpha_1, \alpha_2 \in \mathbb{C}$, and more generally any linear combination of single-qubit errors on different qubits.

(4) Suppose $\mathcal{C}$ is 2-error correcting, and consider an error acting on the first two qubits,

$$N \otimes \underset{3}{I} \otimes \underset{4}{I} \otimes \cdots \otimes \underset{n-1}{I} \otimes \underset{n}{I} \in \mathbb{C}^{2^n\times 2^n}, \qquad \text{any } N \in \mathbb{C}^{4\times 4},$$

where the labels indicate the qubit positions. Recall that $\widehat{\mathsf{P}}_2$ is a basis of $\mathbb{C}^{4\times 4}$, so $N$ is a linear combination of the 16 operators in $\widehat{\mathsf{P}}_2$. Hence $N \otimes I \otimes \cdots \otimes I$ is a linear combination of the Paulis $P_1 \otimes P_2 \otimes I \otimes \cdots \otimes I$, $P_1, P_2 \in \{I, X, Y, Z\}$, each of which has weight at most 2, and $\mathcal{C}$ corrects it. The same argument applies to any pair of qubit positions. Thus, a 2-error correcting code corrects *any* error acting on 2 or fewer qubits, as well as linear combinations of such errors. More generally, a $t$-error correcting code corrects any error acting on $t$ or fewer qubits.

## §23.2. Applying the Knill–Laflamme conditions to $t$-error correction

The Knill–Laflamme conditions are necessary and sufficient conditions for error correction that hold for any choice of code $\mathcal{C}$ and any choice of error set $S_e \subset \mathbb{C}^{2^n \times 2^n}$. We now specialize these conditions to the problem of $t$-error correction, i.e., when $S_e$ is the set of all Paulis of weight at most $t$.

Suppose we want $\mathcal{C}$ to be $t$-error correcting. By the Knill–Laflamme conditions (Lecture 22), this holds if and only if

$$\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \delta_{i,j} \cdot \gamma_{a,b} \quad \text{for all } i, j \text{ and all } E_a, E_b \in S_e,$$

where $\gamma_{a,b}$ does not depend on $i, j$. For $E_a, E_b$ in the set $S_e$ of (23.1), the operator $E_a^\dagger E_b$ has the following form:

- $E_a^\dagger = E_a$, since every Pauli is Hermitian (Lecture 18);
- hence $E_a^\dagger E_b = E_a E_b = \mu P$ for some $P \in \widehat{\mathsf{P}}_n$ and $\mu \in \{\pm 1, \pm i\}$ (Lecture 22);
- $\mathrm{wt}(P) = \mathrm{wt}(E_a E_b) \leq \mathrm{wt}(E_a) + \mathrm{wt}(E_b) \leq t + t = 2t$ (Lecture 22).

So the Knill–Laflamme conditions for $S_e$ only involve Paulis of weight at most $2t$. This leads to the following theorem.

Observe the role the operator $P$ plays in the theorem below: $P$ is the product (up to a global phase) of *two* errors $E_a$ and $E_b$ that we would like to correct, but $P$ itself need not be a correctable error. Since each of $E_a$ and $E_b$ can have weight at most $t$, we must allow $P$ to have weight up to $2t$.

**THEOREM** (Condition for $t$-error correction)**.** *$\mathcal{C}$ is $t$-error correcting if and only if*

$$\langle \phi_i | P | \phi_j \rangle = \delta_{i,j} \cdot \gamma(P) \quad \textit{for all } i, j \in \{1, \ldots, 2^k\} \textit{ and all } P \in \widehat{\mathsf{P}}_n \textit{ with } \mathrm{wt}(P) \leq 2t, \tag{23.2}$$

*where the constant $\gamma(P) \in \mathbb{C}$ depends only on $P$ and not on $i, j$.*

*Proof.* ($\Leftarrow$) Assume (23.2) holds. To show that $\mathcal{C}$ is $t$-error correcting, we prove that the Knill–Laflamme conditions are satisfied for $S_e$. Let $E_a, E_b \in S_e$. As shown above, $E_a^\dagger E_b = \mu P$ for some $P \in \widehat{\mathsf{P}}_n$ with $\mathrm{wt}(P) \leq 2t$ and some $\mu \in \{\pm 1, \pm i\}$; both $\mu$ and $P$ are determined by $E_a, E_b$ and are independent of $i, j$. Then the left-hand side of the Knill–Laflamme conditions is

$$\begin{aligned} \langle \phi_i | E_a^\dagger E_b | \phi_j \rangle &= \langle \phi_i | \mu P | \phi_j \rangle \\ &= \mu \cdot \langle \phi_i | P | \phi_j \rangle \\ &= \delta_{i,j} \cdot \mu\, \gamma(P), \end{aligned}$$

where the last step uses (23.2), which applies since $\mathrm{wt}(P) \leq 2t$. The constant $\gamma_{a,b} := \mu\, \gamma(P)$ does not depend on $i, j$. Hence the Knill–Laflamme conditions hold, and $\mathcal{C}$ corrects $S_e$.

($\Rightarrow$) Assume $\mathcal{C}$ is $t$-error correcting, i.e., $\mathcal{C}$ corrects $S_e$. By the Knill–Laflamme conditions,

$$\langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \delta_{i,j} \cdot \gamma_{a,b} \quad \text{for all } i, j \text{ and all } E_a, E_b \in S_e,$$

with $\gamma_{a,b}$ independent of $i, j$. Pick any $P \in \widehat{\mathsf{P}}_n$ with $\mathrm{wt}(P) \leq 2t$. By the second claim of Lecture 22, there exist $E_a, E_b \in \widehat{\mathsf{P}}_n$ with weights at most $t$, i.e., $E_a, E_b \in S_e$, such that

$$P = E_a E_b = E_a^\dagger E_b.$$

Therefore

$$\langle \phi_i | P | \phi_j \rangle = \langle \phi_i | E_a^\dagger E_b | \phi_j \rangle = \delta_{i,j} \cdot \gamma_{a,b},$$

which is (23.2) with $\gamma(P) := \gamma_{a,b}$, a constant that is independent of $i, j$. ■

I am now including a restatement of the theorem which was not discussed during the lecture. For every Pauli $P$, define a $2^k \times 2^k$ matrix $\Lambda(P)$ whose $(i, j)$ entry is $\langle \phi_i | P | \phi_j \rangle$. If $P$ satisfies the condition stated in the above theorem, i.e.,

$$\langle \phi_i | P | \phi_j \rangle = \delta_{i,j} \cdot \gamma(P),$$

then the off-diagonal entries of $\Lambda(P)$ are zero, and all the diagonal entries are identical: $\Lambda(P) = \gamma(P) I_{2^k \times 2^k}$, i.e., $\Lambda(P)$ is a *scalar matrix*.

**THEOREM** (Condition for $t$-error correction: restatement)**.** *A code $\mathcal{C}$ is $t$-error correcting if and only if*

$$\Lambda(P) \text{ is a scalar matrix for every Pauli } P \text{ of weight at most } 2t.$$

REMARK. *The choice of the orthonormal basis for the code $\mathcal{C}$ does not affect this $t$-error correction criterion. To see this, if $\{|\psi_i\rangle\}$ is another orthonormal basis, then there exists a unitary $V = [v_{i,j}]_{i,j=1,\ldots,2^k}$ such that*

$$|\psi_j\rangle = \sum_{i=1}^{2^k} v_{i,j} |\phi_i\rangle \ \ \forall j.$$

*The analogue of the matrix $\Lambda(P)$ computed with respect to the new basis $\{|\psi_i\rangle\}$ instead of the original basis $\{|\phi_j\rangle\}$ is*

$$V^\dagger \Lambda(P) V.$$

*It is easy to see that this matrix is a scalar matrix if and only if $\Lambda(P)$ is a scalar matrix.*

Given an orthonormal basis $\{|\phi_1\rangle, |\phi_2\rangle, \ldots\}$ of $\mathcal{C}$, suppose we wish to check whether $\mathcal{C}$ is 1-error correcting. Using the above theorem, we check whether $\Lambda(P)$ is a scalar matrix for every Pauli of weight 0, weight 1 and weight 2. If all these $\Lambda$ matrices are scalar matrices, then $\mathcal{C}$ is indeed 1-error correcting.

For 2-error correction, we need to verify whether $\Lambda(P)$ is scalar for Paulis of weights $0, 1, 2, 3$ and 4.

Suppose we want to identify the largest $t$ such that $\mathcal{C}$ is $t$-error correcting. One way to go about this is to run the verification (that is, whether $\Lambda(P)$ is a scalar matrix) on all Paulis starting from weight 0 and going upwards.[1] That is, for each choice of weight $w$, if we have confirmed that $\Lambda(P)$ is indeed scalar for all Paulis of weight up to $w - 1$, we run the verification for weight $w$, and so on. We then stop at the value of the smallest $w$ for which the verification fails. Denote this smallest weight by $d$ and call this the *distance* of the code $\mathcal{C}$.

**DEFINITION.** *The distance of a code $\mathcal{C}$ is the smallest weight $d$ among all Paulis $P$ such that $\Lambda(P)$ is* not *a scalar matrix.*

[1] This is not a computationally practical way to identify $t$. Instead, coding theorists often design codes in a specific way so that they can exploit the code's algebraic or combinatorial structure to analytically argue that the code is $t$-error correcting.

With $d$ defined as above, if $P$ is any Pauli with $\mathrm{wt}(P) \leq d-1$, we are guaranteed that $\Lambda(P)$ is scalar. Further, there is at least one Pauli $P$ with $\mathrm{wt}(P) = d$ such that $\Lambda(P)$ is not scalar.

Clearly, if $t$ is such that $2t \leq d-1$, then $\Lambda(P)$ is indeed a scalar matrix for every Pauli with weight $2t$ or less, and hence, $\mathcal{C}$ is $t$-error correcting. On the other hand, if $2t \geq d$, then there is at least one Pauli with weight less than or equal to $2t$ (in particular, a Pauli of weight $d$) such that $\Lambda(P)$ is not a scalar matrix. Hence, $\mathcal{C}$ is *not* $t$-error correcting. We state this observation as follows.

**COROLLARY.** *$\mathcal{C}$ is $t$-error correcting if and only if $2t+1 \leq d$.*

The largest $t$ for which $\mathcal{C}$ is $t$-error correcting is

$$\left\lfloor \frac{d-1}{2} \right\rfloor,$$

where $\lfloor \cdot \rfloor$ denotes the 'rounding down' operation.

During the lecture there was a discussion about $d$ representing some form of distance between codewords. I made a mistake in claiming that $d$ is the smallest weight of a Pauli $P$ that maps one codeword to another codeword (not equal up to global phase). This statement is certainly true for the class of stabilizer codes, but it is not true for an arbitrary code. Instead, what is true in general is that $d$ is the smallest weight of a Pauli $P$ such that $P|\phi\rangle$ and $|\psi\rangle$ cannot be reliably distinguished from each other for some pair of orthogonal codewords $|\phi\rangle, |\psi\rangle$. That is, $P$ maps $|\phi\rangle$ to a state that has a non-zero correlation with $|\psi\rangle$, and hence is confusable with $|\psi\rangle$. Note that $P|\phi\rangle$ need not belong to the code space $\mathcal{C}$. See the Appendix for more details.

## §23.3. Appendix

**$n/2$-error correction is impossible.** Assume that $\mathcal{C}$ is any $((n, 2^k))$ code with $k \geq 1$. Let $t$ be any integer with $t \geq n/2$. We want to show that $\mathcal{C}$ is *not* $t$-error correcting.

We will use proof by contradiction. Assume that $\mathcal{C}$ is $t$-error correcting. Then for every Pauli of weight up to $2t$, $\Lambda(P)$ is a scalar matrix. Since $2t \geq n$, and the maximum weight of an $n$-qubit Pauli is $n$, we see that $\Lambda(P)$ is a scalar matrix for every Pauli $P \in \widehat{\mathsf{P}}_n$.

Since $\mathcal{C}$ has dimension $2^k \geq 2$, it has at least two orthonormal codewords, say $|\phi_1\rangle$ and $|\phi_2\rangle$. Then, according to the error correction conditions,

$$\langle \phi_1 | P | \phi_2 \rangle = \langle \phi_1 \,|\, \phi_2 \rangle \gamma(P) = 0$$

for all Paulis $P \in \widehat{\mathsf{P}}_n$. Now consider any operator $N \in \mathbb{C}^{2^n \times 2^n}$, and consider its linear expansion $N = \sum_{P \in \widehat{\mathsf{P}}_n} c_P P$ with respect to the basis $\widehat{\mathsf{P}}_n$, where the scalars $c_P \in \mathbb{C}$. Then

$$\langle \phi_1 | N | \phi_2 \rangle = \sum_P c_P \langle \phi_1 | P | \phi_2 \rangle = \sum_P c_P \times 0 = 0.$$

That is, $\langle \phi_1 | N | \phi_2 \rangle = 0$ for all $N \in \mathbb{C}^{2^n \times 2^n}$.

Now, to see the contradiction, pick $N$ to be any operator with $N|\phi_2\rangle = |\phi_1\rangle$. For this choice of $N$, we have

$$\langle \phi_1 | N | \phi_2 \rangle = \langle \phi_1 \,|\, \phi_1 \rangle = 1 \neq 0.$$

**More about the distance of a code.** We know that two pure states $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2^n}$ can be reliably distinguished if and only if they are orthogonal. Indeed, if they are orthogonal, any projective measurement along an orthonormal basis that includes $|\psi\rangle$ and $|\phi\rangle$ among its basis vectors will correctly identify $|\psi\rangle$ versus $|\phi\rangle$ with probability 1. If these two vectors are not orthogonal, then no measurement can reliably distinguish these two states.

Suppose we are given orthogonal code states $|\psi\rangle, |\phi\rangle \in \mathcal{C}$, that is, $\langle\phi \,|\, \psi\rangle = 0$. Now, suppose we would like to start from $|\phi\rangle$ and perturb this state by applying a Pauli $P \in \widehat{\mathsf{P}}_n$ such that the resulting state $P|\phi\rangle$ is no longer reliably distinguishable from $|\psi\rangle$, i.e.,

$$\langle\psi|P|\phi\rangle \neq 0.$$

The task is to find the Pauli $P$ with the smallest possible weight; in other words, find the smallest number of qubits such that applying $2 \times 2$ Paulis on those qubits makes $|\phi\rangle$ no longer orthogonal to $|\psi\rangle$. This smallest number is precisely the distance of the code $\mathcal{C}$ if we minimize it over all possible pairs of orthogonal codewords $|\psi\rangle$ and $|\phi\rangle$. This is what we will prove now.

First, let us show that applying Paulis on $d-1$ or fewer qubits will not break orthogonality.

**CLAIM.** *Let the distance of the code $\mathcal{C}$ be $d$. Then,*

$$\langle\psi|P|\phi\rangle = \langle\psi \,|\, \phi\rangle\, \gamma(P) \text{ for all Paulis } P \text{ with } \mathrm{wt}(P) \leq d-1 \text{ for all } |\psi\rangle, |\phi\rangle \in \mathcal{C}.$$

*Proof.* From the definition of code distance we already know that the statement of the claim holds if we restrict $|\psi\rangle, |\phi\rangle$ to the orthonormal basis $\{|\phi_j\rangle\}$. We extend this result to all of $\mathcal{C}$ through linearity. If $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle$ and $|\phi\rangle = \sum_i \beta_i |\phi_i\rangle$, then $\langle\psi \,|\, \phi\rangle = \sum_i \alpha_i^* \beta_i$. Now pick any Pauli $P$ with weight at most $d-1$. Then

$$\begin{aligned}
\langle\psi|P|\phi\rangle &= \sum_i \sum_j \alpha_i^* \beta_j \langle\phi_i|P|\phi_j\rangle \\
&= \sum_i \sum_j \alpha_i^* \beta_j \gamma(P) \delta_{i,j} \\
&= \sum_i \alpha_i^* \beta_i \gamma(P) \\
&= \langle\psi \,|\, \phi\rangle \gamma(P).
\end{aligned}$$

■

Thus, if $\langle\psi \,|\, \phi\rangle = 0$ and a Pauli $P$ has weight at most $d-1$, the perturbed state $P|\phi\rangle$ is still orthogonal to $|\psi\rangle$. So to break orthogonality between any two code states we need a Pauli of weight at least $d$.

Now we argue that in the best case, perturbing exactly $d$ qubits of $|\phi\rangle$ can make it non-orthogonal to $|\psi\rangle$.

**CLAIM.** *There exist orthonormal code states $|\psi\rangle$ and $|\phi\rangle$ and a Pauli $P$ of weight $d$ such that $|\psi\rangle$ and $P|\phi\rangle$ are not orthogonal.*

*Proof.* From the definition of the distance we know there exists a Pauli $P$ of weight $d$ such that the condition

$$\langle\phi_i|P|\phi_j\rangle = \delta_{i,j}\, \gamma(P) \;\; \forall i, j$$

fails. This failure could happen in two possible ways:

- for some $i \neq j$, we have $\langle\phi_i|P|\phi_j\rangle \neq 0$, or
- for some $i \neq j$, we have $\langle\phi_i|P|\phi_i\rangle \neq \langle\phi_j|P|\phi_j\rangle$.

In the first case, our claim is proved if we simply pick $|\psi\rangle = |\phi_i\rangle$ and $|\phi\rangle = |\phi_j\rangle$.

Now consider the second case under the assumption that the first case does not hold, i.e., assume that $\langle\phi_i|P|\phi_j\rangle = 0$. Using

$$|\psi\rangle = \frac{|\phi_i\rangle + |\phi_j\rangle}{\sqrt{2}} \text{ and } |\phi\rangle = \frac{|\phi_i\rangle - |\phi_j\rangle}{\sqrt{2}}$$

we have

$$\begin{aligned}\langle\psi|P|\phi\rangle &= \frac{1}{2}\big(\langle\phi_i| + \langle\phi_j|\big)\, P\, \big(|\phi_i\rangle - |\phi_j\rangle\big) \\ &= \frac{1}{2}\Big(\langle\phi_i|P|\phi_i\rangle - \langle\phi_i|P|\phi_j\rangle + \langle\phi_j|P|\phi_i\rangle - \langle\phi_j|P|\phi_j\rangle\Big) \\ &= \frac{1}{2}\Big(\langle\phi_i|P|\phi_i\rangle - \langle\phi_j|P|\phi_j\rangle\Big) \\ &\neq 0.\end{aligned}$$

It is easy to check that $|\psi\rangle$ and $|\phi\rangle$ are orthonormal. ■

We will now combine the results from the last two claims. Towards this, let us use the following definitions.

**DEFINITION.** *States $|\phi\rangle$ and $|\psi\rangle$ are* distinguishable *if they are orthogonal, and* confusable *if they are non-orthogonal.*

We now introduce a notion of distance between two states that are distinguishable.

**DEFINITION.** *The* distance between a pair of distinguishable states $\{|\psi\rangle, |\phi\rangle\}$ *is the smallest weight among all Paulis $P$ such that $\{|\psi\rangle, P|\phi\rangle\}$ is confusable,*

$$\mathsf{dist}(|\psi\rangle, |\phi\rangle) := \min\{\mathrm{wt}(P) \;:\; \langle\psi|P|\phi\rangle \neq 0, P \in \widehat{\mathsf{P}}_n\}.$$

The following result follows immediately from the above claims and definitions.

**THEOREM.** *The distance $d$ of a code $\mathcal{C}$ equals the smallest distance among all pairs of distinguishable codewords, i.e.,*

$$d = \min\{\mathsf{dist}(|\psi\rangle, |\phi\rangle) \;:\; |\psi\rangle, |\phi\rangle \in \mathcal{C},\ \langle\psi\,|\,\psi\rangle = \langle\phi\,|\,\phi\rangle = 1 \text{ and } \langle\psi\,|\,\phi\rangle = 0\}.$$

# *Lecture 24*

These notes are based on Chapter 3 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. We will now study the stabilizer framework for constructing quantum codes.

## §24.1. Stabilizer codes

Stabilizer codes are a family of quantum codes. This family does not include all quantum codes. These codes have a strong algebraic structure, and it is this structure that facilitates their construction and the analysis of their distance, dimension, etc. The vast majority of the quantum codes available in the literature are stabilizer codes.

**Notation.** Recall from Lecture 20 that a quantum code $\mathcal{C} \subset \mathbb{C}^{2^n}$ of dimension $K$ is called an $((n, K))$ code. If, in addition, the distance of $\mathcal{C}$ (Lecture 23) is $d$, we say that $\mathcal{C}$ is an

$$((n, K, d)) \text{ code.}$$

When $K = 2^k$, an arbitrary code is thus an $((n, 2^k, d))$ code, where the second parameter $2^k$ is the dimension of the code space. In general, the dimension $K$ need not be a power of 2.

For a stabilizer code, the dimension of the code space is always a power of 2, i.e., $K = 2^k$ (we will prove this in a later lecture). For such codes we use the notation

$$[\![n, k, d]\!],$$

where the second parameter is $k = \log_2(\dim \mathcal{C})$, the number of logical qubits, rather than the dimension itself. This mirrors the notation $[n, k, d]$ used for classical linear codes. Stabilizer codes are also known as *additive codes* or *symplectic codes*; accordingly, codes that are not stabilizer codes are also called *non-stabilizer codes* or *non-additive codes*.

For example, the phase-flip code of Lecture 18 is a $[\![3, 1]\!]$ code, while the Steane code and the Shor code are $[\![7, 1, 3]\!]$ and $[\![9, 1, 3]\!]$ codes, respectively.

**Stabilizer codes are not always the best.** There are non-stabilizer codes that are better than every stabilizer code with the same length and distance. For instance, there exists a $((9, 12, 3))$ code, whereas the best stabilizer code of length 9 and distance 3 is a $[\![9, 3, 3]\!]$ code, i.e., it has a code space of dimension only $2^3 = 8 < 12$. The non-stabilizer code is large enough to encode the quantum information contained in a 12-level (or any $d$-level with $d \leq 12$) quantum system and protect it against one Pauli error, whereas the stabilizer code can protect quantum systems with at most 8 levels only. Nevertheless, the algebraic structure of stabilizer codes makes them much easier to construct, analyze and design decoding algorithms for.

## §24.2. The Pauli group

**Recall.** In Lecture 18 we defined the set of $n$-qubit Paulis

$$\widehat{\mathsf{P}}_n = \{A_1 \otimes A_2 \otimes \cdots \otimes A_n \ : \ A_i \in \{I, X, Y, Z\}\},$$

and

$$|\widehat{\mathsf{P}}_n| = 4^n.$$

The operators in $\widehat{\mathsf{P}}_n$ possess the following properties.

(1) $A^\dagger = A$, $A^{-1} = A$ and $A^2 = I$, since every operator in $\{I, X, Y, Z\}$ has these properties and they carry forward to $\widehat{\mathsf{P}}_n$ through the Kronecker product (see §18.1 of Lecture 18).

(2) If $A \in \widehat{\mathsf{P}}_n \setminus \{I\}$, then $\mathrm{Tr}(A) = 0$, and the eigenvalues of $A$ are $+1$ and $-1$, each with multiplicity $2^{n-1}$. When $A = I$, all its eigenvalues are $+1$. Thus, for any $A \in \widehat{\mathsf{P}}_n$ all its eigenvalues belong to $\{+1, -1\}$ (see Question 1 of Homework 9).

(3) If $B \in \widehat{\mathsf{P}}_n$ as well, then $AB = \pm BA$ (see §18.1 of Lecture 18).

**The Pauli group.** The set $\widehat{\mathsf{P}}_n$ is not closed under multiplication; for example $X, Z \in \widehat{\mathsf{P}}_1$ but $XZ = -iY \notin \widehat{\mathsf{P}}_1$. The remedy is to allow phases (as in Lecture 18, we follow Gottesman's notation):

$$\mathsf{P}_n \triangleq \{\mu\, A_1 \otimes A_2 \otimes \cdots \otimes A_n \;:\; A_i \in \{I, X, Y, Z\},\ \mu \in \{+1, -1, +i, -i\}\}.$$

The elements of $\mathsf{P}_n$ are called "Paulis with phase", or simply "Paulis". Since there are 4 choices of $\mu$ and $4^n$ choices of $A_1 \otimes \cdots \otimes A_n$,

$$|\mathsf{P}_n| = 4^{n+1}.$$

The set $\mathsf{P}_n$ is closed under matrix multiplication and matrix inverse. To see this, for $A = \mu A_1 \otimes \cdots \otimes A_n$ and $B = \nu B_1 \otimes \cdots \otimes B_n$ in $\mathsf{P}_n$,

$$AB = \mu\nu\,(A_1B_1) \otimes \cdots \otimes (A_nB_n).$$

For each $i$ we know that $A_iB_i = \varepsilon_i C_i$ where $\varepsilon_i \in \{\pm 1, \pm i\}$ and $C_i \in \{I, X, Y, Z\}$. Thus,

$$AB = \left(\mu\nu \prod_i \varepsilon_i\right) C_1 \otimes \cdots \otimes C_n$$

which indeed belongs to $\mathsf{P}_n$. Similarly, we have

$$A^{-1} = \mu^{-1}A_1^{-1} \otimes \cdots \otimes A_n^{-1} = \mu^{-1}A_1 \otimes \cdots \otimes A_n \in \mathsf{P}_n.$$

Together with the associativity of matrix multiplication and the fact that $I \in \mathsf{P}_n$, this says that $\mathsf{P}_n$ is a *group* under matrix multiplication, called the *Pauli group*. Note that $\mathsf{P}_n$ is a *non-commutative group* since it contains operators $A$ and $B$ such that $AB \neq BA$.

**Hermitian and skew-Hermitian Paulis.** Say $A \in \mathsf{P}_n$, i.e., $A = \mu A_1 \otimes A_2 \otimes \cdots \otimes A_n$ with $A_i \in \{I, X, Y, Z\}$. Note that

$$A^\dagger = \mu^* A_1^\dagger \otimes \cdots \otimes A_n^\dagger = \mu^* A_1 \otimes \cdots \otimes A_n.$$

If $\mu = \pm 1$, then $\mu^* = \mu$ and if $\mu = \pm i$, we have $\mu^* = -\mu$. Thus we have

$$A^\dagger = A \text{ if } \mu = \pm 1, \quad A^\dagger = -A \text{ if } \mu = \pm i.$$

Similarly, using the fact $\mu^{-1} = \mu^*$ for all $\mu \in \{\pm 1, \pm i\}$, we have

$$A^{-1} = \mu^{-1}A_1^{-1} \otimes \cdots \otimes A_n^{-1} = \mu^* A_1 \otimes \cdots \otimes A_n = A^\dagger.$$

In summary,

- If $\mu = \pm 1$, then $A^\dagger = A$ and $A^2 = AA^\dagger = AA^{-1} = I$.
  In this case, $A$ is *Hermitian*.
- If $\mu = \pm i$, then $A^\dagger = -A$ and $A^2 = -AA^\dagger = -AA^{-1} = -I$.
  In this case, $A$ is *skew-Hermitian*.

Since all the eigenvalues of $A_1 \otimes \cdots \otimes A_n \in \widehat{\mathsf{P}}_n$ lie in $\{+1, -1\}$, the eigenvalues of $A = \mu(A_1 \otimes \cdots \otimes A_n)$ lie in $\{+\mu, -\mu\}$. Hence

- if $\mu = \pm 1$, all the eigenvalues of $A$ lie in $\{+1, -1\}$, and
- if $\mu = \pm i$, all the eigenvalues of $A$ lie in $\{+i, -i\}$.

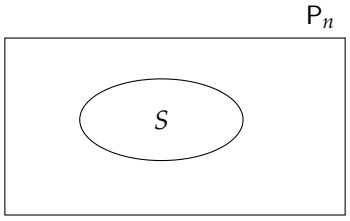
In particular, a skew-Hermitian Pauli does not have $+1$ as an eigenvalue.

Exactly half the operators in $\mathsf{P}_n$ are Hermitian and the other half are skew-Hermitian. We will find it useful to know when the product of two operators from the Hermitian half of $\mathsf{P}_n$ is Hermitian. Suppose $A, B \in \mathsf{P}_n$ are both Hermitian. Recall from (3) that $AB = \pm BA$ (the phases are scalars and do not affect commutation).

- If $AB = BA$, then $(AB)^\dagger = B^\dagger A^\dagger = BA = AB$, so $AB$ is Hermitian.
- If instead $AB = -BA$, then $(AB)^\dagger = B^\dagger A^\dagger = BA = -AB$, so $AB$ is skew-Hermitian.

## §24.3. Stabilizer groups

**Main idea.** Recall that a quantum code $\mathcal{C}$ is a subspace of $\mathbb{C}^{2^n}$. When designing a stabilizer code we do not directly construct this subspace (for instance, we do not directly specify an orthonormal basis for $\mathcal{C}$). Instead, we start with the identification of a subset $S$ of Paulis (with phase). The choice of $S$ identifies the code $\mathcal{C}$.




Given $S \subset \mathsf{P}_n$, we declare the code $\mathcal{C}$ to be the set of all vectors fixed by every operator in $S$:

$$\mathcal{C} = \big\{ |\psi\rangle \in \mathbb{C}^{2^n} \ : \ M|\psi\rangle = |\psi\rangle \text{ for all } M \in S \big\}.$$

This is the space of all $+1$-eigenvectors that are common to every operator in $S$. The code $\mathcal{C}$ is called a *stabilizer code*, and we also use the notation $\mathcal{C}(S)$ for it. The set $S$ is called the *stabilizer* or the *stabilizer group* of the code: every operator in $S$ *stabilizes* every codeword in $\mathcal{C}$. (The stabilizer $S$ is not to be confused with the error set $S_e$ of Lectures 20–23.)

Informally, let us ask: what properties can we impose on $S$? Throughout this discussion we assume that we want a non-trivial code, i.e., $\mathcal{C}$ contains at least one non-zero vector.

**(P1) Closure under multiplication.**

$$A, B \in S \implies AB \in S.$$

Why is this reasonable? Pick any $|\psi\rangle \in \mathcal{C}(S)$; then $A|\psi\rangle = B|\psi\rangle = |\psi\rangle$. What about $AB$? We have

$$AB|\psi\rangle = A\big(B|\psi\rangle\big) = A|\psi\rangle = |\psi\rangle.$$

So $AB$ also stabilizes every codeword, and including $AB$ in $S$ does not change the code $\mathcal{C}(S)$.

**(P2) Closure under inverse.**

$$A \in S \implies A^{-1} \in S.$$

Why is this reasonable? For any $|\psi\rangle \in \mathcal{C}$, $A|\psi\rangle = |\psi\rangle$; multiplying both sides by $A^{-1}$ gives $|\psi\rangle = A^{-1}|\psi\rangle$. Hence $A^{-1}$ stabilizes all codewords, and adding it to $S$ does not change $\mathcal{C}$.

Properties (P1) and (P2), together with the associativity of matrix multiplication, imply that $S$ is a group (assuming $S$ is non-empty). In particular, $I = AA^{-1} \in S$.

**(P3) Hermitian, self-inverse.**

$$A \in S \implies A^\dagger = A \text{ and } A^2 = I \quad (\text{so } A^{-1} = A).$$

Why? Every $A \in S$ has $+1$ as an eigenvalue, with any non-zero codeword as an eigenvector. A skew-Hermitian Pauli does not have $+1$ as an eigenvalue (see §24.2), so $A$ must be one of the Hermitian Paulis, i.e., $\mu = \pm 1$, and then $A^\dagger = A$ and $A^2 = I$.

**(P4) Commutativity.** Assume (P1)–(P3). Then

$$A, B \in S \implies AB = BA.$$

Why? Two reasons:

(a) Non-commuting Paulis have no common eigenvectors (see Question 2 of Homework 9), while we want every vector in $\mathcal{C}(S)$ to be an eigenvector of both $A$ and $B$.

(b) If $AB = -BA$ for some $A, B \in S$, then, since $A$ and $B$ are Hermitian by (P3), $AB$ is skew-Hermitian (see §24.2). But $AB \in S$ by (P1), contradicting (P3).

Thus (P1), (P2) and (P4) together imply that $S$ is an *abelian* (commutative) group.

**(P5) Negative identity is excluded.**

$$-I \notin S.$$

Why? The operator $-I$ does not have $+1$ as an eigenvalue: $-I|\psi\rangle = |\psi\rangle$ only for $|\psi\rangle = 0$. So if $-I \in S$, then $\mathcal{C} = \{0\}$.

**Reducing the list of properties.** It turns out that (P1), (P2) and (P5) already imply the other two properties. That is, if $S \subset \mathsf{P}_n$ is a group that does not contain $-I$, then $S$ is an abelian group and all the operators in $S$ are Hermitian and self-inverse.

**CLAIM.** (P1), (P2), (P5) $\implies$ (P3).

*Proof.* If not, there exists $A \in S$ that is not Hermitian, i.e., $A$ has phase $\mu = \pm i$. Then $A^\dagger = -A$ and $A^2 = -I$. By (P1), $A^2 = A \cdot A \in S$, i.e., $-I \in S$, which contradicts (P5). ■

**CLAIM.** (P1), (P2), (P5) $\implies$ (P4).

*Proof.* By contradiction. Since any two Paulis either commute or anticommute, if (P4) is not true then there exist $A, B \in S$ with $AB = -BA$. By (P1), $AB \in S$ and $BA \in S$, and then by (P2), $(BA)^{-1} \in S$. Using (P1) again,

$$(AB)(BA)^{-1} = -(BA)(BA)^{-1} = -I \in S,$$

which contradicts (P5). ■

**Definition and consequences.** We thus arrive at the following definition.

**DEFINITION.** *A* stabilizer, *or a* stabilizer group, *is a non-empty subset $S$ of $\mathsf{P}_n$ that is*

*(1) closed under multiplication,*

*(2) closed under inverse, and*

*(3) free of $-I$, i.e., $-I \notin S$.*

Note that this definition makes $S$ a group (in particular, a subgroup of $\mathsf{P}_n$). Since every group contains the identity element, we have $I \in S$.

The following properties are consequences of this definition.

(4) All operators in $S$ are Hermitian and self-inverse (they square to $I$).

(5) All operators in $S$ commute pairwise.

(6) If $A \in S$, then $-A \notin S$, $iA \notin S$ and $-iA \notin S$. That is, if $A \in S$, then changing the phase of $A$ while keeping the factors in its Kronecker product takes us outside $S$.

(7) $I \in S$, and $-I$, $iI$, $-iI \notin S$.

*Proof.* Properties (4) and (5) are the two claims above.

Proof of (6). Let $A \in S$. If $-A \in S$, then by (1), $A(-A) = -A^2 = -I \in S$ (using (4)), contradicting (3). The operators $\pm iA$ are skew-Hermitian, since $A$ is Hermitian by (4); hence $\pm iA \notin S$, again by (4).

Proof of (7). Since $S$ is a group we have $I \in S$. Applying (6) to $A = I$ gives $-I, iI, -iI \notin S$. ■

**Examples.**

(1) $S = \{I \otimes I \otimes I,\ X \otimes X \otimes X\}$. Since $(X \otimes X \otimes X)^2 = I \otimes I \otimes I$, this set is closed under multiplication and inverse, and it does not contain $-I$.

(2) $S = \{I \otimes I,\ X \otimes X,\ Z \otimes Z,\ -Y \otimes Y\}$. Using $Y = iXZ$, i.e., $-iY = XZ$,

$$(X \otimes X)(Z \otimes Z) = (XZ) \otimes (XZ) = (-iY) \otimes (-iY) = -Y \otimes Y,$$

and similarly the product of any two elements of $S$ is in $S$. Every element squares to $I \otimes I$, so $S$ is closed under inverse, and $-I \otimes I \notin S$.

The fact that $X \otimes X \in S$ and $Z \otimes Z \in S$ forces $-Y \otimes Y \in S$.

REMARK. *The code $\mathcal{C}(S)$ is the* 1*-dimensional subspace spanned by the EPR state* $(|00\rangle + |11\rangle)/\sqrt{2}$ *(Lecture 19: it is a stabilizer state).*

(3) $S = \{I \otimes I \otimes \cdots \otimes I\}$. This is the smallest possible stabilizer, and $\mathcal{C}(S) = \mathbb{C}^{2^n}$. This code can not correct any non-trivial set of errors.

## §24.4. The size of a stabilizer

The stabilizers in the examples above have sizes 1, 2 and 4, each of which is a power of 2. This observation carries forward to all stabilizers, which is what we will show next.

**CLAIM.** *The size of any stabilizer is a power of* 2*.*

REMARK. *This follows immediately from a group-theoretic result that says that the size of any finite* 2*-group is a power of* 2*. A* 2*-group is a group where the* order *of each element is a power of* 2*. The stabilizer groups are* 2*-groups since either $A^{2^0} = I$ or $A^{2^1} = I$ for every $A \in S$.*

Instead of proving the above claim, we will state and prove a stronger result.

**THEOREM.** *If $S$ is a stabilizer, then there exists an integer $r \geq 0$ such that $|S| = 2^r$, and there exist $M_1, \ldots, M_r \in S$ such that*

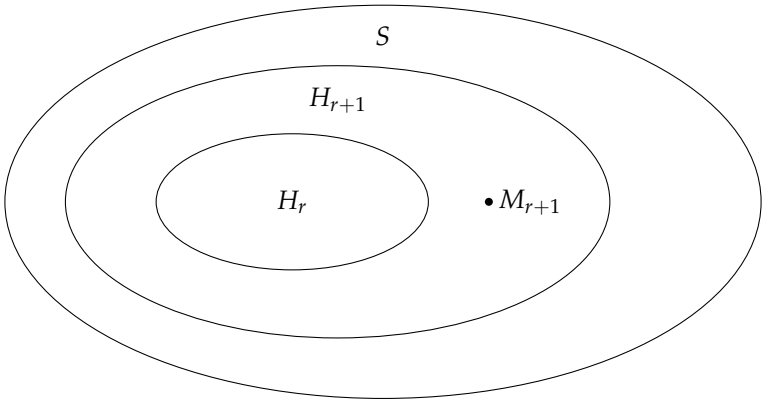
$$S = \left\{ M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r} \ :\ a_i \in \{0,1\}\ \forall i \right\}.$$

REMARK. *The set $S$ is a finite-dimensional vector space over the binary field $\mathbb{F}_2 = \{0,1\}$ (not the complex field $\mathbb{C}$). In $\mathbb{F}_2$ addition and multiplication are performed modulo* 2*. With this observation in hand, the above theorem is simply the fact that $S$ has a basis with $r$ elements where $r$ is the dimension of $S$ over $\mathbb{F}_2$. Now, what makes $S$ an $\mathbb{F}_2$-vector space? Think of elements (operators) in $S$ as 'vectors', and define the* addition *of vectors $A, B \in S$ as $AB$. The* zero vector *is $I$. For a scalar*

$a \in \mathbb{F}_2 = \{0,1\}$ *and a vector* $A \in S$*, define the* multiplication of the scalar $a$ with the vector $A$ *as the operator* $A^a$.

*We will give an elementary proof of the theorem, which is essentially the proof of the existence of a basis when* $S$ *is viewed as an* $\mathbb{F}_2$*-vector space.*

*Proof.* We will use induction: we build a chain of groups $\{I\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subseteq S$, each twice as large as the previous one, until we exhaust $S$.




*Start.* Since $S$ is a stabilizer it must contain $I$. First check if this is the only operator in $S$, that is, check whether $S = \{I\}$. If so, $r = 0$ and we are done. In this case there are no $M_1, M_2, \ldots$ to be chosen. The product $M_1^{a_1} \cdots M_r^{a_r}$ is an empty product. An empty product is the identity element (in the same way as: an empty sum is 0, and the linear span of an empty set of vectors is $\{0\}$).

If $S \neq \{I\}$ then $S \setminus \{I\}$ is non-empty; pick any $M_1 \in S \setminus \{I\}$ and define

$$H_1 := \{I, M_1\} = \{M_1^0, M_1^1\}.$$

It is easy to check that $H_1$ is a group, since $M_1^2 = I$ by property (4). Note that $|H_1| = 2^1$ and its elements are enumerated by the two powers of $M_1$. Also set $H_0 = \{I\}$.

*Induction.* Assume that at step $r \geq 1$ we have:

(a) $H_r \subseteq S$,

(b) $|H_r| = 2^r$,

(c) elements $M_1, \ldots, M_r \in H_r$ such that $H_r = \left\{M_1^{a_1} \cdots M_r^{a_r} \ : \ a_i \in \{0,1\}\right\}$, and

(d) $H_r$ is a group.

Check if $H_r = S$. If yes, we are done. Else, pick $M_{r+1} \in S \setminus H_r$ and define

$$H_{r+1} \triangleq H_r \cup H_r M_{r+1} = \left\{M_1^{a_1} \cdots M_r^{a_r} M_{r+1}^{a_{r+1}} \ : \ a_i \in \{0,1\}\right\},$$

where $H_r M_{r+1} = \{AM_{r+1} : A \in H_r\}$. We need to check if this definition of $H_{r+1}$ allows us to carry forward the induction. That is, we need to check that $H_{r+1}$ satisfies all four assumptions (a)–(d) we made on $H_r$ (with $r$ replaced by $r+1$). This is what we will prove now.

(a) We picked $M_1, \ldots, M_{r+1}$ from $S$. Since $S$ is closed under multiplication we have that $M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} \in S$. Thus, we have $H_{r+1} \subseteq S$.

(c) Clearly, we have $M_1, \ldots, M_{r+1} \in H_{r+1}$; for instance,

$$M_1 = M_1^1 M_2^0 \cdots M_{r+1}^0 \in H_{r+1}.$$

Also, directly by the definition of $H_{r+1}$, we have

$$H_{r+1} = \{M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} \ : \ a_i \in \{0,1\}\}.$$

(d) We need to show that $H_{r+1}$ is closed under multiplication and inverse. This along with the associativity of matrix multiplication will imply that $H_{r+1}$ is a group.

Since the elements of $S$ commute pairwise and square to $I$,

$$(M_1^{a_1} \cdots M_{r+1}^{a_{r+1}})(M_1^{b_1} \cdots M_{r+1}^{b_{r+1}}) = M_1^{(a_1+b_1) \bmod 2} \cdots M_{r+1}^{(a_{r+1}+b_{r+1}) \bmod 2} \in H_{r+1},$$

since $(a_i + b_i) \bmod 2 \in \{0,1\}$. Thus $H_{r+1}$ is closed under multiplication. Since every element of $H_{r+1}$ is in $S$, we know that it is its own inverse, so $H_{r+1}$ is closed under inverse as well. Thus $H_{r+1}$ is a group. In fact it is an abelian group.

(b) It remains to show that $|H_{r+1}| = 2^{r+1}$. We need to show that for any $(a_1, \ldots, a_{r+1}) \in \{0,1\}^{r+1}$ and $(b_1, \ldots, b_{r+1}) \in \{0,1\}^{r+1}$ with $(a_1, \ldots, a_{r+1}) \neq (b_1, \ldots, b_{r+1})$, i.e., $a_j \neq b_j$ for some $j$,

$$M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} \neq M_1^{b_1} \cdots M_{r+1}^{b_{r+1}}.$$

Assume to the contrary that

$$M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} = M_1^{b_1} \cdots M_{r+1}^{b_{r+1}}.$$

Choose $j$ to be the largest index such that $a_j \neq b_j$; then we have $a_i = b_i$ for all $i > j$. This implies that both LHS and RHS above have the common factor $M_{j+1}^{a_{j+1}} \cdots M_{r+1}^{a_{r+1}}$. Cancelling this common factor (this is allowed since this common factor is an invertible matrix) we have

$$M_1^{a_1} \cdots M_j^{a_j} = M_1^{b_1} \cdots M_j^{b_j},$$

with the crucial fact that $a_j \neq b_j$. Rearranging the terms and using commutativity,

$$M_1^{a_1-b_1} M_2^{a_2-b_2} \cdots M_{j-1}^{a_{j-1}-b_{j-1}} = M_j^{b_j-a_j}.$$

Since $M_i^{-1} = M_i$, we have

$$M_1^{(a_1-b_1) \bmod 2} M_2^{(a_2-b_2) \bmod 2} \cdots M_{j-1}^{(a_{j-1}-b_{j-1}) \bmod 2} = M_j^{(b_j-a_j) \bmod 2}.$$

Each factor $M_i^{(a_i-b_i) \bmod 2}$ on the left equals either $M_i^0$ or $M_i^1$ so the left-hand side belongs to $H_{j-1}$ (this follows from the induction hypothesis; for $j = 1$ it is the empty product $I \in H_0$). Since $b_j - a_j = \pm 1$, the right-hand side equals $M_j$. But $M_j$ was picked from $S \setminus H_{j-1}$, so $M_j \notin H_{j-1}$. This is a contradiction. We reach the conclusion $|H_{r+1}| = 2^{r+1}$.

All the induction assumptions thus hold at step $r + 1$.

*Termination.* The sizes $|H_1| < |H_2| < \cdots$ strictly increase, while all the $H_r$ are contained in $S \subseteq \mathsf{P}_n$, which is finite ($|\mathsf{P}_n| = 4^{n+1}$). Hence the procedure stops at some step $r$ with $H_r = S$, which gives $|S| = 2^r$ and $S = \{M_1^{a_1} \cdots M_r^{a_r} : a_i \in \{0,1\}\}$. ■

# *Lecture 25*

We continue our study of the stabilizer framework, following Chapter 3 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. In this lecture we formally define *generating sets* of a stabilizer, prove that the dimension of a stabilizer code is a power of 2 (as promised in Lecture 24), and ask how a given stabilizer group can be enlarged.

## §25.1. Recap and generating sets

**Recap.** Recall the set of $n$-qubit Paulis and the Pauli group,

$$\widehat{\mathsf{P}}_n = \{A_1 \otimes \cdots \otimes A_n \ : \ A_i \in \{I, X, Y, Z\}\},$$

$$\mathsf{P}_n = \{\mu\, A_1 \otimes \cdots \otimes A_n \ : \ A_i \in \{I, X, Y, Z\},\ \mu \in \{\pm 1, \pm i\}\}.$$

The Pauli group $\mathsf{P}_n$ is a non-abelian group. A stabilizer is a subset $S \subset \mathsf{P}_n$ such that

(1) $S$ is a group, and

(2) $-I \notin S$.

In Lecture 24 we showed that these two properties imply

(3) $S$ is abelian, and

(4) every $A \in S$ satisfies $A^2 = I$ and $A^\dagger = A$.

We also proved that $|S| = 2^r$ for some integer $r \geq 0$, and that there exist $M_1, \ldots, M_r \in S$ such that

$$S = \{M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r} \ : \ a_i \in \{0, 1\}\}.$$

**Generating sets.** The operators $M_1, \ldots, M_r$ are to the stabilizer $S$, as a basis is to a vector space. These operators are *independent* (none of these operators can be written as a product of powers of the other operators in this collection), and these operators generate the group $S$ (that is, every operator in $S$ is a product of some powers of $M_1, \ldots, M_r$).

**DEFINITION.** *Let $S$ be a stabilizer with $|S| = 2^r$. A set of operators $\{M_1, \ldots, M_r\} \subseteq S$ such that $S = \{M_1^{a_1} \cdots M_r^{a_r} : a_i \in \{0, 1\}\}$ is called a* minimal generating set *or an* independent generating set *of $S$.*

REMARK. *Any subset of $S$ of size $r - 1$ (or fewer), say $N_1, \ldots, N_{r-1}$, cannot generate $S$: $N_1, \ldots, N_{r-1}$ commute and square to $I$, so the best we can hope for is that the $2^{r-1}$ products $N_1^{a_1} \cdots N_{r-1}^{a_{r-1}}$, $a_i \in \{0, 1\}$, are all distinct. But even this will cover only $2^{r-1}$ elements from $S$.*

Sometimes we will simply call $\{M_1, \ldots, M_r\}$ a *generating set*.
We use the following terminology:

- $M_1, \ldots, M_r$ are the *stabilizer generators*;
- any $M \in S$ is a *stabilizer element*;
- $S$ is the *stabilizer* or the *stabilizer group*.

REMARK. *In general, the generating set of a given stabilizer is not unique. This is similar to the fact that a vector space, in general, has more than one choice of basis.*

EXAMPLE. *Consider* $S = \{I \otimes I,\ X \otimes X,\ Z \otimes Z,\ -Y \otimes Y\}$ *from Lecture 24, for which* $r = 2$. *Each of the following is a generating set of* $S$*:*

$$\{X \otimes X,\ Z \otimes Z\},$$

$$\{X \otimes X,\ -Y \otimes Y\},$$

$$\{Z \otimes Z,\ -Y \otimes Y\}.$$

*In fact, these are the only possible generating sets for this stabilizer.*

Indeed, Lecture 24 showed that $(X \otimes X)(Z \otimes Z) = -Y \otimes Y$. Similarly, using $XY = iZ$ and $ZY = -iX$,

$$(X \otimes X)(-Y \otimes Y) = -(XY) \otimes (XY) = -(iZ) \otimes (iZ) = Z \otimes Z,$$

$$(Z \otimes Z)(-Y \otimes Y) = -(ZY) \otimes (ZY) = -(-iX) \otimes (-iX) = X \otimes X.$$

So in each case the two generators, their product and $I \otimes I$, i.e., $\{I, M_1, M_2, M_1M_2\}$ cover all of $S$.

**The code is determined by the generators.** We know that we can specify a stabilizer code $\mathcal{C}(S)$ by specifying the stabilizer group $S$. Note that $S$ has $2^r$ elements. Instead of listing all the elements of $S$ it is sufficient to list only $r$ generators of $S$. These $r$ operators $M_1, \ldots, M_r$ specify $S$ and hence identify the code $\mathcal{C}(S)$ as well. We have already done this for the Steane code ($M_1, \ldots, M_6$, Lecture 18) and the Shor code ($M_1, \ldots, M_8$, Lecture 19).

Recall that the stabilizer code defined by $S$ is

$$\mathcal{C}(S) \triangleq \big\{|\psi\rangle \ :\ M|\psi\rangle = |\psi\rangle \text{ for all } M \in S\big\}.$$

The next claim says that, in order to check whether an arbitrary $|\psi\rangle \in \mathbb{C}^{2^n}$ is a codeword, it is enough to check the generators; it is not necessary to check all the stabilizer elements.

**CLAIM.** *If* $\{M_1, \ldots, M_r\}$ *is a generating set of* $S$*, then*

$$\mathcal{C}(S) = \big\{|\psi\rangle \ :\ M_i|\psi\rangle = |\psi\rangle \textit{ for all } i = 1, \ldots, r\big\}.$$

*Proof.* (A) If $|\psi\rangle \in \mathcal{C}(S)$, then immediately $M_i|\psi\rangle = |\psi\rangle$ for all $i$, since each $M_i \in S$.

(B) Conversely, suppose $M_i|\psi\rangle = |\psi\rangle$ for all $i = 1, \ldots, r$. Pick any $M \in S$; we show $M|\psi\rangle = |\psi\rangle$. We can write $M = M_1^{a_1} \cdots M_r^{a_r}$ with $a_i \in \{0, 1\}$. Then

$$M|\psi\rangle = M_1^{a_1} \cdots M_{r-1}^{a_{r-1}} \big(M_r^{a_r}|\psi\rangle\big) = M_1^{a_1} \cdots M_{r-1}^{a_{r-1}}|\psi\rangle,$$

since $M_r^{a_r}|\psi\rangle = |\psi\rangle$ whether $a_r = 0$ or $a_r = 1$. Repeating this argument for $M_{r-1}, \ldots, M_1$ gives $M|\psi\rangle = |\psi\rangle$. ∎

## §25.2. Dimension of a stabilizer code

So far we saw how a stabilizer code is defined and identified: through a group $S$ or its generators $M_1, \ldots, M_r$. Our next task is to identify the dimension of the code and the distance of the code. We first attack the dimension.

Suppose $\{M_1, \ldots, M_r\}$ is a minimal generating set of a stabilizer $S \subset \mathsf{P}_n$. By the claim above,

$$\mathcal{C}(S) = \text{space of common } +1\text{-eigenvectors of } M_1, \ldots, M_r.$$

We will compute the dimension of this space. Towards this, note that:

(1) Each $M_i$ is Hermitian; hence it is unitarily diagonalizable.

(2) The operators $M_1, \ldots, M_r$ commute pairwise.

*Simultaneous diagonalization:* Facts (1) and (2) imply that $M_1, \ldots, M_r$ are *simultaneously unitarily diagonalizable*: there exists an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{2^n}\rangle\}$ of $\mathbb{C}^{2^n}$ such that each $|\psi_j\rangle$ is an eigenvector of each $M_i$; this is a well-known result in matrix analysis. Using $|\psi_1\rangle, \ldots, |\psi_{2^n}\rangle$ as the columns of a unitary matrix $U$, we have

$$U^\dagger M_i U = \Lambda_i \quad \text{(diagonal)}, \qquad \text{for all } i = 1, \ldots, r.$$

This is precisely the spectral decomposition of $M_i$: the columns of $U$ are its eigenvectors and the diagonal entries of the diagonal matrix $\Lambda_i$ are its eigenvalues.

An orthonormal basis for the code $\mathcal{C}(S)$ can be found as follows: go through the list of vectors $|\psi_1\rangle, \ldots, |\psi_{2^n}\rangle$, and pick the vectors that have eigenvalue $+1$ for each of $M_1, \ldots, M_r$. The number of such vectors then gives the dimension of the code $\mathcal{C}(S)$. Now let's proceed with this counting.

**Counting the common +1-eigenvectors.** The diagonal entries of $\Lambda_i$ are the eigenvalues of $M_i$; the $j$-th diagonal entry of $\Lambda_i$, say $\lambda_{ij}$, satisfies $M_i|\psi_j\rangle = \lambda_{ij}|\psi_j\rangle$. That is, $\lambda_{ij}$ is the eigenvalue of $M_i$ for the eigenvector $|\psi_j\rangle$.

Since $M_i^\dagger = M_i$ and $M_i \in \mathsf{P}_n$, we know that the eigenvalues of $M_i$ lie in $\{+1, -1\}$ (Lecture 24, §24.2). Therefore

$$\text{each diagonal entry of } \Lambda_i \in \{+1, -1\},$$

$$\text{each diagonal entry of } \frac{I + \Lambda_i}{2} \in \{0, 1\}.$$

For example (with $n = 2$, $r = 2$),

$$\Lambda_1 = \begin{bmatrix} +1 & & & \\ & +1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \qquad \Lambda_2 = \begin{bmatrix} +1 & & & \\ & -1 & & \\ & & -1 & \\ & & & +1 \end{bmatrix},$$

$$\frac{I + \Lambda_1}{2} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{bmatrix}, \qquad \frac{I + \Lambda_2}{2} = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1 \end{bmatrix}.$$

In this case only $|\psi_1\rangle \in \mathcal{C}(S)$: the first diagonal entries of $\Lambda_1$ and $\Lambda_2$ are both $+1$. For diagonal positions $j = 2, 3, 4$, at least one of $\Lambda_1$ or $\Lambda_2$ has $-1$ in the $j^{\text{th}}$ location. This is translated into a logical AND condition if we use the matrices $(I + \Lambda_i)/2$: the only diagonal location $j$ that has 1 (and not 0) in both $(I + \Lambda_1)/2$ and $(I + \Lambda_2)/2$ is $j = 1$.

In general, consider the diagonal matrix

$$\prod_{i=1}^{r} \left( \frac{I + \Lambda_i}{2} \right). \qquad (*)$$

Its diagonal entries lie in $\{0, 1\}$. We now know that $|\psi_j\rangle \in \mathcal{C}(S)$ if and only if the $j^{\text{th}}$ diagonal entry of $(*)$ equals 1. The number of such orthonormal vectors is simply the trace of $(*)$, and this is precisely the dimension of $\mathcal{C}(S)$.

**Computing the trace.** To find the trace, we go back from the "spectral domain" to the "Pauli domain" (we already know how to find the trace of Paulis: only $\pm I, \pm iI$ have non-zero trace; all other operators in $\mathsf{P}_n$ have trace equal to 0). Using the cyclic property of the

trace and $U^\dagger U = I$,

$$\begin{aligned}\dim \mathcal{C}(S) &= \mathrm{Tr}\left[\left(\frac{I+\Lambda_1}{2}\right)\cdots\left(\frac{I+\Lambda_r}{2}\right)\right] \\ &= \mathrm{Tr}\left[U\left(\frac{I+\Lambda_1}{2}\right)\cdots\left(\frac{I+\Lambda_r}{2}\right)U^\dagger\right] \\ &= \mathrm{Tr}\left[U\left(\frac{I+\Lambda_1}{2}\right)U^\dagger\cdots U\left(\frac{I+\Lambda_r}{2}\right)U^\dagger\right].\end{aligned}$$

Since $U\Lambda_i U^\dagger = M_i$ and $UIU^\dagger = I$, we have $U(\frac{I+\Lambda_i}{2})U^\dagger = \frac{I+M_i}{2}$. Hence

$$\begin{aligned}\dim \mathcal{C}(S) &= \mathrm{Tr}\left[\frac{1}{2}(I+M_1)\cdots\frac{1}{2}(I+M_r)\right] \\ &= \mathrm{Tr}\left[\frac{1}{2^r}(I+M_1)\cdots(I+M_r)\right].\end{aligned}$$

Expanding the product,

$$\dim \mathcal{C}(S) = \frac{1}{2^r}\,\mathrm{Tr}\left[\sum_{\substack{a_1,\ldots,a_r \\ a_i\in\{0,1\}}} M_1^{a_1}M_2^{a_2}\cdots M_r^{a_r}\right].$$

Since $\{M_1,\ldots,M_r\}$ is a minimal generating set, as $(a_1,\ldots,a_r)$ ranges over $\{0,1\}^r$ the product $M_1^{a_1}\cdots M_r^{a_r}$ ranges over every element of $S$ exactly once. Therefore

$$\dim \mathcal{C}(S) = \frac{1}{2^r}\,\mathrm{Tr}\left[\sum_{M\in S} M\right] = \frac{1}{2^r}\sum_{M\in S}\mathrm{Tr}(M).$$

We now evaluate $\mathrm{Tr}(M)$ for each $M \in S$.

(1) If $M = I$ (i.e., $a_1 = \cdots = a_r = 0$), then $\mathrm{Tr}(M) = 2^n$.

(2) If $M \in S \setminus \{I\}$, then $M \neq \pm I, \pm iI$, since $-I, \pm iI \notin S$ (Lecture 24, consequence (7)). So $M = \mu\, A_1 \otimes \cdots \otimes A_n$ with at least one $A_i \neq I$, and therefore $\mathrm{Tr}(M) = \mu\mathrm{Tr}(A_1)\cdots\mathrm{Tr}(A_n) = 0$, since $\mathrm{Tr}(X) = \mathrm{Tr}(Y) = \mathrm{Tr}(Z) = 0$.

Only the term $M = I$ survives, and we conclude

$$\dim \mathcal{C}(S) = \frac{2^n}{2^r} = 2^{n-r}.$$

That is, the stabilizer code has $k = \log_2 \dim \mathcal{C}(S)$ logical qubits with

$$k = n - r.$$

In particular, the dimension of every stabilizer code is a power of 2, which justifies the $[\![n,k,d]\!]$ notation of Lecture 24.

REMARK. *The same proof also shows that the operator $\frac{1}{2^r}(I+M_1)\cdots(I+M_r) = U(*)U^\dagger$ is the orthogonal projector onto $\mathcal{C}(S)$, since $(*)$ is the diagonal projector onto the span of those $|\psi_j\rangle$ that lie in $\mathcal{C}(S)$. It is well-known that the trace of a projection operator equals the dimension of the subspace that it projects onto. See Chapter 3 of Gottesman's book.*

**Consequences.**

**COROLLARY.** *If $S \subset \mathsf{P}_n$ is a stabilizer with $|S| = 2^r$, then $r \leq n$.*

*Proof.* With the definition $\mathcal{C}(S) \triangleq \{|\psi\rangle : M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$, $\mathcal{C}(S)$ is a subspace of $\mathbb{C}^{2^n}$, so $\dim \mathcal{C}(S) \in \{0, 1, 2, \dots\}$ is an integer. Since $\dim \mathcal{C}(S) = 2^{n-r}$, the number $2^{n-r}$ is an integer. This forces $n - r \geq 0$, i.e., $r \leq n$. ■

The extreme case $r = n$ gives a code of dimension $2^0 = 1$ and uses the largest possible stabilizer group.

**DEFINITION.** *A* stabilizer state $|\psi\rangle$ *is a common $+1$-eigenvector of all the operators in a stabilizer of size $2^n$ (i.e., $r = n$).*

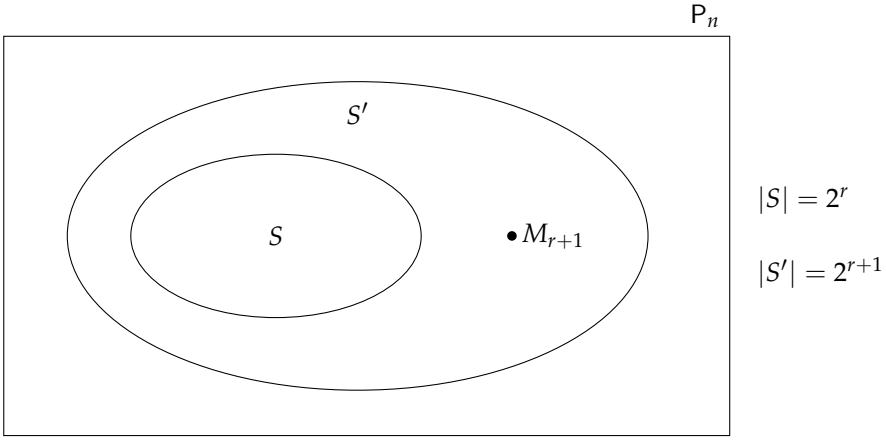
Since $\dim \mathcal{C}(S) = 1$ in this case, the subspace $\mathcal{C}(S)$ is spanned by a single non-zero vector. The normalized (unit-norm) version of this vector is the only pure quantum state residing in $\mathcal{C}(S)$; any other unit-norm vector in $\mathcal{C}(S)$ differs only by a global phase, and hence represents the same quantum state. For example, the EPR state $(|00\rangle + |11\rangle)/\sqrt{2}$ is the stabilizer state of $S = \{I \otimes I,\ X \otimes X,\ Z \otimes Z,\ -Y \otimes Y\}$, which has $n = r = 2$.

## §25.3. How to enlarge a stabilizer?

A subspace of a vector space can be enlarged by appending a new vector to its basis: as long as this new vector is linearly independent of the basis vectors of the subspace, the new subspace will be strictly larger than the given subspace. We would like to ask a similar question where the stabilizer group $S$ plays the role of the subspace. Given a stabilizer $S \subset \mathsf{P}_n$ of size $2^r$, how can we enlarge it to a new stabilizer $S'$ such that $S \subset S'$ and $|S'| = 2^{r+1}$? We would like to do so by enlarging the generating set:

- the generating set of the 'small' stabilizer $S$ is, say, $M_1, \dots, M_r$
- the generators of the new stabilizer are obtained by appending a new operator $M_{r+1}$: $M_1, \dots, M_r, M_{r+1}$.

We now ask: how should one choose $M_{r+1}$ so that $S'$ is strictly larger than $S$? We first identify some necessary conditions on $M_{r+1}$; we then show that these conditions are sufficient as well.




**Observation 1.** $M_{r+1} \notin S$.

Why? If $M_{r+1} \in S$, then $M_1, \dots, M_{r+1}$ are not independent: $M_{r+1} = M_1^{a_1} \cdots M_r^{a_r}$ for some choice of $a_1, \dots, a_r$. Then every product of $M_1, \dots, M_{r+1}$ is already a product of $M_1, \dots, M_r$, so the new stabilizer equals the old stabilizer, and it has size $2^r$, not $2^{r+1}$.

**Observation 2.** We cannot choose any operator from $S$. Instead, can we pick an operator from $S$ and modify its phase:

$$M_{r+1} = \mu\, M_1^{a_1} \cdots M_r^{a_r} \quad \text{for } \mu \in \{-1, \pm i\}?$$

We cannot choose $\mu = +i$ or $\mu = -i$: the operator $M_1^{a_1} \cdots M_r^{a_r} \in S$ is Hermitian, and this would make $M_{r+1}$ skew-Hermitian, which is not allowed in a stabilizer (since we need $M_{r+1} \in S'$).

The choice $\mu = -1$ is not allowed either, because this would imply that both $M_1^{a_1} \cdots M_r^{a_r}$ and $-M_1^{a_1} \cdots M_r^{a_r} = M_{r+1}$ belong to the new stabilizer $S'$, contradicting consequence (6) of Lecture 24 (if $A$ is in a stabilizer then $-A$ is not).

Therefore $M_{r+1}$ cannot be chosen from

$$S \cup (-S) \cup (iS) \cup (-iS) = \pm S \cup \pm iS,$$

where $\mu S \triangleq \{\mu M : M \in S\}$.

**Observation 3.** We have to pick $M_{r+1} \in \mathsf{P}_n$ so that

$$M_{r+1}^\dagger = M_{r+1},$$

since we need $M_{r+1} \in S'$ and every element of the stabilizer $S'$ must be Hermitian. This also implies that $M_{r+1}^2 = I$.

**Observation 4.** Since $M_1, \ldots, M_{r+1}$ must generate $S'$, which is abelian, we must choose $M_{r+1}$ to be an operator that commutes with $M_1, \ldots, M_r$.

Observations 1–4 are all necessary conditions on $M_{r+1}$.

**Are these conditions sufficient as well?** Suppose $M_{r+1} \in \mathsf{P}_n$ satisfies conditions 1–4. Is

$$S' = \left\{ M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} \;:\; a_i \in \{0,1\} \right\}$$

a stabilizer group of size $2^{r+1}$? We have to show:

(a) $S'$ is closed under multiplication;

(b) $S'$ is closed under inverse;

(c) $-I \notin S'$;

(d) $|S'| = 2^{r+1}$.

*Proof.* First note that $M_1, \ldots, M_{r+1}$ commute pairwise ($M_1, \ldots, M_r$ do since they lie in $S$, and $M_{r+1}$ commutes with them by condition 4), and each of them squares to $I$: for $M_1, \ldots, M_r$ this holds since they lie in $S$, and since $M_{r+1}^\dagger = M_{r+1}$ (condition 3), $M_{r+1}$ is a Hermitian Pauli, so $M_{r+1}^2 = I$ (Lecture 24, §24.2).

(a) Take two elements of $S'$,

$$M_1^{a_1} \cdots M_{r+1}^{a_{r+1}} \quad \text{and} \quad M_1^{b_1} \cdots M_{r+1}^{b_{r+1}}, \qquad a_i, b_i \in \{0,1\}.$$

Rearranging the factors (they commute) and using $M_i^2 = I$, their product is

$$\prod_{i=1}^{r+1} M_i^{(a_i+b_i) \bmod 2} \in S'.$$

(b) For $M_1^{a_1} \cdots M_{r+1}^{a_{r+1}}$, the inverse is itself: by (a) its square is $\prod_i M_i^{(2a_i) \bmod 2} = I$. So the inverse lies in $S'$.

(c) Consider $M = M_1^{a_1} \cdots M_r^{a_r} M_{r+1}^{a_{r+1}} \in S'$.

If $a_{r+1} = 0$, then $M = M_1^{a_1} \cdots M_r^{a_r} \in S$. Since $S$ is a stabilizer it does not contain $-I$. Hence $M \neq -I$.

If $a_{r+1} = 1$, then $M = \left(M_1^{a_1} \cdots M_r^{a_r}\right) M_{r+1}$. If $M = -I$, then, multiplying on the left by $M_1^{a_1} \cdots M_r^{a_r}$ (which is its own inverse),

$$M_{r+1} = -M_1^{a_1} \cdots M_r^{a_r},$$

so $M_{r+1} \in -S$. This contradicts condition 2.

(d) We use a technique similar to part (c). The $2^r$ products with $a_{r+1} = 0$ are exactly the elements of $S$, and they are distinct since $|S| = 2^r$. The $2^r$ products with $a_{r+1} = 1$ are the operators $AM_{r+1}$ with $A \in S$; these are distinct as well, since $AM_{r+1} = BM_{r+1}$ implies $A = B$ ($M_{r+1}$ is invertible). Finally, no product of the first kind equals one of the second kind: if $A = BM_{r+1}$ with $A, B \in S$, then

$$M_{r+1} = B^{-1}A = BA \in S,$$

which contradicts condition 1. Hence the $2^{r+1}$ products are all distinct, and $|S'| = 2^r + 2^r = 2^{r+1}$.

By (a)–(c), $S'$ is a stabilizer and by (d) it has size $2^{r+1}$ with minimal generating set $\{M_1, \ldots, M_{r+1}\}$. ■

We summarize this result as

**THEOREM.** *A generating set $M_1, \ldots, M_r$ of a stabilizer $S$ extends to a generating set $M_1, \ldots, M_r$, $M_{r+1}$ of a strictly larger stabilizer $S'$ if and only if*

- *$M_{r+1}$ commutes with $M_1, \ldots, M_r$,*
- *$M_{r+1}$ is Hermitian, and*
- *$M_{r+1} \notin \pm S \cup \pm iS$.*

In the next lecture we will tie this result to the distance of the stabilizer code $\mathcal{C}(S)$.

# *Lecture 26*

This lecture is based on Chapter 3 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*. Our plan is to relate the distance of a stabilizer code $\mathcal{C}(S)$ to the algebraic properties of its stabilizer $S$. The theorem we proved towards the end of the last lecture will help us.

## §26.1. Recap: enlarging a stabilizer

**Recap.** Recall the Pauli group, which is a non-abelian group,

$$\mathsf{P}_n = \big\{\mu\, A_1 \otimes \cdots \otimes A_n \;:\; \mu \in \{\pm 1, \pm i\},\ A_i \in \{I, X, Y, Z\}\big\}.$$

A stabilizer is a subset $S \subset \mathsf{P}_n$ such that

(1) $S$ is a group, and

(2) $-I \notin S$.

These two are the defining properties of a stabilizer, and have the following consequences (Lecture 24):

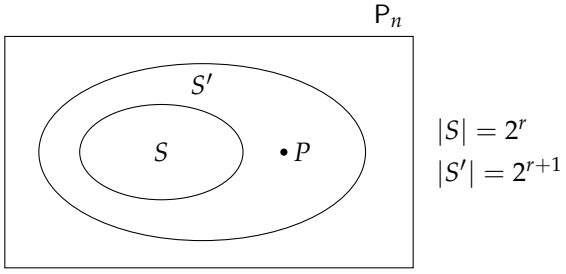
(3) if $M \in S$, then $M^\dagger = M$ and $M^2 = I$;

(4) if $M \in S$, then $-M \notin S$ and $\pm iM \notin S$.

If $\{M_1, \ldots, M_r\}$ is a minimal generating set of $S$, then we know that

$$S = \big\{M_1^{a_1} \cdots M_r^{a_r} \;:\; a_i \in \{0,1\}\big\}, \qquad |S| = 2^r.$$

Now append an operator $P \in \mathsf{P}_n$ to the generators of $S$, and let $S'$ be the group of operators generated by $M_1, \ldots, M_r, P$. We would like $S'$ to be a new stabilizer that is strictly larger than $S$, as shown below.




The result of Lecture 25, with $P$ in the role of $M_{r+1}$, is the following.

**THEOREM.** *$S'$ is a stabilizer of size $2^{r+1}$ if and only if*

*(1) $P$ commutes with $M_1, \ldots, M_r$,*

*(2) $P \notin \pm S \cup \pm iS$, and*

*(3) $P^\dagger = P$.*

In this lecture we will rephrase condition (1) above in terms of what is known as the *normalizer* or the *centralizer* of $S$.

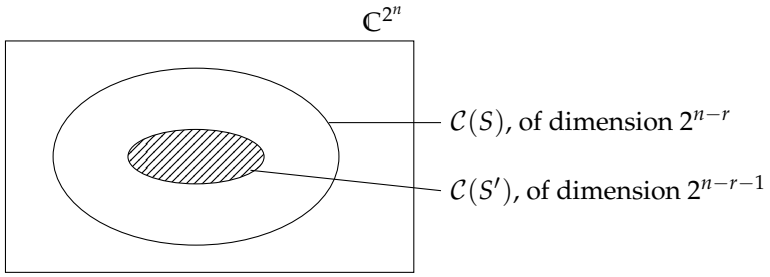
**Relation between the two codes.** Suppose $S'$ is a stabilizer as in the above theorem. The two codes are

$$\mathcal{C}(S) = \text{all kets in } \mathbb{C}^{2^n} \text{ stabilized by } M_1, \ldots, M_r,$$
$$\mathcal{C}(S') = \text{all kets in } \mathbb{C}^{2^n} \text{ stabilized by } M_1, \ldots, M_r, P.$$

Any ket stabilized by $M_1, \ldots, M_r, P$ is, in particular, stabilized by $M_1, \ldots, M_r$. Hence $\mathcal{C}(S) \supset \mathcal{C}(S')$. We think of $M_1, \ldots, M_r, P$ as imposing constraints on the codewords (similar to the parity-check conditions for classical linear codes). A ket in $\mathcal{C}(S')$ must satisfy all the conditions satisfied by every ket in $\mathcal{C}(S)$, and further, must be a $+1$-eigenvector of $P$. From Lecture 25, the dimensions of these two codes are

$$\dim \mathcal{C}(S) = 2^{n-r},$$
$$\dim \mathcal{C}(S') = 2^{n-r-1} = \frac{1}{2} \dim \mathcal{C}(S).$$

The additional constraint (a ket in $\mathcal{C}(S')$ must be a $+1$-eigenvector of $P$) cuts the dimension of the code by half. Each of the $r$ constraints on $\mathcal{C}(S)$ (imposed by the generators $M_1, \ldots, M_r$) halves the dimension of the code starting from the Hilbert space $\mathbb{C}^{2^n}$.




Since $\mathcal{C}(S')$ is the part of $\mathcal{C}(S)$ that is stabilized by $P$, we note that

- if $|\psi\rangle \in \mathcal{C}(S')$, then $P|\psi\rangle = |\psi\rangle$;
- if $|\psi\rangle \in \mathcal{C}(S) \setminus \mathcal{C}(S')$, then $P|\psi\rangle \neq |\psi\rangle$.

These two observations will be used in characterizing the distance of the stabilizer code $\mathcal{C}(S)$.

The code $\mathcal{C}(S')$ is a subspace of $\mathcal{C}(S)$, and therefore it inherits the error correction capabilities of $\mathcal{C}(S)$:

(1) the distance of $\mathcal{C}(S')$ is at least the distance of $\mathcal{C}(S)$;

(2) if $\mathcal{C}(S)$ corrects $S_e$, then $\mathcal{C}(S')$ corrects $S_e$.

Point (2) follows from the fact that any decoder for $\mathcal{C}(S)$ can be used to decode $\mathcal{C}(S')$ too, since every codeword of $\mathcal{C}(S')$ is a codeword of $\mathcal{C}(S)$. Thus, if the decoder for $\mathcal{C}(S)$ corrects the error set $S_e$, the same decoder corrects $S_e$ when used with the code $\mathcal{C}(S')$. For (1), first choose an orthonormal basis $|\psi_1\rangle, \ldots, |\psi_{2^{k-1}}\rangle$, where $k = n - r$, for the smaller code $\mathcal{C}(S')$, and then extend this to an orthonormal basis $|\psi_1\rangle, \ldots, |\psi_{2^k}\rangle$ for the code $\mathcal{C}(S)$. With this choice of basis, the claim follows immediately from the definition of the code distance (Lecture 23).

## §26.2. The normalizer of a stabilizer

We now provide two conditions on $P \in \mathsf{P}_n$, each of which is equivalent to condition (1) of the theorem stated in §26.1.

**CLAIM.** *Let $P \in \mathsf{P}_n$. Then $P$ commutes with $M_1, \ldots, M_r$ if and only if $P$ commutes with every $M \in S$.*

*Proof.* ($\Leftarrow$) This is immediate, since $M_1, \ldots, M_r \in S$.

($\Rightarrow$) Let $M \in S$. Then $M = M_1^{a_1} \cdots M_r^{a_r}$ for some $a_1, \ldots, a_r \in \{0, 1\}$. Moving $P$ to the right, past one generator at a time,

$$\begin{aligned} P\big(M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r}\big) &= M_1^{a_1} P M_2^{a_2} \cdots M_r^{a_r} \\ &= \cdots \\ &= M_1^{a_1} \cdots M_r^{a_r} P \\ &= MP. \end{aligned}$$

■

**CLAIM.** *Let $P \in \mathsf{P}_n$. $P$ commutes with all $M \in S$ if and only if $PMP^{-1} \in S$ for all $M \in S$.*

This claim converts the commutativity condition into a membership condition. The transformation $M \mapsto PMP^{-1}$ is called a *similarity* transformation. In group theory, this operation is called *conjugation*.

*Proof.* Since $P, M \in \mathsf{P}_n$, these two operators either commute or anticommute. That is,

$$PM = \epsilon\, MP, \quad \text{where} \quad \epsilon = \begin{cases} +1 & \text{if } MP = PM, \\ -1 & \text{otherwise.} \end{cases}$$

Multiplying on the right by $P^{-1}$ gives

$$PMP^{-1} = \epsilon\, M.$$

If $P$ commutes with $M$, then $\epsilon = 1$ and $PMP^{-1} = M \in S$. On the other hand, if $P$ does not commute with $M$ then $PMP^{-1} = -M$, and since $M \in S$ and $S$ is a stabilizer, we have $-M \notin S$. ■

**DEFINITION.** *Let $S$ be a stabilizer. We define*

$$\begin{aligned} N(S) &\triangleq \big\{P \in \mathsf{P}_n \;:\; PM = MP \text{ for all } M \in S\big\} \\ &= \big\{P \in \mathsf{P}_n \;:\; PMP^{-1} \in S \text{ for all } M \in S\big\}. \end{aligned}$$

The second form is the group-theoretic definition of the *normalizer of $S$ in $\mathsf{P}_n$*, and the first form is that of the *centralizer of $S$ in $\mathsf{P}_n$*. By the second claim above, the two definitions coincide in our setting (when $S$ is a stabilizer subgroup of the Pauli group $\mathsf{P}_n$). We will call $N(S)$ the normalizer.

Using the first claim above, condition (1) of the theorem is simply

$$P \in N(S).$$

**Properties.**

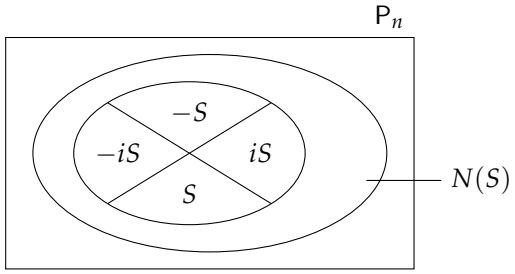
(1) If $P \in N(S)$, then $\pm P, \pm iP \in N(S)$, since scalars commute with every operator. In general, for any scalar $\mu \neq 0$, $PM = MP$ if and only if $(\mu P)M = M(\mu P)$.

(2) $S \subset N(S)$, because $S$ is an abelian group. An operator $P \in \mathsf{P}_n$ belongs to $N(S)$ if and only if it commutes with every element of $S$. Since $S$ is abelian, every $P \in S$ commutes with every operator in $S$.

(3) From (1) and (2),

$$\pm S \cup \pm iS \subset N(S).$$

Note that the four sets $\pm S, \pm iS$ are non-intersecting.




Conditions (1) and (2) of the theorem together say that $P \in N(S) \setminus (\pm S \cup \pm iS)$. We can now restate the theorem from §26.1.

**THEOREM.** *$S'$ is a stabilizer of size $2^{r+1}$ if and only if*

$$P \in N(S) \setminus (\pm S \cup \pm iS) \quad \textit{and} \quad P^\dagger = P.$$

**Example: the Steane code.** We now identify a Pauli $P \in N(S) \setminus (\pm S \cup \pm iS)$. For the Steane code ($n = 7$), the generators are

$$\begin{array}{lccccccc}
M_1 = & I & I & I & X & X & X & X \\
M_2 = & I & X & X & I & I & X & X \\
M_3 = & X & I & X & I & X & I & X \\
M_4 = & I & I & I & Z & Z & Z & Z \\
M_5 = & I & Z & Z & I & I & Z & Z \\
M_6 = & Z & I & Z & I & Z & I & Z
\end{array}$$

so $r = 6$, $|S| = 2^6 = 64$ and $k = 1$. Consider the Hermitian operator

$$P = Y \otimes Y \otimes Y \otimes I \otimes I \otimes I \otimes I.$$

We claim that $P \in N(S) \setminus (\pm S \cup \pm iS)$.

*$P \in N(S)$:* The support of $P$ (that is, the qubits where $P$ does not have the identity operator) is disjoint from the supports of $M_1$ and $M_4$, so $P$ commutes with these two generators. Each of $M_2, M_3, M_5, M_6$ overlaps with the support of $P$ in exactly two qubits. In each of these two qubits the factors anticommute ($Y$ anticommutes with both $X$ and $Z$), and so $P$ commutes with $M_2, M_3, M_5, M_6$ since $(-1)^2 = 1$.

*$P \notin \pm S \cup \pm iS$:* We prove this by contradiction. Suppose $P \in (\pm S \cup \pm iS)$. Then, for some choice of $\mu \in \{\pm 1, \pm i\}$ and $a_1, \ldots, a_6 \in \{0, 1\}$ we have

$$P = \mu M_1^{a_1} \cdots M_6^{a_6}.$$

$P$ has $Y$ in the first qubit. This necessarily means that we need $a_3 = a_6 = 1$ since all other generators have identity on the first qubit. Similarly, since $P$ has $Y$ on the second qubit we require $a_2 = a_5 = 1$ as well. Now, on the third qubit $M_2, M_3$ each have $X$ and $M_5, M_6$ each have $Z$, and these four generators together contribute $X \cdot X \cdot Z \cdot Z = I$. Further, both $M_1$ and $M_4$ have the identity on the first three qubits, so irrespective of the values of $a_1$ and $a_4$ the third qubit of $M_1^{a_1} \cdots M_6^{a_6}$ will be identity, whereas $P$ has $Y$ on this qubit. This is a contradiction.

Note that

$$\mathrm{wt}(P) = 3 = 2t + 1 \quad \text{for } t = 1,$$

and the Steane code is a 1-error correcting quantum code.

The size of the normalizer of any stabilizer code is $|N(S)| = 4 \times 2^{n+k}$, where $k = n - r$ (we have not proved this result yet). For the Steane code, this is $4 \times 2^8 = 1024$.

**A note on common eigenvectors.** Recall that matrices that commute and are individually unitarily diagonalizable are simultaneously unitarily diagonalizable. Apply this to the set of matrices $M_1, \ldots, M_r, P$. Each of these matrices is *normal* (i.e., $AA^\dagger = A^\dagger A$), and hence, is unitarily diagonalizable. Further, if $P \in N(S)$, these $r+1$ operators commute. Thus, they are simultaneously unitarily diagonalizable. This means that it is possible to find an orthonormal basis $\{|\psi_i\rangle\}$ of $\mathbb{C}^{2^n}$ such that each basis vector $|\psi_i\rangle$ is a common eigenvector of $M_1, \ldots, M_r, P$. This does not mean that every (common) eigenvector of $M_1, \ldots, M_r$ is also an eigenvector of $P$. This is the reason why not all the vectors in $\mathcal{C}(S)$ are stabilized by $P$. The following elementary example illustrates what commutativity does and does not guarantee. Consider

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

These two operators commute, and so there exist $|\psi_1\rangle, |\psi_2\rangle$ such that $|\psi_i\rangle$ is a common eigenvector of both $I$ and $Z$ for $i = 1, 2$ (namely, $|0\rangle$ and $|1\rangle$). However, this does *not* imply that every eigenvector of $I$ is an eigenvector of $Z$: for example, $|+\rangle$ and $|-\rangle$ are eigenvectors of $I$ but neither of them is an eigenvector of $Z$.

## §26.3. Knill–Laflamme conditions and the distance of stabilizer codes

**Recall.** Let us first recall the definition of the distance of a quantum code (which arises from the Knill–Laflamme conditions). Let $\mathcal{C}$ be any code and let $P \in \mathsf{P}_n$. We say that $P$ satisfies *Property* $(*)$ if

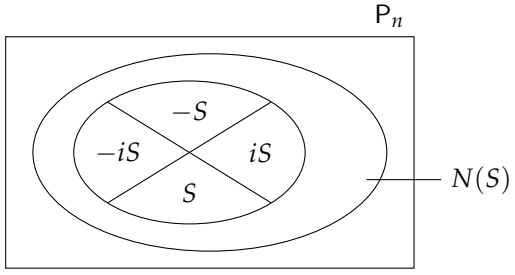
$$\langle\psi|P|\phi\rangle = \langle\psi\,|\,\phi\rangle\,\gamma(P) \quad \text{for all } |\psi\rangle, |\phi\rangle \in \mathcal{C}, \qquad \text{(Property } *\text{)}$$

for some choice of the constant $\gamma(P) \in \mathbb{C}$ (this is equivalent to the matrix $\Lambda(P)$ of Lecture 23 being a scalar matrix). Thus the distance of $\mathcal{C}$ is

$$d(\mathcal{C}) = \text{smallest weight among all Paulis } P \text{ that } \textit{do not satisfy } (*).$$

*Next step:* We will show that, for a stabilizer code $\mathcal{C}(S)$, the Paulis that do not satisfy $(*)$ are exactly those in $N(S) \setminus (\pm S \cup \pm iS)$. As a corollary, we obtain

$$d = \text{minimum weight among all Paulis in } N(S) \setminus (\pm S \cup \pm iS).$$




Since $N(S)$ contains $\pm S \cup \pm iS$, we see that the sets $N(S)$ and $\pm S \cup \pm iS$ split the group $\mathsf{P}_n$ into three regions:

- the operators in $\pm S \cup \pm iS$,
- those outside $N(S)$, and
- those lying in between, i.e., $N(S) \setminus (\pm S \cup \pm iS)$.

We consider them one at a time, and verify if the operators satisfy $(*)$.

**A preliminary observation.** If $P$ satisfies $(*)$, then so does $\mu P$, where $\mu$ is any scalar. Why? We have

$$\langle\psi|\mu P|\phi\rangle = \mu\langle\psi|P|\phi\rangle = \mu\,\gamma(P)\,\langle\psi\,|\,\phi\rangle,$$

and $\mu\,\gamma(P)$ is a constant, which we choose to call $\gamma(\mu P)$. Also, we define the weight of $\mu A_1 \otimes \cdots \otimes A_n$ to be the same as the weight of $A_1 \otimes \cdots \otimes A_n$. Thus, the definition of the code distance does not change if we consider Paulis with phase (i.e., $P \in \mathsf{P}_n$) instead of Paulis without phase (i.e., $P \in \widehat{\mathsf{P}}_n$).

**The Paulis that satisfy the property.**

**CLAIM.** *Every Pauli in $\pm S \cup \pm iS$ satisfies $(*)$ for the code $\mathcal{C}(S)$.*

*Proof.* By the preliminary observation, it is enough to show this for $P \in S$. Pick any $P \in S$. For all $|\psi\rangle, |\phi\rangle \in \mathcal{C}(S)$, we have $P|\phi\rangle = |\phi\rangle$. Hence

$$\langle\psi|P|\phi\rangle = \langle\psi\,|\,\phi\rangle = \langle\psi\,|\,\phi\rangle\,\gamma(P),$$

where we choose $\gamma(P) = 1$. ■

**CLAIM.** *Every Pauli in $\mathsf{P}_n \setminus N(S)$ satisfies $(*)$ for the code $\mathcal{C}(S)$.*

*Proof.* Say $P \in \mathsf{P}_n \setminus N(S)$. Then there exists an $M \in S$ such that $P$ does not commute with $M$, i.e., $PM = -MP$ (note: this does not mean that $P$ anticommutes with *every* operator in $S$). For all $|\psi\rangle, |\phi\rangle \in \mathcal{C}(S)$,

$$\begin{aligned}
\langle\psi|P|\phi\rangle &= \langle\psi|PM|\phi\rangle && (M|\phi\rangle = |\phi\rangle)\\
&= \langle\psi|(-MP)|\phi\rangle\\
&= -\langle\psi|MP|\phi\rangle\\
&= -\langle\psi|M^\dagger P|\phi\rangle && (M^\dagger = M)\\
&= -\langle\psi|P|\phi\rangle && (M|\psi\rangle = |\psi\rangle).
\end{aligned}$$

Therefore $\langle\psi|P|\phi\rangle = 0$, which equals $\langle\psi\,|\,\phi\rangle\,\gamma(P)$ with $\gamma(P) = 0$. ■

**The Paulis that do not satisfy the property.**

**CLAIM.** *If $P \in N(S) \setminus (\pm S \cup \pm iS)$, then $P$ does not satisfy $(*)$ for the code $\mathcal{C}(S)$.*

*Proof.* Every element of $\mathsf{P}_n$ is either Hermitian or skew-Hermitian (Lecture 24). If $P$ is skew-Hermitian, use $iP$ instead of $P$ in this proof: $iP$ is Hermitian and it also lies in $N(S) \setminus (\pm S \cup \pm iS)$, and by the preliminary observation, if $P$ satisfies $(*)$ then so does $iP$. So, without loss of generality, we can assume that

$$P^\dagger = P \quad \text{and} \quad P \in N(S) \setminus (\pm S \cup \pm iS).$$

By the theorem of §26.2, we can use $P$ to enlarge the stabilizer $S$ to a new stabilizer $S'$, with $|S| = 2^r$ and $|S'| = 2^{r+1}$. We have two codes, $\mathcal{C}(S) \supset \mathcal{C}(S')$, of dimensions $2^{n-r}$ and $\frac{1}{2}\,2^{n-r}$, respectively.

Now, for $P$ to satisfy $(*)$, it is necessary for it to satisfy the special case of $(*)$ where $|\psi\rangle = |\phi\rangle \in \mathcal{C}(S)$ and $\|\psi\| = 1$. Under this special case $(*)$ reduces to

$$\langle\psi|P|\psi\rangle = \langle\psi\,|\,\psi\rangle\,\gamma(P) = \gamma(P).$$

If $P$ does not satisfy this special case it definitely does not satisfy $(*)$.

Now suppose, for the sake of contradiction, that $P$ satisfies $(*)$, and hence this special case as well. Pick $|\psi\rangle \in \mathcal{C}(S')$ with $\||\psi\rangle\| = 1$; this is possible since $\dim \mathcal{C}(S') \geq 1$. Then $P|\psi\rangle = |\psi\rangle$, and

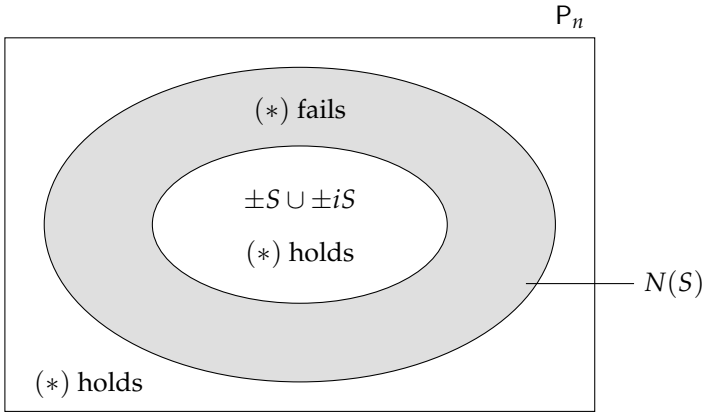
$$\langle\psi|P|\psi\rangle = \langle\psi\,|\,\psi\rangle = 1.$$

This implies that $\gamma(P) = 1$.

Pick $|\psi\rangle \in \mathcal{C}(S) \setminus \mathcal{C}(S')$ with $\||\psi\rangle\| = 1$; this is possible since $\mathcal{C}(S')$ is a proper subspace of $\mathcal{C}(S)$. Such a $|\psi\rangle$ is *not* stabilized by $P$, and hence

$$\langle\psi|P|\psi\rangle = \langle\psi| \cdot \big(P|\psi\rangle\big) \neq 1.$$

Why? We have $\|P|\psi\rangle\| = 1$ since $P$ is unitary, and two unit-norm vectors are equal if and only if their inner product is 1. This implies that $\gamma(P) \neq 1$, a contradiction. Thus, $P$ does not satisfy $(*)$. ■




Combining the three claims, we have the following.

**THEOREM.** *Let $P \in \mathsf{P}_n$ and $\mathcal{C}(S)$ be a stabilizer code. There exists a constant $\gamma(P)$ such that*

$$\langle\psi|P|\phi\rangle = \langle\psi\,|\,\phi\rangle\,\gamma(P) \quad \textit{for all } |\psi\rangle, |\phi\rangle \in \mathcal{C}(S)$$

*if and only if $P \notin N(S) \setminus (\pm S \cup \pm iS)$.*

The following results are immediate consequences of this theorem.

**COROLLARY** (Distance of stabilizer codes)**.** *The distance of a stabilizer code is*

$$d = \min\big\{\mathrm{wt}(P) \;:\; P \in N(S) \setminus (\pm S \cup \pm iS)\big\}.$$

REMARK. *When $k = 0$, i.e., $r = n$, $\mathcal{C}(S)$ is a stabilizer state and $N(S) = \pm S \cup \pm iS$. The set $N(S) \setminus (\pm S \cup \pm iS)$ is empty, and in a strict sense, the distance of this code is infinite.*

EXAMPLE. *For the Steane code, we saw that*

$$P = Y \otimes Y \otimes Y \otimes I \otimes I \otimes I \otimes I \in N(S) \setminus (\pm S \cup \pm iS),$$

*and hence $d \leq \mathrm{wt}(P) = 3$. On the other hand, the Steane code corrects $t = 1$ error, and so $d \geq 2t + 1 = 3$ (Lecture 23). Therefore $d = 3$, and the Steane code is a $[\![7, 1, 3]\!]$ code.*

Now the Knill–Laflamme conditions specialized to stabilizer codes.

**COROLLARY** (Knill–Laflamme for stabilizer codes)**.** *Let $\mathcal{C}(S)$ be any stabilizer code, and let $S_e \subset \mathsf{P}_n$ be any set of errors. Then $\mathcal{C}(S)$ corrects $S_e$ if and only if*

$$E_a^\dagger E_b \notin N(S) \setminus (\pm S \cup \pm iS) \quad \textit{for all } E_a, E_b \in S_e.$$

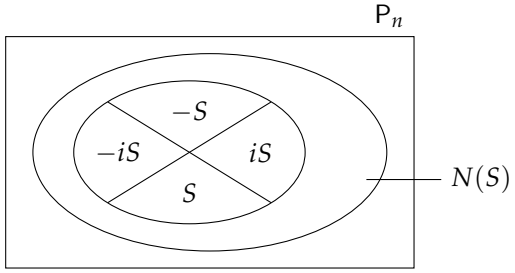
*Proof.* By the basis-free version of the Knill–Laflamme conditions (Lecture 22), $\mathcal{C}(S)$ corrects $S_e$ if and only if $E_a^\dagger E_b$ satisfies $(*)$ for all $E_a, E_b \in S_e$. Note that $E_a^\dagger E_b \in \mathsf{P}_n$ for any $E_a, E_b \in \mathsf{P}_n$. From the theorem above, an operator in $\mathsf{P}_n$ satisfies $(*)$ if and only if it does not lie in $N(S) \setminus (\pm S \cup \pm iS)$. ■

The proof presented in this section highlights how Paulis act on codewords of a stabilizer code. We discuss more about this in the appendix (this material was not presented during the lecture).

## §26.4. Appendix

We investigate how each Pauli $P \in \mathsf{P}_n$ acts on the codewords of a stabilizer code $\mathcal{C}(S)$. As usual, we partition $\mathsf{P}_n$ into three regions

- $P = \mu M$ for $M \in S$ and $\mu = \pm 1, \pm i$,
- $P \notin N(S)$, and
- the rest.




Let $|\phi\rangle \in \mathcal{C}(S)$ and let $P$ represent an error acting on the codeword $|\phi\rangle$ to produce $|\zeta\rangle = P|\phi\rangle$. We ask how $|\zeta\rangle$ is related to $\mathcal{C}(S)$.

$$|\tilde{\phi}\rangle \in \mathbb{C}^{2^k} \xrightarrow[k \text{ qubits}]{} \boxed{\text{Encoder}} \xrightarrow[n \text{ qubits}]{|\phi\rangle \in \mathcal{C}(S)} \boxed{P} \xrightarrow[n \text{ qubits}]{} |\zeta\rangle = P|\phi\rangle$$

*Case: $P = \mu M$, with $M \in S$.* We have

$$|\zeta\rangle = P|\phi\rangle = \mu M|\phi\rangle = \mu|\phi\rangle \equiv |\phi\rangle \text{ up to global phase.}$$

Thus, the Paulis in $\pm S \cup \pm iS$ act trivially on the codewords and are harmless errors.

*Case: $P \notin N(S)$.* From our treatment of this case earlier, we know that

$$\langle \psi \,|\, \zeta \rangle = \langle \psi | P | \phi \rangle = 0 \text{ for all } |\psi\rangle, |\phi\rangle \in \mathcal{C}(S).$$

Thus, $|\zeta\rangle$ is orthogonal to every vector in $\mathcal{C}(S)$. That is, $|\zeta\rangle$ belongs to the orthogonal complement of the subspace $\mathcal{C}(S)$ in the Hilbert space $\mathbb{C}^{2^n}$.

*Case: $P \in N(S) \setminus (\pm S \cup \pm iS)$.* We first recognize that $|\zeta\rangle \in \mathcal{C}(S)$, that is, $P$ maps a codeword to a codeword:

$$M_i|\zeta\rangle = M_i P|\phi\rangle = PM_i|\phi\rangle = P|\phi\rangle = |\zeta\rangle \text{ for all } i = 1, \ldots, r,$$

that is, $|\zeta\rangle$ is stabilized by all minimal generators of $S$, and hence, $|\zeta\rangle \in \mathcal{C}(S)$. Without loss of generality, assume that $P$ is Hermitian: if $P$ is skew-Hermitian, then $iP$ is Hermitian, lies in the same set, and differs from $P$ only by a global phase. Further, from our earlier discussion we know that there are choices of codewords $|\phi_1\rangle$ such that

$$P|\phi_1\rangle = |\phi_1\rangle$$

and also choices of codewords $|\phi_2\rangle$ such that

$$P|\phi_2\rangle \neq |\phi_2\rangle.$$

Clearly, there is at least one vector $|\phi\rangle$ in $\mathcal{C}(S)$ such that $P|\phi\rangle \neq |\phi\rangle$ modulo global phase. To see this, if $P|\phi_2\rangle \neq |\phi_2\rangle$ modulo global phase we are done. Otherwise we have $P|\phi_2\rangle = e^{i\theta}|\phi_2\rangle$ where $\theta \in (0, 2\pi)$; in fact this makes $|\phi_2\rangle$ an eigenvector of $P$ with eigenvalue $-1$ since the only eigenvalues of $P$ are $\pm 1$. Using $|\phi\rangle = |\phi_1\rangle + |\phi_2\rangle$, we have

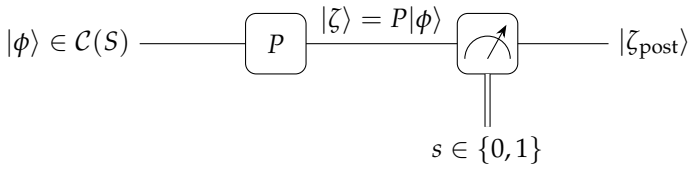
$$P(|\phi_1\rangle + |\phi_2\rangle) = |\phi_1\rangle - |\phi_2\rangle \neq |\phi_1\rangle + |\phi_2\rangle \text{ modulo global phase.}$$

Thus, although $P$ maps $\mathcal{C}(S)$ to $\mathcal{C}(S)$, it acts on $\mathcal{C}(S)$ in a non-trivial way. This is what makes $P$ an *undetectable error*.

**Detecting Pauli errors for a stabilizer code.** Suppose we want to *detect* the occurrence of a Pauli error; we are not interested in identifying the error or correcting its action. For stabilizer codes we can invoke the following circuit where we use a projective measurement defined by two projection operators $\Pi_0$ and $\Pi_1$. Here, $\Pi_0$ is the projection onto the codespace $\mathcal{C}(S)$, which has dimension $2^k$, and $\Pi_1$ is the projection onto its orthogonal complement

$$\mathcal{C}(S)^\perp := \left\{ |\psi\rangle \in \mathbb{C}^{2^n} \ : \ \langle \psi \,|\, \phi \rangle = 0 \text{ for all } |\phi\rangle \in \mathcal{C}(S) \right\}.$$

Note that the dimension of this orthogonal complement is $2^n - 2^k$. We want to use the classical outcome $s$ to indicate whether an error occurred.




If $P \in \pm S \cup \pm iS$, then $|\zeta\rangle \in \mathcal{C}(S)$, and the classical outcome is $s = 0$ and further $|\zeta_{\text{post}}\rangle = |\zeta\rangle$. The classical outcome $s = 0$ indicates that no error occurred ($P = \mu I$) or the error is a stabilizer element which is harmless.

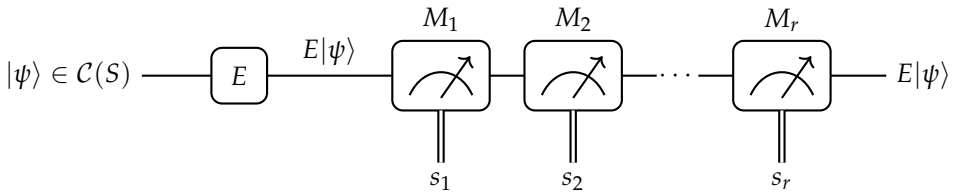
If $P \notin N(S)$, then $|\zeta\rangle \in \mathcal{C}(S)^\perp$, and we have $s = 1$, indicating that a non-trivial error occurred. Still, we have $|\zeta_{\text{post}}\rangle = |\zeta\rangle$.

Our detection algorithm fails when $P \in N(S) \setminus (\pm S \cup \pm iS)$. In this case we still have $s = 0$ (since $|\zeta\rangle \in \mathcal{C}(S)$) and $|\zeta_{\text{post}}\rangle = |\zeta\rangle$, but $|\zeta\rangle$ need not be equal to $|\phi\rangle$ modulo global phase. The measurement device will indicate that no error occurred when in fact one did. Such errors are called undetectable.

**THEOREM.** *A Pauli error $P \in \mathsf{P}_n$ is an undetectable error for a stabilizer code $\mathcal{C}(S)$ if and only if $P \in N(S) \setminus (\pm S \cup \pm iS)$.*

# *Homework 11*

1. **Syndromes and stabilizer codes.** Consider correcting Pauli errors $E \in \mathsf{P}_n$ for a stabilizer code $\mathcal{C}(S)$ with minimal generating set $M_1, \ldots, M_r$. Let $|\psi\rangle \in \mathcal{C}(S)$ be exposed to the error $E$. The erroneous vector $E|\psi\rangle$ is measured using observables $M_1, \ldots, M_r$, one at a time. The resulting syndrome is $s = (s_1, \ldots, s_r) \in \{\pm 1\}^r$.




   (a) Compare the syndromes of the following errors: $E, \mu E, E^\dagger$, where $\mu \in \{\pm 1, \pm i\}$.

   (b) Let $E$ and $E'$ be any Paulis, and let their syndromes be $(s_1, \ldots, s_r)$ and $(s'_1, \ldots, s'_r)$, respectively. Show that $E^\dagger E'$ and $EE'$ have syndrome $(s_1 s'_1, \ldots, s_r s'_r)$.
   REMARK. This map, from error $E \in \mathsf{P}_n$ to syndrome $s \in \{\pm 1\}^r$, is a *group homomorphism*. The *kernel* of this homomorphism is the set of all Paulis that map to the 'all $+1$' syndrome. We will identify the kernel next.
   REMARK. Compare this with a linear transformation: $x \mapsto Ax$. The kernel is the set of all vectors $x$ that map to the all-zero vector.

   (c) Identify all the Pauli errors $E$ with syndrome $(+1, +1, \ldots, +1)$.
   REMARK. The kernel is useful in identifying when two errors have the same syndrome. This is the next question.

   (d) When do errors $E, E' \in \mathsf{P}_n$ have the same syndrome, i.e., $s_i = s'_i$ for all $i$?

   (e) How many Pauli errors have the 'all $+1$' syndrome?
   HINT. Use part (c) and the size of this set stated in Lecture 26. We have not proved that result yet; you may assume it here.

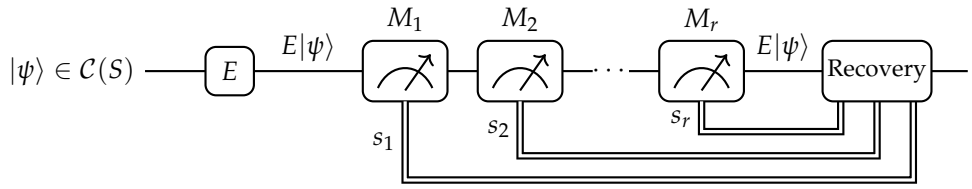
   (f) Let $s = (s_1, \ldots, s_r)$ be a pattern of $\pm 1$, and let $E_0 \in \mathsf{P}_n$ have syndrome $s$. How many Pauli errors (including $E_0$) have the same syndrome $s$?
   HINT. Show that there is a one-to-one mapping between the following two sets

$$\{E \in \mathsf{P}_n \ : \ \text{syndrome is } (+1, \ldots, +1)\} \quad \text{and}$$
$$\{E' \in \mathsf{P}_n \ : \ \text{syndrome is } (s_1, \ldots, s_r)\}.$$

   Thus, these two sets have the same size.

   (g) You must argue that for every choice of $s \in \{\pm 1\}^r$, there is a Pauli $E$ with syndrome $s$.
   HINT. Partition $\mathsf{P}_n$ into subsets such that: all Paulis in the same subset have the same syndrome, and Paulis from different subsets have different syndromes. What is the size of each subset? Use this to count the number of subsets.

2. **Correcting errors using syndrome measurement.** Assume the same context as the previous question. Now we are interested in decoding using a recovery step.




For recovery, we are free to do the following: for each possible syndrome $s$, pick any unitary (call it $U_s$), and use it as the recovery gate. The choice of the unitary must depend only on the syndrome. We want to characterize the error correction behaviour of this circuit. Let $S_e \subset \mathsf{P}_n$ be a set of errors we wish to correct using this circuit.

You must show that $\mathcal{C}(S)$ corrects $S_e$ using this circuit if and only if $E^\dagger E' \notin N(S) \setminus (\pm S \cup \pm iS)$ for all $E, E' \in S_e$.

HINT. You only need to prove one direction of the statement because the other direction follows from Knill–Laflamme: for $\mathcal{C}(S)$ to correct $S_e$ (using *any* circuit, not just the one shown above) it is necessary to have $E^\dagger E' \notin N(S) \setminus (\pm S \cup \pm iS)$ for all $E, E' \in S_e$. So, in your proof assume that $S_e$ in fact satisfies this condition, and show that you can choose $U_s$ in such a way that the errors can be corrected.

3. Consider the circuit (syndrome measurement + recovery) and the context in the previous question. What is the largest size of an error set $S_e \subset \mathsf{P}_n$ such that $\mathcal{C}(S)$ corrects $S_e$ using this circuit?

4. Let stabilizer $S$ be generated by the independent set $M_1, \ldots, M_r$. Since these operators commute and they are Hermitian, they are simultaneously unitarily diagonalizable. Let $|\psi_1\rangle, \ldots, |\psi_{2^n}\rangle$ be an orthonormal set of eigenvectors common to $M_1, \ldots, M_r$.

   *Question.* Fix any $s_1, \ldots, s_r \in \{\pm 1\}$. Identify the number of eigenvectors $|\psi_j\rangle$ such that

   $$\text{for each } i = 1, \ldots, r\text{: } |\psi_j\rangle \text{ is an eigenvector of } M_i \text{ with eigenvalue } s_i.$$

5. **Modifying a stabilizer via sign changes.** Consider a stabilizer $S$ with minimal generating set $M_1, \ldots, M_r$. Define a new stabilizer $S'$ with generators $-M_1, M_2, \ldots, M_r$.

   (a) Show that the codes $\mathcal{C}(S)$ and $\mathcal{C}(S')$ are orthogonal, i.e., every vector in $\mathcal{C}(S)$ is orthogonal to every vector in $\mathcal{C}(S')$.

   (b) Are the sets $\pm S \cup \pm iS$ and $\pm S' \cup \pm iS'$ identical?

   (c) Compare the normalizers $N(S)$ and $N(S')$.

   (d) If $\mathcal{C}(S)$ corrects $S_e$, do you think $\mathcal{C}(S')$ corrects $S_e$ as well?

   REMARK. Start from a stabilizer code $\mathcal{C}(S)$. For each choice of $s \in \{\pm 1\}^r$, define the code $\mathcal{C}(S')$ where $S'$ is generated by $s_1 M_1, \ldots, s_r M_r$. Thus, we have $2^r = 2^{n-k}$ codes (subspaces) in $\mathbb{C}^{2^n}$. These subspaces are pairwise orthogonal, and form a direct-sum decomposition of $\mathbb{C}^{2^n}$.

6. For the Steane code show that $N(S) \setminus (\pm S \cup \pm iS)$ does not contain any Pauli of weight $0, 1, 2$.

7. Identify one Pauli of weight 3 in $N(S) \setminus (\pm S \cup \pm iS)$ for the Shor code.

8. Find all the operators in the normalizer of $S = \{II, XX\} \subset \mathsf{P}_2$.

9. Let $S$ and $S'$ be stabilizers in $\mathsf{P}_n$. Argue that

$$S \neq S' \quad \Rightarrow \quad \mathcal{C}(S) \neq \mathcal{C}(S').$$

HINT. Consider the following cases:

- $|S| \neq |S'|$. Can the two codes be equal?
- Say $|S| = |S'|$ but $S \neq S'$. So there is an $M \in S'$ such that $M \notin S$. What if $M \in -S$?
- What if $M \in S'$ and $M \notin \pm S$? Does this mean $M \notin (\pm S \cup \pm iS)$?

10. Recall the 5 properties of the stabilizers from Lecture 24.

    (a) Do (P1), (P2), (P3) imply (P5)?

    (b) Do (P1), (P2), (P4) imply (P5)?

11. **The** $[[4,1,2]]$ **code.** Consider the code with $n = 4$ and $k = 1$ spanned by

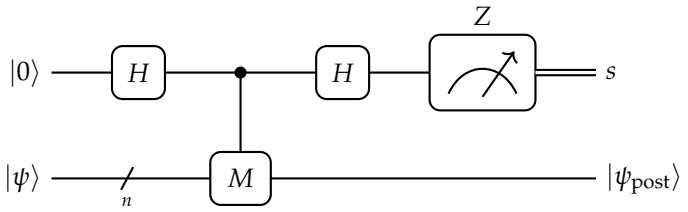
$$|\bar{0}\rangle = \frac{|0000\rangle + |1111\rangle}{\sqrt{2}} \text{ and } |\bar{1}\rangle = \frac{|0011\rangle + |1100\rangle}{\sqrt{2}}.$$

    This is a stabilizer code.

    (a) Can you identify its stabilizer generators?

    (b) Show that the distance of the code is $d = 2$.

12. **On measuring a Pauli observable.** The syndrome measurement of stabilizer codes uses $r$ measurements, in each of which we measure a Hermitian Pauli $M$. We can use a standard measurement device that measures the observable $Z$ on a qubit (that is, measurement along the standard basis for a qubit) to realize this measurement (with the help of some unitary gates). This crucially relies on the fact that the eigenvalues of $M$ are $\pm 1$. The circuit for this measurement is shown below (see Figure 10.13 in Section 10.5.8 of Chapter 10 of Nielsen and Chuang).




    The unitary gate after the first Hadamard is the 'control-$M$' gate; it acts as follows:

$$|0\rangle \otimes |\psi\rangle \mapsto |0\rangle \otimes |\psi\rangle \text{ and } |1\rangle \otimes |\psi\rangle \mapsto |1\rangle \otimes M|\psi\rangle.$$

    Through this gate the ancilla qubit controls what happens to the input state $|\psi\rangle$. Hence, the ancilla and the input register get entangled, unless $|\psi\rangle$ is an eigenvector of $M$.

    (a) Write the composite state immediately after the second Hadamard as

$$|0\rangle \otimes |\phi_1\rangle + |1\rangle \otimes |\phi_2\rangle$$

    for suitable choice of vectors $|\phi_i\rangle$.

    (b) Show that $|\phi_1\rangle$ is the projection of $|\psi\rangle$ onto the $+1$-eigenspace of $M$.

    (c) What about $|\phi_2\rangle$?

(d) What are the post-measurement states and the probabilities corresponding to each of the classical outcomes $s \in \{+1, -1\}$? Does this match with measuring $M$ directly on the state $|\psi\rangle$?

13. Let $\mathcal{C}(S)$ be a stabilizer code with $n \geq 2$, $k \geq 1$ and $r \geq 1$. In the lectures we saw that if $P \in N(S) \setminus (\pm S \cup \pm iS)$ and if $P^\dagger = P$ then

- there exists a $|\psi\rangle \in \mathcal{C}(S)$ with $\||\psi\rangle\| = 1$ such that $\langle\psi|P|\psi\rangle = 1$, and
- there exists a $|\psi\rangle \in \mathcal{C}(S)$ with $\||\psi\rangle\| = 1$ such that $\langle\psi|P|\psi\rangle \neq 1$.

You must prove the following stronger version of the above observation:

*Question:* Let $P \in N(S) \setminus (\pm S \cup \pm iS)$ and $P^\dagger = P$, and let $\alpha$ be any value in the interval $[-1, 1]$. Show that there exists a $|\psi\rangle \in \mathcal{C}(S)$ with $\||\psi\rangle\| = 1$ such that

$$\langle\psi|P|\psi\rangle = \alpha.$$

HINT. One way to solve the problem uses the following intermediate step: identify one well-chosen value of $\alpha$ and solve the question for this particular value of $\alpha$. If your choice of $\alpha$ in this intermediate step is good, then your solution can be quickly generalized to all $\alpha \in [-1, 1]$.

# *Lecture 27*

**Main idea.** We will represent the operators in $\mathsf{P}_n$ as binary vectors of length $2n$. As we do so, we ignore the phase $\mu$ of the Pauli $\mu A_1 \otimes \cdots \otimes A_n$, so that

$$\pm P,\ \pm iP \ \longrightarrow\ \text{the same binary vector.}$$

This map captures and simplifies the code design and analysis problem, and it acts as a bridge connecting quantum coding to classical coding. Losing the information about the phase $\mu$ happens to be harmless (see Question 5 of Homework 11).

Before we can use this map, we need the language of vectors and linear algebra over the binary field. This is the subject of the present lecture.

## §27.1. Vectors over the binary field

**The binary field.** The binary field is the set $\mathbb{F}_2 = \{0, 1\}$ together with the following addition and multiplication operations.

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Addition is addition modulo 2 (the logical XOR), and multiplication is the logical AND. Since $1 + 1 = 0$, the additive inverse of 1 is 1 itself, i.e.,

$$-1 = 1.$$

Hence $a + b = a - b$ for all $a, b \in \mathbb{F}_2$. Regarding multiplicative inverses, $1^{-1} = 1$, whereas $0^{-1}$ is not defined.

The triple $(\mathbb{F}_2, +, \cdot)$ has the following properties.

(1) Addition:

   (a) addition is commutative;
   (b) addition is associative;
   (c) 0 is the additive identity;
   (d) $-a$ exists for all $a \in \mathbb{F}_2$; we have $-0 = 0$ and $-1 = 1$.

(2) Multiplication:

   (a) multiplication is commutative;
   (b) multiplication is associative;
   (c) 1 is the multiplicative identity;
   (d) $a^{-1}$ exists if $a \neq 0$.

(3) The distributive law holds:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{for all } a, b, c \in \mathbb{F}_2.$$

These properties make $\mathbb{F}_2$ a *field*. In fact, this is the smallest field, since a field must contain an additive identity and a distinct multiplicative identity. Because $\mathbb{F}_2$ is a field, we can do linear algebra over $\mathbb{F}_2$. In this course, we will use vectors of length $m$ over $\mathbb{F}_2$, and the vector space is $\mathbb{F}_2^m$. Vectors are added component-wise, and the scalars are the elements of $\mathbb{F}_2$. Note that $\mathbb{F}_2^m$ has exactly $2^m$ elements.

**Conventions.** We write the vectors in $\mathbb{F}_2^m$ as row vectors, which is the typical convention in classical coding theory. We do not use the bra-ket notation for $\mathbb{F}_2^m$:

$$a \in \mathbb{F}_2^m \quad \Rightarrow \quad a = (a_1, \ldots, a_m), \quad \text{where } a_i \in \mathbb{F}_2 \text{ for all } i.$$

Contrast this with the ket $|\psi\rangle$ of a quantum state. In examples, we will drop the commas and write (1 1 1 1) for (1, 1, 1, 1).

**Dot product.** For $a, b \in \mathbb{F}_2^m$, we define the dot product

$$a \cdot b = a_1 b_1 + \cdots + a_m b_m \quad (\text{over } \mathbb{F}_2).$$

In matrix notation,

$$a \cdot b = (a_1, \ldots, a_m) \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = ab^T.$$

**DEFINITION.** *We say that a is orthogonal to b if $a \cdot b = 0$.*

**Example 1.** Let $a = (1\ 1\ 1\ 1) \in \mathbb{F}_2^4$. If $x \in \mathbb{F}_2$, then $x^2 = x$. Therefore,

$$a \cdot a = \sum_{i=1}^{4} a_i a_i = \sum_{i=1}^{4} a_i = 1 + 1 + 1 + 1 = 0.$$

Thus, this non-zero vector is orthogonal to itself. More generally,

$$a_1 + \cdots + a_m = 0 \quad \text{if and only if an even number of the } a_i \text{ are 1,}$$

because the sum over $\mathbb{F}_2$ is the number of 1s reduced modulo 2. Orthogonality here is a purely algebraic notion, and it does not involve the geometric picture associated with Euclidean spaces.

**Example 2.** Let $a = (1\ 1\ 1\ 1)$. We want to find all $b \in \mathbb{F}_2^4$ such that $a \cdot b = 0$. We have

$$a \cdot b = (1\ 1\ 1\ 1) \cdot (b_1\ b_2\ b_3\ b_4) = b_1 + b_2 + b_3 + b_4,$$

and this is 0 if and only if an even number of the $b_i$ are 1. There are exactly 8 such vectors, since

$$\binom{4}{0} + \binom{4}{2} + \binom{4}{4} = 1 + 6 + 1 = 8.$$

## §27.2. Linear algebra over the binary field

**What works over the binary field.** The following concepts and results carry over from linear algebra over $\mathbb{R}$ or $\mathbb{C}$, with the understanding that all operations must use the addition and multiplication rules of $\mathbb{F}_2$:

- linear dependence and independence,
- the span of a set of vectors, and subspaces,
- matrices, determinant, inverse, left inverse, right inverse,
- row rank = column rank = number of pivots,
- row reduction, and the rank-nullity theorem,
- column space, row space, null space.

**What does not work.** The following do not carry over:

- inner product and norm,
- the Cauchy–Schwarz inequality,
- orthonormality and orthogonal projection,
- singular value decomposition (SVD),
- unitary matrices and unitary diagonalization.

These rely on an inner product satisfying $\langle v, v\rangle > 0$ for all $v \neq 0$. This has no meaning over $\mathbb{F}_2$, and Example 1 shows that $v \cdot v$ can be 0 for a non-zero $v$. The dot product $a \cdot b$ defined earlier for vectors in $\mathbb{F}_2^m$ is *not* a true inner product.

**Linear independence.** Vectors $v_1, \ldots, v_k \in \mathbb{F}_2^m$ are *linearly dependent* if there exist scalars $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_2$, not all zero, such that

$$\sum_i \alpha_i v_i = 0.$$

Since each $\alpha_i$ is either 0 or 1, this condition reads

$$\sum_{i\,:\,\alpha_i = 1} v_i = 0.$$

That is, the vectors are linearly dependent if and only if a non-empty subset of $\{v_1, \ldots, v_k\}$ sums to the zero vector. They are *linearly independent* otherwise.

If $v_1, \ldots, v_k$ are linearly independent, then each linear combination has a unique set of coefficients:

$$\begin{aligned} & \alpha_1 v_1 + \cdots + \alpha_k v_k = \beta_1 v_1 + \cdots + \beta_k v_k \\ \text{if and only if} \quad & (\alpha_1 - \beta_1) v_1 + \cdots + (\alpha_k - \beta_k) v_k = 0 \\ \text{if and only if} \quad & \alpha_i - \beta_i = 0 \quad \text{for all } i \\ \text{if and only if} \quad & \alpha_i = \beta_i \quad \text{for all } i. \end{aligned}$$

**Span.** The span of a collection of vectors is

$$\operatorname{span}(v_1, \ldots, v_k) = \Big\{ \sum_i \alpha_i v_i \;:\; \alpha_i \in \{0, 1\} \Big\}.$$

There are $2^k$ choices for $(\alpha_1, \ldots, \alpha_k)$. If $v_1, \ldots, v_k$ are linearly independent, then different choices yield different vectors, as we have just seen, and so the size of the span is $2^k$.

**Subspace.** A non-empty subset $W \subseteq \mathbb{F}_2^m$ is a *subspace* if it is closed under linear combinations, i.e., if $v, w \in W$ and $\alpha, \beta \in \mathbb{F}_2$, then $\alpha v + \beta w \in W$. This is essentially checking if

$$v + w \in W \quad \text{and} \quad 0 \in W,$$

since the only possible values of $\alpha v + \beta w$ are $0, v, w$ and $v + w$. In fact, the condition $0 \in W$ is redundant: picking $v = w$ in the condition $v + w \in W$ gives us $v + v \in W$, i.e., $0 \in W$. Thus, a non-empty subset $W \subseteq \mathbb{F}_2^m$ is a subspace if and only if $W$ is closed under addition.

**Basis.** Let $W$ be a subspace of $\mathbb{F}_2^m$. We say that $v_1, \ldots, v_k$ is a *basis* of $W$ if

(1) $v_1, \ldots, v_k$ are linearly independent, and

(2) $\operatorname{span}(v_1, \ldots, v_k) = W$.

Then $|W| = 2^k$, and $k$ is the *dimension* of the subspace.

**Example: row space.** Let $G$ be any matrix of size $p \times m$ over $\mathbb{F}_2$. The row space of $G$ is

$$\text{row}(G) = \{aG \ : \ a \in \mathbb{F}_2^p\}.$$

The vector $aG$ is the linear combination of the rows of $G$ with coefficients $a_1, \ldots, a_p$, and so $\text{row}(G)$ is the span of the rows of $G$.

**Example: null space.** Suppose $H \in \mathbb{F}_2^{r \times m}$. The null space of $H$ is

$$\text{null}(H) = \{x \in \mathbb{F}_2^m \ : \ Hx^T = 0^T\}.$$

Both $\text{null}(H)$ and $\text{row}(G)$ are subspaces. To verify this we only need to check closure under addition; both contain the zero vector and are hence non-empty. For $\text{null}(H)$: if $x, y \in \text{null}(H)$, then $Hx^T = Hy^T = 0^T$, and so $H(x+y)^T = Hx^T + Hy^T = 0^T$. Thus, $x + y \in \text{null}(H)$. For the row space, if $x, y \in \text{row}(G)$, there exist $a, b$ such that $x = aG$ and $y = bG$. Then, $x + y = aG + bG = (a+b)G$, which belongs to $\text{row}(G)$.

Conversely, it is true that for any subspace $W$, there exist matrices $G$ and $H$ such that

$$W = \text{row}(G) = \text{null}(H).$$

In particular, we can pick $G$ to be any matrix whose rows form a basis (or any spanning set) for $W$. For $H$, we pick its rows to be a basis (or a spanning set) of the orthogonal dual of $W$ (defined in §27.3).

## §27.3. The orthogonal dual

**DEFINITION.** *Let $W$ be any subspace of $\mathbb{F}_2^m$. The* orthogonal dual *of $W$ is defined as*

$$W^\perp = \{v \in \mathbb{F}_2^m \ : \ v \cdot w = 0 \text{ for all } w \in W\}.$$

It is easy to see that $W^\perp$ is a subspace too: if $v_1, v_2 \in W^\perp$, then $(v_1 + v_2) \cdot w = v_1 \cdot w + v_2 \cdot w = 0 + 0 = 0$, thus, $v_1 + v_2 \in W^\perp$. Further, clearly, $0 \in W^\perp$.

**Example.** Consider the following subspace of $\mathbb{F}_2^4$ of dimension 2, with basis $(1\,1\,0\,0)$ and $(0\,0\,0\,1)$:

$$W = \{(0\,0\,0\,0),\ (1\,1\,0\,0),\ (0\,0\,0\,1),\ (1\,1\,0\,1)\}.$$

A vector $v = (v_1, v_2, v_3, v_4)$ is orthogonal to every element of $W$ if and only if it is orthogonal to these two basis vectors, i.e., if and only if $v_1 + v_2 = 0$ and $v_4 = 0$. Therefore,

$$W^\perp = \{(0\,0\,0\,0),\ (1\,1\,0\,0),\ (0\,0\,1\,0),\ (1\,1\,1\,0)\}.$$

**CLAIM.** *If $W = \text{row}(H)$, then $W^\perp = \text{null}(H)$.*

*Proof.* Note that $\text{row}(H)$ is the collection of all the vectors $aH$. The orthogonal dual is the set of all vectors $v$ that are orthogonal to every vector in $W$, i.e., $aHv^T = 0$ for all possible $a$. In other words, the vector $vH^T$ is such that it is orthogonal to every $a$, which means that $vH^T = 0$, i.e., $v \in \text{null}(H)$. ■

**CLAIM.** *For any subspace $W \subseteq \mathbb{F}_2^m$,*

$$\dim(W) + \dim(W^\perp) = \dim(\mathbb{F}_2^m) = m.$$

*Proof.* Choose a matrix $G$ with $\text{row}(G) = W$. Then $\text{rank}(G) = \dim(W)$, and by the previous claim, $W^\perp = \text{null}(G)$. The result now follows from the rank-nullity theorem. ■

We state the next result without proof.

**CLAIM.** *For any subspace $W$, we have $(W^\perp)^\perp = W$.*

We can now justify the choice of $H$ made in §27.2. Choose $H$ with $\text{row}(H) = W^\perp$, i.e., the rows of $H$ span the subspace $W^\perp$. Then

$$\text{null}(H) = \big(\text{row}(H)\big)^\perp = (W^\perp)^\perp = W.$$

**The subspaces can overlap.** It is possible to have

$$W \cap W^\perp \neq \{0\}.$$

It is also possible to have $W \subseteq W^\perp$ or $W^\perp \subseteq W$ (or even $W = W^\perp$). This is unlike the orthogonal complement over $\mathbb{R}$ or $\mathbb{C}$, where a vector in $W \cap W^\perp$ is orthogonal to itself and hence must be zero. For instance, in the first example of this section, the vector $(1\ 1\ 0\ 0)$ lies in both $W$ and $W^\perp$. Note that it is not necessary that $W$ and $W^\perp$ form a direct-sum decomposition of $\mathbb{F}_2^m$; such a decomposition exists only when $W \cap W^\perp = \{0\}$.

**Example.** Let

$$W = \big\{(0\,0\,0\,0),\ (1\,1\,1\,1)\big\}.$$

A vector is orthogonal to $(1\ 1\ 1\ 1)$ if and only if it has an even number of 1s (Example 2 of §27.1). Therefore,

$$\begin{aligned} W^\perp = \big\{&(0\,0\,0\,0),\ (1\,1\,0\,0),\ (1\,0\,1\,0),\ (1\,0\,0\,1),\\ &(0\,1\,1\,0),\ (0\,1\,0\,1),\ (0\,0\,1\,1),\ (1\,1\,1\,1)\big\}. \end{aligned}$$

We see that $W \subseteq W^\perp$. If we instead start from the subspace $W' = W^\perp$, then $(W')^\perp = W$, and we have an example where $(W')^\perp \subseteq W'$.

# *Lecture 28*

This lecture is based on Chapter 3 of Daniel Gottesman's book, *Surviving as a Quantum Computer in a Classical World*.

**Agenda.** We will map the Paulis in $\mathsf{P}_n$ to binary vectors in $\mathbb{F}_2^{2n}$, ignoring the phase. The map, which we will denote by $\tau$, sends

$$\pm P,\ \pm iP \ \xrightarrow{\tau}\ \text{the same vector},$$

and so it is a 4-to-1 map. Ignoring the phase in this way is the same as working with the $n$-qubit Paulis $\widehat{\mathsf{P}}_n$ of Lecture 18.

Using this map, we will rephrase the stabilizer code design problem in terms of subspaces of $\mathbb{F}_2^{2n}$. The design of stabilizer codes then boils down to a discrete mathematics problem, and this allows us to see the connections between quantum coding theory and classical coding theory.

## §28.1. Binary symplectic representation of Paulis

The map $\tau : \mathsf{P}_n \to \mathbb{F}_2^{2n}$ can be defined for every $n \geq 1$. We will start with the case $n = 1$.

**The simplest case.** Let $n = 1$. Then

$$\mathsf{P}_1 = \{\mu I,\ \mu X,\ \mu Y,\ \mu Z\ :\ \mu \in \{\pm 1, \pm i\}\}.$$

We define $\tau : \mathsf{P}_1 \to \mathbb{F}_2^2$ by the following table.

| $P$ | $\mu I$ | $\mu X$ | $\mu Z$ | $\mu Y = i\mu XZ$ |
|---|---|---|---|---|
| $\tau(P)$ | $(0\,0)$ | $(1\,0)$ | $(0\,1)$ | $(1\,1)$ |

We view each Pauli as a product of $X^0$ or $X^1$ with $Z^0$ or $Z^1$ modulo phase. The first component of $\tau(P)$ records whether an $X$ is present, and the second records whether a $Z$ is present. In other words, every $P \in \mathsf{P}_1$ can be written as

$$P = \mu X^x Z^z$$

for some phase $\mu$ and some $x, z \in \{0, 1\}$, and then $\tau(P) = (x\ z)$.

**Observations.** The map $\tau$ captures the multiplication (modulo phase) and the commutativity and anti-commutativity of the Paulis. For all $A, B \in \mathsf{P}_1$, the following hold.

(1) $\tau(AB) = \tau(A) + \tau(B)$. That is, multiplication (ignoring the phase) in $\mathsf{P}_1$ is vector addition in $\mathbb{F}_2^2$.

(2) Let $\tau(A) = (x\ z)$ and $\tau(B) = (x'\ z')$. Then

$$\begin{aligned} AB = BA \quad &\text{when} \quad xz' + zx' = 0 \text{ over } \mathbb{F}_2, \\ AB = -BA \quad &\text{when} \quad xz' + zx' = 1 \text{ over } \mathbb{F}_2. \end{aligned}$$

Note that $xz' + zx'$ is *not* the dot product between $(x\ z)$ and $(x'\ z')$; instead, one of these two vectors is permuted and then a dot product is taken.

Both properties can be checked directly from the multiplication table of the Pauli matrices. To verify (1), note that $\mu I \mapsto (0\,0)$, and hence, if either $A$ or $B$ is $\mu I$, the result is indeed true. Also, when $A = B$ up to phase $\mu$, we have $AB \equiv I$, i.e., $AB = I$ modulo phase; this is the same as the fact that any vector in $\mathbb{F}_2^2$ when added to itself yields $(0\,0)$. Finally, when

$A, B, C \in \{\mu X, \mu Z, \mu Y\}$ are distinct (modulo phase), we see that $AB = C$ modulo phase. This is captured by the additive structure of $\{(1\,0), (0\,1), (1\,1)\}$.

To verify (2), first consider $A = \mu I$. This commutes with every Pauli. Now $\mu I \mapsto (0\,0)$ and we have $xz' + zx' = 0$ when $(x\,z) = (0\,0)$. Now consider the case $A = B$ up to phase, where we have $AB = BA$. In this case, $x = x'$ and $z = z'$, and thus $xz' + zx' = xz + xz = 0$. Anti-commutativity occurs only when $A, B \in \{\mu X, \mu Z, \mu Y\}$ are distinct modulo phase. Clearly, when $(x\,z)$ and $(x'\,z') \in \{(1\,0), (0\,1), (1\,1)\}$ are distinct we have $xz' + zx' = 1$.

**An aside.** The expression $xz' + zx'$ is similar to complex multiplication: if $(x\,z), (x'\,z') \in \mathbb{R}^2$ the imaginary part of $(x + iz)(x' + iz')$ is $xz' + zx'$. Just as the field $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree 2, there is a field $\mathbb{F}_4$ with four elements that is an extension of $\mathbb{F}_2$ of degree 2:

$$\begin{array}{cc} \mathbb{C} & \mathbb{F}_4 \\ \big|2 & \big|2 \\ \mathbb{R} & \mathbb{F}_2 \end{array}$$

The properties (1) and (2) can be framed over $\mathbb{F}_4$ (the resulting product is called the *trace-Hermitian inner product over* $\mathbb{F}_4$), but we will not do this in this course.

**The general case.** We extend this idea to all $n \geq 1$ and define $\tau : \mathsf{P}_n \to \mathbb{F}_2^{2n}$ as follows. If $\tau(A_i) = (x_i\,z_i)$ is the single-qubit map above, then

$$\mu\, A_1 \otimes \cdots \otimes A_n \overset{\tau}{\longmapsto} (x_1\ \cdots\ x_n\, z_1\ \cdots\ z_n),$$

where the phase $\mu$ is ignored. Note the ordering: all the $x_i$ come first, followed by all the $z_i$. We will write $\tau(P) = (x\,z)$, where $x = (x_1\ \cdots\ x_n)$ and $z = (z_1\ \cdots\ z_n)$ are in $\mathbb{F}_2^n$. For example,

$$\tau(\mu\, X \otimes Y \otimes Z \otimes I) = (\underset{x_1}{1}\ \underset{x_2}{1}\ \underset{x_3}{0}\ \underset{x_4}{0}\ \ \underset{z_1}{0}\ \underset{z_2}{1}\ \underset{z_3}{1}\ \underset{z_4}{0}).$$

Conversely, if $\tau(P) = (x_1\ \cdots\ x_n\, z_1\ \cdots\ z_n)$, then

$$P \equiv X^{x_1} Z^{z_1} \otimes X^{x_2} Z^{z_2} \otimes \cdots \otimes X^{x_n} Z^{z_n},$$

where $\equiv$ denotes equality modulo global phase: we write $A \equiv B$ if $A = \mu B$ for some $\mu \in \{\pm 1, \pm i\}$. In particular, $\tau(A) = \tau(B)$ if and only if $A \equiv B$, and the preimage of every vector from $\mathbb{F}_2^{2n}$ is a collection of four Paulis that differ only in their phase.

**CLAIM.** *For any $A, B \in \mathsf{P}_n$, we have*

$$\tau(AB) = \tau(A) + \tau(B),$$

*where the addition is in $\mathbb{F}_2^{2n}$.*

*Proof.* Let $\tau(A) = (x_1\ \cdots\ x_n\, z_1\ \cdots\ z_n)$ and $\tau(B) = (x'_1\ \cdots\ x'_n\, z'_1\ \cdots\ z'_n)$. Then

$$A \equiv X^{x_1} Z^{z_1} \otimes \cdots \otimes X^{x_n} Z^{z_n},$$
$$B \equiv X^{x'_1} Z^{z'_1} \otimes \cdots \otimes X^{x'_n} Z^{z'_n}.$$

By the mixed-product property of the Kronecker product,

$$AB \equiv \left(X^{x_1} Z^{z_1} X^{x'_1} Z^{z'_1}\right) \otimes \cdots \otimes \left(X^{x_n} Z^{z_n} X^{x'_n} Z^{z'_n}\right).$$

Using the property that $XZ = -ZX$, ignoring the global phase and using $X^2 = Z^2 = I$, as in the case $n = 1$, each factor in the Kronecker product satisfies

$$X^{x_i} Z^{z_i} X^{x'_i} Z^{z'_i} \equiv X^{x_i + x'_i} Z^{z_i + z'_i},$$

with the addition in the exponents over $\mathbb{F}_2$. Therefore,

$$\tau(AB) = (x_1 + x'_1\ \cdots\ x_n + x'_n\ \ z_1 + z'_1\ \cdots\ z_n + z'_n) = \tau(A) + \tau(B). \qquad \blacksquare$$

Thus

$$(\mathsf{P}_n, \cdot) \xrightarrow{\tau} (\mathbb{F}_2^{2n}, +)$$

is a *group homomorphism*: it converts products of Paulis into sums of binary vectors.

**DEFINITION.** *Let $x, z, x', z' \in \mathbb{F}_2^n$. The* symplectic product *between $(x\ z)$ and $(x'\ z')$ is*

$$(x\ z) \odot (x'\ z') = x \cdot z' + z \cdot x' \quad \textit{(over } \mathbb{F}_2\textit{)}.$$

**CLAIM.** *Let $A, B \in \mathsf{P}_n$ with $\tau(A) = (x\ z)$ and $\tau(B) = (x'\ z')$, where $x, x', z, z' \in \mathbb{F}_2^n$. Then*

$$AB = BA \quad \textit{if and only if} \quad x \cdot z' + z \cdot x' = 0,$$

*i.e., if and only if $(x\ z) \odot (x'\ z') = 0$. Otherwise, $AB = -BA$.*

*Proof.* Write

$$A = \mu\, A_1 \otimes \cdots \otimes A_n, \quad \tau(A_i) = (x_i\ z_i),$$
$$B = \epsilon\, B_1 \otimes \cdots \otimes B_n, \quad \tau(B_i) = (x_i'\ z_i').$$

Then

$$AB = \mu\epsilon\, (A_1 B_1) \otimes \cdots \otimes (A_n B_n),$$
$$BA = \mu\epsilon\, (B_1 A_1) \otimes \cdots \otimes (B_n A_n).$$

For each $i$, either $A_i B_i = B_i A_i$ or $A_i B_i = -B_i A_i$. Hence $AB = (-1)^m BA$, where

$$m = \#\{i \ :\ A_i B_i = -B_i A_i\},$$

and so $A$ and $B$ commute when $m$ is even, and anticommute when $m$ is odd. By Observation (2), $A_i B_i = -B_i A_i$ if and only if $x_i z_i' + z_i x_i' = 1$. Therefore, modulo 2,

$$m = \sum_{i=1}^{n} \left(x_i z_i' + z_i x_i'\right) = x \cdot z' + z \cdot x' \quad (\text{over } \mathbb{F}_2).$$

Thus $AB = BA$ if and only if $x \cdot z' + z \cdot x' = 0$. ■

REMARK. *The symplectic product has the following properties, which follow directly from the definition. For all $u, v, w \in \mathbb{F}_2^{2n}$ and $\alpha, \beta \in \mathbb{F}_2$,*

*(a) it is symmetric: $u \odot v = v \odot u$;*

*(b) it is bilinear: $u \odot (\alpha v + \beta w) = \alpha\,(u \odot v) + \beta\,(u \odot w)$;*

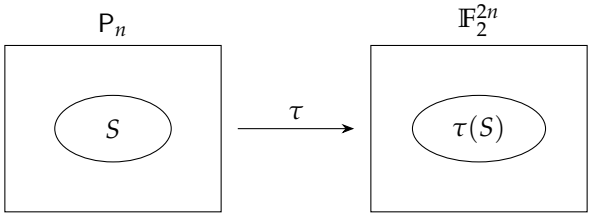
*(c) every vector is symplectically orthogonal to itself: if $v = (x\ z)$, then $v \odot v = x \cdot z + z \cdot x = 2\, x \cdot z = 0$.*

*Property (c) matches the fact that every Pauli commutes with itself.*

## §28.2. Characterizing stabilizers

Let $S \subset \mathsf{P}_n$ be a stabilizer, and consider its image under $\tau$,

$$\tau(S) = \left\{\tau(M)\ :\ M \in S\right\} \subseteq \mathbb{F}_2^{2n}.$$



What are the properties of $\tau(S)$? Suppose $|S| = 2^r$ and $S$ is generated (minimally) by $M_1, \ldots, M_r$ (Lecture 25), so that the code $\mathcal{C}(S)$ has dimension $2^k$ with $k = n - r$.

(1) $|\tau(S)| = 2^r$, i.e., $\tau$ is one-to-one when restricted to $S$.

*Why?* Let $A, B \in S$ with $A \neq B$. We know that $A \neq \mu B$ for every phase $\mu$: indeed, if $A = \mu B$ with $\mu \in \{-1, \pm i\}$, then $\mu B \in S$, which contradicts consequence (6) of the definition of a stabilizer (Lecture 24). Since $A$ and $B$ are distinct modulo phase, their binary representations are distinct as well.

(2) $\tau(S)$ is a subspace of $\mathbb{F}_2^{2n}$.

*Why?* If $A, B \in S$, then $AB \in S$. Consequently, if $v, v' \in \tau(S)$, then there exist $A, B \in S$ such that $v = \tau(A)$ and $v' = \tau(B)$, and

$$v + v' = \tau(A) + \tau(B) = \tau(AB) \in \tau(S).$$

Further, $I \in S$, and so $(0 \cdots 0) = \tau(I) \in \tau(S)$.

By (1) and (2), $\tau(S)$ is a subspace with $2^r$ elements, and therefore

$$\dim\big(\tau(S)\big) = r,$$

i.e., every basis of $\tau(S)$ has $r$ vectors. We will identify one such basis now.

(3) Let $v_i = \tau(M_i)$ for $i = 1, \ldots, r$. Then $\{v_1, \ldots, v_r\}$ is a basis for $\tau(S)$.

*Proof.* Clearly $v_1, \ldots, v_r \in \tau(S)$. Since $\dim(\tau(S)) = r$, it is enough to show that these $r$ vectors are linearly independent. Suppose

$$\sum_{i=1}^{r} a_i v_i = 0, \quad a_i \in \mathbb{F}_2.$$

Since $\tau$ is a homomorphism, $\tau\big(M_1^{a_1} \cdots M_r^{a_r}\big) = \sum_i a_i v_i = 0 = \tau(I)$, i.e.,

$$M_1^{a_1} \cdots M_r^{a_r} \equiv I. \tag{†}$$

Note that the $2^r$ products $M_1^{b_1} \cdots M_r^{b_r}$, with $(b_1, \ldots, b_r) \in \mathbb{F}_2^r$, are distinct, since they make up all of $S$ and $|S| = 2^r$. Since $M_1^0 \cdots M_r^0 = I$, the product $M_1^{b_1} \cdots M_r^{b_r}$, when $(b_1, \ldots, b_r) \neq (0, \ldots, 0)$, is an element of $S \setminus \{I\}$. Since $S$ is a stabilizer, $-I, \pm iI \notin S$ (consequence (7) of Lecture 24), and so no element of $S \setminus \{I\}$ is equal to $I$ modulo phase. Hence, (†) implies that $(a_1, \ldots, a_r) = (0, \ldots, 0)$. ■

(4) For all $i$ and $j$,

$$v_i \odot v_j = 0,$$

because $M_i$ and $M_j$ commute. In fact, $v \odot v' = 0$ for all $v, v' \in \tau(S)$, since all the elements of $S$ commute pairwise. (This is consistent with the fact that $v \odot v = 0$ for every $v$.)

**Symplectic dual.** From now on, we denote the subspace $\tau(S)$ by $W$.

**DEFINITION.** *Given a subspace $W \subseteq \mathbb{F}_2^{2n}$, define its* symplectic dual

$$W^{\perp_s} \triangleq \big\{v \in \mathbb{F}_2^{2n} \;:\; v \odot w = 0 \text{ for all } w \in W\big\}.$$

This is the orthogonal dual of Lecture 27 with the dot product replaced by the symplectic product. In this language, property (4) reads

$$W^{\perp_s} \supseteq W,$$

since every vector in $W$ is symplectically orthogonal to every vector in $W$.

**Check matrix.**

**DEFINITION.** *A* check matrix *of the stabilizer $S$, or of the stabilizer code $\mathcal{C}(S)$, is the $r \times 2n$ binary matrix whose rows are $v_1, \ldots, v_r$:*

$$H = \begin{bmatrix} \longleftarrow & v_1 & \longrightarrow \\ \longleftarrow & v_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & v_r & \longrightarrow \end{bmatrix}_{r \times 2n}.$$

The check matrix depends on the choice of the generators $M_1, \ldots, M_r$. It has the following properties.

(1) The rows of $H$ are linearly independent (by property (3) above).

(2) $v_i \odot v_j = 0$ for all $i, j$ (by property (4) above).

Further, $W = \mathrm{row}(H)$, by property (3). Property (2) implies $W^{\perp_s} \supseteq W$: every vector in $W$ is a linear combination of the rows of $H$, and by bilinearity of $\odot$, any two such linear combinations are symplectically orthogonal.

**Example.** The Shor code of Lecture 19 has the generators

$$M_1 = XXX\ XXX\ III, \quad M_3 = ZZI\ III\ III, \quad M_5 = III\ ZZI\ III, \quad M_7 = III\ III\ ZZI,$$
$$M_2 = III\ XXX\ XXX, \quad M_4 = IZZ\ III\ III, \quad M_6 = III\ IZZ\ III, \quad M_8 = III\ III\ IZZ,$$

so $n = 9$, $r = 8$ and $k = 1$. Its check matrix is the $8 \times 18$ matrix

$$H = \left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc} 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0 \\ \hline 0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \end{array}\right],$$

where the vertical line separates the $x$ part from the $z$ part, and the gaps separate the three blocks of three qubits. The $X$-type generators $M_1, M_2$ contribute rows with a zero $z$ part, and the $Z$-type generators $M_3, \ldots, M_8$ contribute rows with a zero $x$ part. The rows are clearly linearly independent since the check matrix is in row echelon form, as required by property (1). Property (2) is also easy to check. It is clear that the top two rows are symplectically orthogonal to each other; the same holds for the bottom six rows. Now pick any row $v = (x\ z)$ from the top two and any row $v' = (x'\ z')$ from the bottom six. We have $x' = z = 0$, and hence, $v \odot v' = x \cdot z'$. It is easy to verify that $x \cdot z'$ is indeed 0.

**Matrix form of the symplectic product.** Here is another restatement of property (2). Let

$$v_i = (x\ z), \quad v_j = (x'\ z'), \quad x, z, x', z' \in \mathbb{F}_2^n.$$

Then

$$\begin{aligned} v_i \odot v_j &= x \cdot z' + z \cdot x' \\ &= \begin{bmatrix} x & z \end{bmatrix} \begin{bmatrix} z'^T \\ x'^T \end{bmatrix} \\ &= \begin{bmatrix} x & z \end{bmatrix} \underbrace{\begin{bmatrix} 0_n & I_n \\ I_n & 0_n \end{bmatrix}}_{\text{call this } J} \begin{bmatrix} x'^T \\ z'^T \end{bmatrix}. \end{aligned}$$

That is,

$$v_i \odot v_j = v_i J v_j^T,$$

where $J$ is the $2n \times 2n$ permutation matrix that swaps the $x$ and $z$ halves of a vector. Note that $J^T = J$ and $J^2 = I_{2n}$; in particular, $J$ is invertible. Since the $(i,j)$ entry of $HJH^T$ is $v_i J v_j^T$, the condition $v_i \odot v_j = 0$ for all $i, j$ can be written as

$$HJH^T = 0.$$

**Computing the symplectic dual.** Recall the definition of $W^{\perp_s}$: a vector $v$ belongs to $W^{\perp_s}$ if and only if it is symplectically orthogonal to each of the $2^r$ vectors in $W$. We now show that it is enough to check whether $v$ is symplectically orthogonal to a specific set of $r$ vectors in $W$.

**CLAIM.** *With $W^{\perp_s}$ defined as above,*

$$W^{\perp_s} = \left\{ v \in \mathbb{F}_2^{2n} \,:\, v \odot v_i = 0 \text{ for all } i = 1, \ldots, r \right\}.$$

*Proof.* One direction is easy: if $v \in W^{\perp_s}$, then $v \odot v_i = 0$ for every $i$, since $v_i \in W$. So $v$ belongs to the right-hand side.

Conversely, suppose $v$ belongs to the right-hand side. Pick any $w \in W$. Since $v_1, \ldots, v_r$ is a basis of $W$, we have $w = \sum_i \alpha_i v_i$ for some $\alpha_i \in \mathbb{F}_2$. Then

$$v \odot w = v \odot \sum_i \alpha_i v_i = \sum_i \alpha_i \left( v \odot v_i \right) = \sum_i \alpha_i \cdot 0 = 0.$$

Thus $v \in W^{\perp_s}$. ∎

Observe that

$$\begin{aligned}
v \in W^{\perp_s} \quad & \text{if and only if} \quad v_i \odot v = 0 \quad \text{for all } i = 1, \ldots, r \\
& \text{if and only if} \quad v_i J v^T = 0 \quad \text{for all } i = 1, \ldots, r \\
& \text{if and only if} \quad \begin{bmatrix} \longleftarrow & v_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & v_r & \longrightarrow \end{bmatrix} J v^T = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},
\end{aligned}$$

i.e., if and only if $HJv^T = 0^T$, i.e., if and only if $v \in \text{null}(HJ)$. Hence

$$W = \text{row}(H) \quad \text{and} \quad W^{\perp_s} = \text{null}(HJ).$$

(Contrast this with $W^{\perp}$, which is equal to $\text{null}(H)$, not $\text{null}(HJ)$.) Consequently, $W^{\perp_s}$ is a subspace, and by the rank-nullity theorem,

$$\begin{aligned}
\dim\left(W^{\perp_s}\right) &= \text{nullity of } HJ \\
&= (\text{number of columns of } HJ) - \text{rank}(HJ) \\
&= 2n - \text{rank}(H) \\
&= 2n - r \\
&= 2n - (n - k) \\
&= n + k.
\end{aligned}$$

Here $\text{rank}(HJ) = \text{rank}(H)$ because $J$ is invertible, and $\text{rank}(H) = r$ because the rows of $H$ are linearly independent. Therefore,

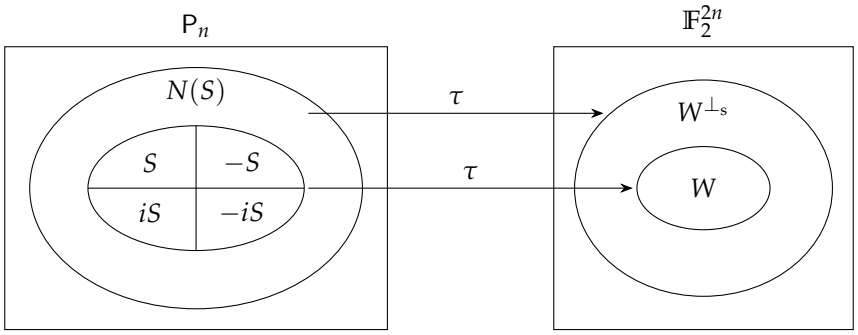
$$\left|W^{\perp_s}\right| = 2^{n+k}.$$

For a set $V \subseteq \mathbb{F}_2^{2n}$, let $\tau^{-1}(V) = \{P \in \mathsf{P}_n : \tau(P) \in V\}$ denote its preimage under $\tau$. Since each vector is the image of exactly four Paulis,

$$\left|\tau^{-1}\left(W^{\perp_s}\right)\right| = 4 \times 2^{n+k}.$$

**The normalizer.**

**CLAIM.** $\tau\big(N(S)\big) = W^{\perp_s}$. *In particular,* $N(S) = \tau^{-1}\big(W^{\perp_s}\big)$.




The four disjoint sets $S, -S, iS, -iS$ are all mapped onto $W$, and $N(S)$ is mapped onto $W^{\perp_s}$.

*Proof.* Let $P \in \mathsf{P}_n$. Then

$$\begin{aligned} P \in N(S) \quad &\text{if and only if} \quad PM_i = M_iP \quad \text{for all } i = 1, \dots, r \\ &\text{if and only if} \quad \tau(P) \odot v_i = 0 \quad \text{for all } i = 1, \dots, r \\ &\text{if and only if} \quad \tau(P) \in W^{\perp_s}. \end{aligned}$$

The first step holds because $P$ commutes with every element of $S$ if and only if it commutes with the generators $M_1, \dots, M_r$ (Lecture 26), the second step is the symplectic-product claim of §28.1, and the third step is the claim above. ■

**COROLLARY.** $|N(S)| = 4 \times 2^{n+k}$.

This proves the size of the normalizer stated without proof in Lecture 26.

We now state another observation which was used during the lecture but not emphasized. A Pauli $P$ belongs to $\pm S \cup \pm iS$ if and only if $\tau(P) \in W$ because $\tau$ ignores phase and $S$ and $W$ are in a one-to-one correspondence. To analyze the error correction capability of a stabilizer code, we need to characterize $N(S) \setminus (\pm S \cup \pm iS)$. We now use the two facts available to us: for any $P \in \mathsf{P}_n$

- $P \in N(S)$ if and only if $\tau(P) \in W^{\perp_s}$, and
- $P \in (\pm S \cup \pm iS)$ if and only if $\tau(P) \in W$.

Combining these two we arrive at the following result.

**COROLLARY.** *A Pauli* $P \in \mathsf{P}_n$ *belongs to* $N(S) \setminus (\pm S \cup \pm iS)$ *if and only if* $\tau(P) \in W^{\perp_s} \setminus W$.

## §28.3. Binary characterization of error correction conditions

**Knill–Laflamme conditions.** We now restate the Knill–Laflamme conditions for a set of errors $S_e \subset \mathsf{P}_n$ and a stabilizer code with check matrix $H$. Recall (Lecture 26) that $\mathcal{C}(S)$ corrects $S_e \subset \mathsf{P}_n$ if and only if

$$E_a^\dagger E_b \notin N(S) \setminus (\pm S \cup \pm iS) \quad \text{for all } E_a, E_b \in S_e.$$

Every element of $\mathsf{P}_n$ is either Hermitian or skew-Hermitian (Lecture 24), so $E_a^\dagger = \mu E_a$ for some $\mu \in \{\pm 1\}$. Therefore the condition is equivalent to each of the following:

$$\begin{aligned} &\mu E_a E_b \notin N(S) \setminus (\pm S \cup \pm iS), \\ &E_a E_b \notin N(S) \setminus (\pm S \cup \pm iS), \\ &\tau(E_a) + \tau(E_b) \notin W^{\perp_s} \setminus W. \end{aligned}$$

The second line follows from the first because the set $N(S) \setminus (\pm S \cup \pm iS)$ is closed under multiplication by any phase $\mu \in \{\pm 1, \pm i\}$. The third line follows from the second because $\tau(E_a E_b) = \tau(E_a) + \tau(E_b)$.

**THEOREM.** *Let $\mathcal{C}(S)$ be a stabilizer code with check matrix $H$, and let $W = \mathrm{row}(H)$ and $W^{\perp_s} = \mathrm{null}(HJ)$. Then $\mathcal{C}(S)$ corrects $S_e \subset \mathsf{P}_n$ if and only if*

$$\tau(E_a) + \tau(E_b) \notin W^{\perp_s} \setminus W \quad \text{for all } E_a, E_b \in S_e.$$

Everything in this condition is in terms of matrices and vectors over $\mathbb{F}_2$.

**Distance of the code.** Let $P \in \mathsf{P}_n$, with

$$P = \mu\, A_1 \otimes \cdots \otimes A_n, \quad \tau(A_i) = (x_i\, z_i),$$

so that $\tau(P) = v = (x\, z)$ with $x, z \in \mathbb{F}_2^n$. The factor $A_i$ is not $I$ if and only if $x_i = 1$ or $z_i = 1$. Therefore,

$$\begin{aligned} \mathrm{wt}(P) &= \#\{i \ : \ x_i \vee z_i = 1\} \\ &= \text{number of ones in the vector } x \vee z, \end{aligned}$$

where $\vee$ denotes the logical OR, applied component-wise.

**DEFINITION.** *The* symplectic weight *of $(x\ z) \in \mathbb{F}_2^{2n}$ is the number of ones in $x \vee z$. We denote it by* $\mathrm{swt}(x\ z)$.

Thus $\mathrm{wt}(P) = \mathrm{swt}(\tau(P))$. By Lecture 26, the distance of $\mathcal{C}(S)$ is

$$\begin{aligned} d &= \min\big\{\mathrm{wt}(P) \ : \ P \in N(S) \setminus (\pm S \cup \pm iS)\big\} \\ &= \min\big\{\mathrm{swt}(v) \ : \ v \in W^{\perp_s} \setminus W\big\}, \end{aligned}$$

where the second equality holds because $N(S) \setminus (\pm S \cup \pm iS) = \tau^{-1}(W^{\perp_s} \setminus W)$ and $\mathrm{wt}(P) = \mathrm{swt}(\tau(P))$.

We have thus proved the following.

**THEOREM.** *Let $H$ be the check matrix of the stabilizer code $\mathcal{C}(S)$ and let $W = \mathrm{row}(H)$. Then the distance of $\mathcal{C}(S)$ is*

$$d = \min\big\{\mathrm{swt}(v) \ : \ v \in W^{\perp_s} \setminus W\big\}.$$

The following example was not done during the lecture.

**Example.** Consider the Shor code with the check matrix $H$ of §28.2 ($n = 9$, $r = 8$, $k = 1$). We find $W^{\perp_s} = \mathrm{null}(HJ)$ directly from the claim of §28.2: $v = (x\ z) \in W^{\perp_s}$ if and only if $v \odot v_i = x \cdot z_i + z \cdot x_i = 0$ for each row $v_i = (x_i\ z_i)$ of $H$.

- The rows from $M_3, \ldots, M_8$ have $x_i = 0$, and so they give $x \cdot z_i = 0$:

  $$x_1 + x_2 = x_2 + x_3 = 0, \quad x_4 + x_5 = x_5 + x_6 = 0, \quad x_7 + x_8 = x_8 + x_9 = 0.$$

  That is, $x$ is constant on each block of three qubits:

  $$x = (a\ a\ a\ \ b\ b\ b\ \ c\ c\ c) \quad \text{for some } a, b, c \in \mathbb{F}_2. \tag{$*$}$$

- The rows from $M_1, M_2$ have $z_i = 0$, and so they give $z \cdot x_i = 0$:

  $$\begin{aligned} z_1 + z_2 + z_3 + z_4 + z_5 + z_6 &= 0, \\ z_4 + z_5 + z_6 + z_7 + z_8 + z_9 &= 0. \end{aligned}$$

  Split the vector $z$ into three blocks (of three bits each) and let $p_j$ denote the parity (the sum over $\mathbb{F}_2$) of the three entries of $z$ in block $j$. These two equations say $p_1 + p_2 = 0$ and $p_2 + p_3 = 0$, i.e.,

  $$p_1 = p_2 = p_3. \tag{$**$}$$

That is, $(x\ z) \in W^{\perp_s}$ if and only if $(*)$ and $(**)$ hold.

On the other hand, $W = \mathrm{row}(H)$ consists of the vectors $(x\ z)$ with

$$x \in \big\{(0\,0\,0\ 0\,0\,0\ 0\,0\,0),\ (1\,1\,1\ 1\,1\,1\ 0\,0\,0),\ (0\,0\,0\ 1\,1\,1\ 1\,1\,1),\ (1\,1\,1\ 0\,0\,0\ 1\,1\,1)\big\},$$

i.e., $a + b + c = 0$, and with $z$ having even parity in every block, i.e., $p_1 = p_2 = p_3 = 0$.

Therefore, a vector $v = (x\ z) \in \mathbb{F}_2^{2n}$ lies in $W^{\perp_s}$ but not in $W$ if and only if

(a) $a + b + c = 1$, or

(b) $p_1 = p_2 = p_3 = 1$.

In case (a), at least one of $a, b, c$ equals 1, so $x$ contains a whole block of three 1s and this implies that $\mathrm{swt}(v) \geq 3$. In case (b), every block of $z$ has odd parity, hence contains at least one 1, and again $\mathrm{swt}(v) \geq 3$. Thus, we have $\mathrm{swt}(v) \geq 3$ if $v \in W^{\perp_s} \setminus W$.

On the other hand, we observe that

$$v = (1\,1\,1\ 0\,0\,0\ 0\,0\,0\ \ 0\,0\,0\ 0\,0\,0\ 0\,0\,0)$$

indeed belongs to $W^{\perp_s}$ and does not belong to $W$. This vector has symplectic weight exactly 3. Hence $d = 3$, and the Shor code is a $[\![9, 1, 3]\!]$ code.

# *Lecture 29*

**Agenda.** In this lecture we will get introduced to classical linear codes. We will then see how two classical codes can be combined using the CSS construction to arrive at a quantum code. The stabilizer formalism, and the CSS technique in particular, acts as a bridge to import code constructions from the classical setup to the quantum world.

## §29.1. Recap

In Lecture 28 we introduced the map

$$\tau : \mathsf{P}_n \to \mathbb{F}_2^{2n}, \qquad \mu\, X^{x_1}Z^{z_1} \otimes \cdots \otimes X^{x_n}Z^{z_n} \longmapsto (x_1 \ \ldots \ x_n \ z_1 \ \ldots \ z_n).$$

To describe a stabilizer code $\mathcal{C}(S)$ it suffices to describe $S$, and to describe $S$ it suffices to describe its generators $M_1, \ldots, M_r$. Applying $\tau$, these are described by the vectors

$$v_1, \ldots, v_r \in \mathbb{F}_2^{2n}, \qquad v_i = \tau(M_i).$$

These $r$ row vectors are stacked vertically to obtain the check matrix

$$H = \begin{bmatrix} \longleftarrow & v_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & v_r & \longrightarrow \end{bmatrix}_{r \times 2n},$$

and we showed that

$$W \triangleq \mathrm{row}(H) = \tau(S) = \tau(\pm S \cup \pm iS) \subseteq \mathbb{F}_2^{2n},$$
$$W^{\perp_{\mathrm{s}}} = \mathrm{null}(HJ) = \tau\big(N(S)\big),$$

and that the distance of $\mathcal{C}(S)$ is

$$d\big(\mathcal{C}(S)\big) = \min\big\{\mathrm{swt}(v) \ : \ v \in W^{\perp_{\mathrm{s}}} \setminus W\big\}.$$

Note that any matrix $H$ that satisfies the following two properties forms the check matrix of some stabilizer code:

- the rows are linearly independent (this ensures that the number of minimal generators of the stabilizer group equals the number of rows of $H$, and the stabilizer does not contain $-I$); and
- the rows are symplectically orthogonal to each other (this ensures that the stabilizer generators are pairwise commuting).

**Specifying a code by its check matrix.** Typically, a stabilizer code is specified using its check matrix $H$. But each row of $H$ identifies a Pauli only modulo the phase:

$$\tau^{-1}(v_i) = \{M_i, -M_i, iM_i, -iM_i\}.$$

The last two are skew-Hermitian, and hence cannot belong to a stabilizer (every element of a stabilizer is Hermitian, Lecture 24). So we can choose either $M_i$ or $-M_i$, i.e., we choose $s_iM_i$ where $s_i \in \{\pm 1\}$. Thus, given $v_1, \ldots, v_r$, we obtain a stabilizer by choosing the generators

$$s_1M_1, \ \ldots, \ s_rM_r \quad \text{for some choice of } s_1, \ldots, s_r \in \{\pm 1\},$$

and so there are $2^r$ possible stabilizers with the same check matrix. By Question 5 of Homework 11, all of them have the same

- number of logical qubits $k$;
- normalizer $N(S)$, and the same set $\pm S \cup \pm iS$;

Since the distance and the set of correctable Pauli errors depend solely on $N(S) \setminus (\pm S \cup \pm iS)$, and since this set is the same for all these $2^r$ codes, we immediately see that the distance and the (Pauli) error correction capabilities of these codes are identical. These $2^r$ stabilizer codes are considered equivalent to each other.

## §29.2. Classical codes

We now review the basics of classical error correcting codes with the aim of using this background to understand the CSS construction. We start with the definition of a classical linear code.

**DEFINITION.** *A* classical linear code*, or simply a* classical code*, of length $n$ is a subspace of $\mathbb{F}_2^n$. The vectors present in a code are called* codewords*.*

EXAMPLE. *The repetition code of length $n$ is $V = \{(0\ 0\ \cdots\ 0), (1\ 1\ \cdots\ 1)\}$. This is clearly a subspace since it is closed under addition.*

A classical code can be used to protect data against errors in a communication or a storage scenario. We spread the information present in $k$ classical bits $m_1, \ldots, m_k$ into $n$ coded bits (with $n \geq k$) $x_1, \ldots, x_n$, such that if any $t$ or fewer bits among $x_1, \ldots, x_n$ are flipped (for a small enough value of $t$) a decoder can retrieve $m_1, \ldots, m_k$ from the noisy version of $x_1, \ldots, x_n$. In a communication scenario, the encoding happens at the transmitter, noise affects the codeword during transmission through a communication medium (or as the data waits in a storage medium), and decoding is performed at the receiver to clean up the noise and retrieve the raw message bits.

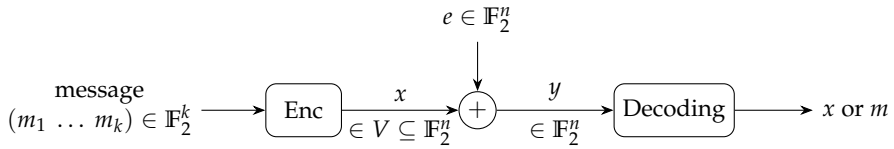
**Encoding.** Suppose $V$ has dimension $k$. Pick any basis $g_1, \ldots, g_k \in V$. This basis is used in communication as follows. We encode $k$ message bits $m_1, \ldots, m_k \in \mathbb{F}_2$ into the codeword

$$x = \sum_{i=1}^{k} m_i g_i \in V.$$

Since $g_i \in V$ for all $i$, and since $V$ is closed under linear combinations, we have $x \in V$. The map

$$\mathbb{F}_2^k \to V, \qquad (m_1\ \ldots\ m_k) \mapsto \sum_i m_i g_i$$

is a one-to-one correspondence, since $g_1, \ldots, g_k$ is a basis of $V$. Note that both $\mathbb{F}_2^k$ and $V$ are $k$-dimensional vector spaces over $\mathbb{F}_2$ and have the same size: $2^k$. The codeword is sent through a noisy channel, which adds an error vector $e \in \mathbb{F}_2^n$, and the decoder must recover $x$, or equivalently $m$, from the received vector $y \in \mathbb{F}_2^n$:




**Errors.** The received vector is

$$y = x + e \quad \text{over } \mathbb{F}_2,$$

where $e$ is the *error vector*. That is, for $i = 1, \ldots, n$, we have $y_i = x_i + e_i$, i.e.,

$$y_i = \begin{cases} x_i, & \text{if } e_i = 0 \quad \text{(no bit flip)}, \\ 1 + x_i, & \text{if } e_i = 1 \quad \text{(a bit flip)}. \end{cases}$$

**DEFINITION.** *The* Hamming weight *of* $u \in \mathbb{F}_2^n$ *is*

$$w_H(u) = \#\{i \,:\, u_i = 1\}.$$

So $w_H(e)$ is the number of bit flips introduced by the noise. At the decoder we want to identify and undo the bit flips. The *decoding problem* is to identify $x$ or $m$, given

(i) the received vector $y$, and

(ii) the basis $g_1, \ldots, g_k$ (the basis describes the code $V$ and also the encoding map $(m_1, \ldots, m_k) \mapsto (x_1, \ldots, x_n)$).

In particular, the receiver does not know the location of the bit flips, and this is precisely what it wants to figure out: given $y$, decoding $x$ is the same problem as decoding $e$ since

$$x = y + e.$$

Thus, the decoding problem is equivalent to the problem of finding $e$ given $y, g_1, \ldots, g_k$.

**A specific case: $t$-error correction.** As in the quantum case, a code cannot be used to correct an arbitrary set of errors. The most popular model in the classical coding literature is to assume that the error introduced by the channel will flip only a small number of codeword bits. This model is called $t$-error correction. We will assume that the error vector has Hamming weight at most $t$, i.e.,

$$e \in \mathcal{B}_t \triangleq \left\{e \in \mathbb{F}_2^n \,:\, w_H(e) \leq t\right\}.$$

The set $\mathcal{B}_t$ is called the *Hamming ball of radius $t$*. We want to identify the criterion under which a code can correct any error in $\mathcal{B}_t$. For simplicity, we will assume that the receiver uses *syndrome decoding*. When decoding is performed with the objective of correcting the errors in $\mathcal{B}_t$, it is known as *bounded distance decoding* (BDD).

**Parity-check matrix.** Assume $H$ is a matrix such that

$$\text{null}(H) = V.$$

To identify such an $H$: first identify the subspace $V^\perp$, then find any basis for $V^\perp$, and use these basis vectors as the rows of $H$. Then

$$Hx^T = 0^T \iff x \in V,$$

i.e., we claim that $\text{null}(H) = V$. This follows from the following claim.

**CLAIM.** *If $H$ is such that* $\text{row}(H) = V^\perp$, *then* $\text{null}(H) = V$.

*Proof.* We know that the row space and the null space of any matrix are orthogonal duals of each other. Since $\left(V^\perp\right)^\perp = V$ the result follows. ■

**DEFINITION.** *A matrix $H$ with* $\text{null}(H) = V$ *is called a* parity-check matrix *of the classical code $V$. That is,*

$$V = \text{null}(H) = \left\{x \in \mathbb{F}_2^n \,:\, Hx^T = 0^T\right\}.$$

REMARK. *There is no guaranteed relation between $V$ and $V^\perp$. All of the following are possible (Lecture 27): $V \cap V^\perp = \{0\}$, or $V \subseteq V^\perp$, or $V^\perp \subseteq V$, or $V = V^\perp$, or some other non-trivial intersection between $V$ and $V^\perp$.*

**Syndrome decoding.** We are given $y$ and $H$ (and $g_1, \ldots, g_k$), which describe the code $V$, and we assume $e \in \mathcal{B}_t$. The goal is to find $e$; once $e$ is known, $y + e$ equals $x$, and $x$ in turn determines $m$. We compute

$$\begin{aligned} s^T &\triangleq Hy^T \\ &= H(x+e)^T \\ &= Hx^T + He^T \\ &= He^T, \end{aligned}$$

since $x \in V = \text{null}(H)$. The vector $s$ is called the *syndrome* of the error $e$. It is computed from $y$ alone, and its value depends only on $e$, not on the transmitted codeword $x$. At this point, we see that we have partial information about $e$: we know that $e$ satisfies $He^T = s^T$. With no other restriction on $e$, it will be impossible to infer the value of $e$ from $He^T$ (unless $H$ is invertible; but in this case the code $V = \{0\}$ is trivial and can carry no information). This is the point at which our assumption $e \in \mathcal{B}_t$ is useful. The problem is to solve a system of linear equations with non-linear constraints:

$$\text{find } e \text{ such that } He^T = s^T, \text{ under the condition } e \in \mathcal{B}_t.$$

In this lecture we will not be concerned with the computational complexity of solving this problem; we will only be interested in identifying codes $V$ for which this problem has a unique solution. Uniqueness guarantees that the correct error $e$ can be identified by the decoder given access to sufficient computational resources.

**Feasibility.** Is it possible to identify $e$ from $He^T$, given that $e \in \mathcal{B}_t$? This is the same as asking: for any two distinct $e_1, e_2 \in \mathcal{B}_t$, do we have

$$He_1^T \neq He_2^T \,?$$

If so, we can correct any error from $\mathcal{B}_t$, since distinct errors have distinct syndromes. This condition is equivalent to each of the following:

$$\begin{aligned} &He_1^T + He_2^T \neq 0, \\ &H(e_1+e_2)^T \neq 0, \\ &e_1 + e_2 \notin V, \end{aligned}$$

for all $e_1, e_2 \in \mathcal{B}_t$ with $e_1 \neq e_2$. Since $e_1 + e_2 = 0$ exactly when $e_1 = e_2$, the last condition can also be written as

$$e_1 + e_2 \notin V \setminus \{0\} \quad \text{for all } e_1, e_2 \in \mathcal{B}_t. \tag{$*$}$$

We call $(*)$ the *t-error correction condition*, and we say $V$ is *t-error correcting* if it holds. Note that $(*)$ depends only on the code $V$, not on the choice of $H$. In general, there are many choices of parity-check matrix for a given code $V$; any of them can be used for syndrome decoding.

REMARK. *Compare $(*)$ with the conditions for correcting Pauli errors using stabilizer codes:*

$$E_a^\dagger E_b \notin N(S) \setminus (\pm S \cup \pm iS).$$

*Addition in $(*)$ is replaced by matrix multiplication, $V$ by $N(S)$, and $V \setminus \{0\}$ by $N(S) \setminus (\pm S \cup \pm iS)$; equivalently, $\{0\}$ is replaced by $\pm S \cup \pm iS$. In the classical case, errors act on codewords via addition; in the quantum case, they act via matrix-vector multiplication. In the classical case, $V$ is the set of all error vectors that map a codeword to a codeword (via addition); in the quantum case, $N(S)$ is the set of all Paulis that map codewords to codewords. The error vector $e = 0$ acts trivially on a classical codeword; the Paulis in $\pm S \cup \pm iS$ act trivially on quantum codewords.*

**Distance.** As in the quantum scenario, the error correction condition $(*)$ can be expressed in terms of a single parameter of the code.

**DEFINITION.** *The* distance *or the* minimum distance *of a classical code $V$ is*

$$d(V) \triangleq \min\{w_H(u) \,:\, u \in V,\ u \neq 0\}.$$

We now rephrase the error correction condition in terms of $d(V)$.

**THEOREM.** *$V$ is $t$-error correcting if and only if $d(V) \geq 2t+1$.*

*Proof.* ($\Leftarrow$) Assume $d(V) \geq 2t+1$. If $x \in V$ and $x \neq 0$, then $w_H(x) \geq d(V) \geq 2t+1$. We need to show that for all $e_1, e_2 \in \mathcal{B}_t$ with $e_1 \neq e_2$, we have $H(e_1+e_2)^T \neq 0$. First, $e_1+e_2 \neq 0$ since $e_1 \neq e_2$. Also,

$$w_H(e_1+e_2) \leq w_H(e_1) + w_H(e_2) \qquad \text{(triangle inequality)},$$

since $e_1+e_2$ can have a 1 only in positions where $e_1$ or $e_2$ has a 1. Therefore, $e_1+e_2$ has weight at most $2t$. Hence $e_1+e_2$ is not a codeword, since every non-zero codeword has weight at least $2t+1$.

($\Rightarrow$) This direction was skipped in class. Suppose $d(V) \leq 2t$, and let $u \in V$ be a non-zero codeword with $w_H(u) = d(V)$. Split the positions of the 1s of $u$ into two parts, with $\lceil d(V)/2 \rceil \leq t$ and $\lfloor d(V)/2 \rfloor \leq t$ positions respectively, and let $e_1$ and $e_2$ be the vectors with 1s exactly in these two parts. Then $e_1, e_2 \in \mathcal{B}_t$ and $e_1 + e_2 = u \in V \setminus \{0\}$, which violates $(*)$. (Indeed $e_1 \neq e_2$, and the two errors have the same syndrome.) ■

A fundamental problem in classical coding theory is to identify codes that have large distance and can be decoded with low complexity. We denote a classical linear code of length $n$, dimension $k$ and distance $d$ as $[n,k,d]$. For given values of $n$ and $k$, one would like to identify and use codes with as large a value of $d$ as possible so that we can correct as many bit flips as possible.

EXAMPLE. *The repetition code of length $n$ is an $[n,1,n]$ code: it has dimension 1, and its only non-zero codeword $(1\ 1\ \cdots\ 1)$ has weight $n$. Another example is the $[7,4,3]$ Hamming code, which is studied in Homework 12.*

**A brief history.** Classical coding theory started in the late 1940s. Examples of well-known families of classical codes are BCH codes, Reed-Muller codes, Reed-Solomon codes, LDPC codes, polar codes, etc. The stabilizer framework acts as a bridge between these classical codes and quantum codes.

## §29.3. CSS codes

CSS (Calderbank-Shor-Steane) codes are a specific class of stabilizer codes. They are the most popular stabilizer codes. Examples include the Shor code, the Steane code, surface codes (used by Google), quantum LDPC codes, and bivariate bicycle codes (used by IBM).

**Construction.** Start with two classical codes $V_1, V_2$, both of length $n$. For each $j = 1, 2$:

- identify a basis for $V_j^\perp$;
- use these basis vectors as rows to obtain a matrix $H_j$.

Then $V_j = \text{null}(H_j)$, and $H_j$ has linearly independent rows. Let

$$k_j = \dim(V_j).$$

Then the number of rows in $H_j$ is $\dim(V_j^\perp) = n - k_j$.

Now, we must also pick $V_1$ and $V_2$ such that

$$V_2^\perp \subseteq V_1,$$

or, equivalently (taking orthogonal duals of both sides and using $(W^\perp)^\perp = W$),

$$V_2 \supseteq V_1^\perp.$$

Thus, this dual-containing condition on $V_1$ and $V_2$ is symmetric. We construct the CSS code through its check matrix:

$$H \triangleq \left[\begin{array}{c|c} 0 & H_1 \\ \hline H_2 & 0 \end{array}\right] \begin{array}{l} \} \; n-k_1 \text{ rows} \\ \} \; n-k_2 \text{ rows} \end{array}$$

where the vertical line separates the $x$ part from the $z$ part. The first $n-k_1$ rows of the form $(0\ u)$ correspond to $Z$-type Paulis, and the last $n-k_2$ rows of the form $(v\ 0)$ to $X$-type Paulis. Therefore, the number of stabilizer generators is

$$r = (n-k_1) + (n-k_2),$$

and the number of logical qubits is

$$k = n - r = n - (2n - k_1 - k_2) = k_1 + k_2 - n.$$

(Note $k \geq 0$: since $V_1^\perp \subseteq V_2$, we have $\dim(V_1^\perp) \leq \dim(V_2)$, that is, $n - k_1 \leq k_2$.)

**Is this a valid check matrix?** We need to check two things.

(1) *Are the rows linearly independent?* This is easy. A linear combination of the rows of $H$ with coefficient vectors $a$ (for the top block) and $b$ (for the bottom block) is

$$a\,(0\ \ H_1) + b\,(H_2\ \ 0) = (bH_2\ \ aH_1).$$

If this is zero, then $aH_1 = 0$ and $bH_2 = 0$, and so $a = 0$ and $b = 0$, since $H_1$ and $H_2$ have linearly independent rows.

(2) *Any two rows must be symplectically orthogonal.* Recall $(x\ z) \odot (x'\ z') = x \cdot z' + z \cdot x'$. There are three cases.

(i) Two rows from the top block, $(0 \cdots 0\ \ * \cdots *)$ and $(0 \cdots 0\ \ * \cdots *)$: both $x$ parts are zero, so the symplectic product is 0.

(ii) Two rows from the bottom block: the other way around; both $z$ parts are zero.

(iii) One row from each block, $(0\ u)$ with $u \in V_1^\perp$, and $(v\ 0)$ with $v \in V_2^\perp$, since every row of $H_i$ belongs to $V_i^\perp$. Their symplectic product is $0 \cdot 0 + u \cdot v = u \cdot v$. Now

$$u \in V_1^\perp \implies u \in V_2 \quad \text{since our construction assumes } V_1^\perp \subseteq V_2,$$

and $v \in V_2^\perp$. Therefore $u \cdot v = 0$, and these two rows of $H$ are symplectically orthogonal.

**Distance.** The distance of a CSS code can be bounded in terms of the distances of the two classical codes.

**THEOREM.** *The distance of the CSS code satisfies*

$$d \geq \min\left\{d(V_1),\, d(V_2)\right\}.$$

*Proof.* This proof was not done in class. We use the distance theorem of Lecture 28,

$$d = \min\{\text{swt}(v) : v \in W^{\perp_s} \setminus W\}.$$

A vector $(x\ z) \in \mathbb{F}_2^{2n}$ lies in $W^{\perp_s} = \text{null}(HJ)$ if and only if $HJ\,(x\ z)^T = 0^T$. For the CSS check matrix, this translates into

$$H_1 x^T = 0^T \text{ and } H_2 z^T = 0^T.$$

This is the same as $x \in V_1$ and $z \in V_2$. Thus, we have

$$W^{\perp_s} = \{(x\ z) : x \in V_1, z \in V_2\}.$$

We now analyze the distance, which is the minimum symplectic weight among $W^{\perp_s} \setminus W$. Firstly, $0 \in W$ ($W$ is a subspace); hence, the distance is lower bounded by the smallest swt among all vectors in $W_s^\perp \setminus \{0\}$ since

$$W_s^\perp \setminus \{0\} \supseteq W_s^\perp \setminus W.$$

The minimum can only reduce when we enlarge a set. For any non-zero $(x\ z) \in W^{\perp_s}$, we have either $x \neq 0$ or $z \neq 0$. Further, since

$$\text{swt}((x\ z)) = w_H(x \vee z)$$

we have

$$\text{swt}((x\ z)) \geq w_H(x) \quad \text{and} \quad \text{swt}((x\ z)) \geq w_H(z).$$

At least one of $x$ or $z$ is non-zero; if $x \neq 0$ we have $w_H(x) \geq d(V_1)$, and if $z \neq 0$ we have $w_H(z) \geq d(V_2)$. Combining these observations we arrive at

$$\text{swt}((x\ z)) \geq \min\{d(V_1), d(V_2)\}.$$

■

REMARK. *The theorem above gives only a lower bound on the distance. The exact distance of a CSS code, in terms of the classical codes $V_1$ and $V_2$ and their duals, is the subject of a question in Homework 12.*

**Example: the Steane code.** The Steane code of Lectures 18 and 19 is a CSS code. Let $V$ be the $[7,4,3]$ Hamming code; it satisfies $V^\perp \subset V$ (Homework 12). Choosing $V_1 = V_2 = V$, the condition $V_2^\perp \subseteq V_1$ holds, and the CSS construction gives a code with $n = 7$ and

$$k = k_1 + k_2 - n = 4 + 4 - 7 = 1,$$

and, by the theorem above, distance $d \geq \min\{d(V_1), d(V_2)\} = 3$. A question in Homework 12 asks you to show that the distance of the Steane code is exactly 3.

**Example: Quantum Reed-Muller codes.** Reed-Muller (RM) codes are one of the first and best-known families of classical codes. These codes were invented in the early 1950s. We now give a brief description of RM codes at a level that is sufficient for us to use them in the CSS construction.

The length of every RM code is a power of 2. For each integer $m \geq 1$, there are $m+1$ distinct RM codes of length $n = 2^m$. We will denote these codes (which are subspaces of $\mathbb{F}_2^n = \mathbb{F}_2^{2^m}$) as $U_0, \ldots, U_m$. These subspaces are nested:

$$U_0 \subset U_1 \subset U_2 \subset \cdots \subset U_{m-1} \subset U_m,$$

where $U_0 = \{(0\ \cdots\ 0), (1\ \cdots\ 1)\}$ is the repetition code and $U_m = \mathbb{F}_2^{2^m}$. For $0 \leq i \leq m$,

$$\dim(U_i) = \sum_{l=0}^{i} \binom{m}{l} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{i}, \qquad d(U_i) = 2^{m-i},$$

and, for $0 \le i \le m-1$,

$$U_i^{\perp} = U_{m-1-i}.$$

These are the basic facts on RM codes. We next use them as ingredients in the CSS construction.

Pick the component codes of the CSS construction as

$$V_1 = U_i, \qquad V_2 = U_j$$

for suitable choices of $i$ and $j$. Then

$$V_2^{\perp} \subseteq V_1 \iff U_j^{\perp} = U_{m-1-j} \subseteq U_i \iff m-1-j \le i \quad (\text{for } 0 \le j \le m-1),$$

i.e., the construction is valid when $i + j \ge m-1$. The distance of the quantum code satisfies

$$d \ge \min\left\{d(V_1),\, d(V_2)\right\} = \min\left\{2^{m-i},\, 2^{m-j}\right\}.$$

EXAMPLE. *Let $m = 4$ and $i = j = 2$, so $n = 16$ and $i + j = 4 \ge m - 1 = 3$. Here $k_1 = k_2 = \dim(U_2) = 1 + 4 + 6 = 11$, so $k = k_1 + k_2 - n = 11 + 11 - 16 = 6$, and $d \ge 2^{4-2} = 4$. In this case the lower bound on the distance is exact, i.e., $d = 4$. This CSS code is the $[\![16, 6, 4]\!]$* tesseract code. *A modification of it, a $[\![16, 4, 4]\!]$ code, was implemented in hardware by Microsoft and Quantinuum in 2024.*

# *Homework 12*

1. Let $V$ be any subspace of $\mathbb{F}_2^{2n}$ (do not assume that $V \subseteq V^{\perp_s}$ or $V \subseteq V^{\perp}$).

   (a) Argue that
   $$\left(V^{\perp_s}\right)^{\perp_s} = V \text{ and } \left(V^{\perp}\right)^{\perp} = V.$$
   The second statement is in fact true for any $\mathbb{F}_2^m$, $m$ even or odd.

   (b) Under what conditions on $V$ do we have $V^{\perp_s} = V^{\perp}$?

   (c) Show that, if $V$ and $U$ are subspaces, then
   $$V \subseteq U \;\Rightarrow\; V^{\perp} \supseteq U^{\perp}.$$

2. Let $V$ be the subspace of $\mathbb{F}_2^m$ consisting of all the vectors with an even number of 1s. Identify the values of $m$ such that $V^{\perp} \subseteq V$. What happens for other values of $m$?

3. For each of the following matrices over $\mathbb{F}_2$ determine if the matrix possesses an inverse or a left inverse or a right inverse. If so, identify the inverse/a left inverse/a right inverse.

   REMARK. We say that a matrix $A$ has a left inverse if there exists a $B$ such that $BA = I$; $A$ has a right inverse if there exists a matrix $B$ such that $AB = I$. From matrix theory we know that $A$ has a left inverse if and only if it has linearly independent columns; $A$ has a right inverse if and only if it has linearly independent rows.

   (a) $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

   (b) $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

   (c) $\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$

4. Suppose an $n \times m$ binary matrix $A$ has linearly independent rows. How many distinct right inverses does $A$ have?

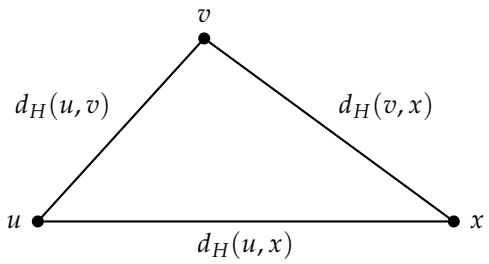
   HINT. If both $B_1$ and $B_2$ are right inverses of $A$ what can you say about the columns of $B_2 - B_1$?

5. For any binary vector $v \in \mathbb{F}_2^m$, we define its Hamming weight $w_H(v)$ to be the number of non-zero components of $v$:
   $$w_H(v) := |\{i \,:\, v_i \neq 0\}|.$$
   For two binary vectors $u, v$, we define the Hamming distance between them as the number of entries in which these two vectors differ, i.e.,
   $$d_H(u, v) := w_H(u + v).$$
   Show the following:

(a) For any $u, v \in \mathbb{F}_2^m$: $w_H(u+v) = w_H(u) + w_H(v) - 2w_H(u \wedge v)$, where $\wedge$ denotes the logical AND, applied component-wise.

REMARK. This shows that if two binary vectors have even weight their sum has even weight too. Thus, the set of all even-weighted vectors in $\mathbb{F}_2^m$ forms a subspace.

(b) *Triangle inequality.* For any three vectors $u, v, x$: $d_H(u,v) + d_H(v,x) \geq d_H(u,x)$.




Going from $u$ to $x$ via $v$ can never be shorter than going directly.

6. Let $V$ be a classical linear code of dimension $k$ and length $n$, with $k \geq 1$. Let $H$ be a parity-check matrix of $V$. Prove the following.

(a) The smallest Hamming distance between any two distinct vectors in $V$ equals the smallest weight among all non-zero vectors of $V$, that is

$$\min_{\substack{u,v \in V \\ u \neq v}} d_H(u,v) = \min_{v \in V \setminus \{0\}} w_H(v).$$

(b) Show that the minimum distance of $V$ equals the smallest number of columns of $H$ that sum to the all-zero vector. Use the fact that $V = \text{null}(H)$.

For example, if $H$ equals the matrix in question 3 (b) then the smallest number of columns of $H$ that sum to the all-zero vector is 4 since: no column vector of $H$ is all-zero, the sum of no two columns of $H$ is all-zero, and also, the sum of no three columns of $H$ is all-zero either. However, the sum of the first four columns is all-zero.

7. **Hamming codes.** Fix any $r \geq 2$ and let $n = 2^r - 1$. Let $H$ be the $r \times n$ matrix whose columns are all the distinct *non-zero* vectors in $\mathbb{F}_2^r$ (arranged in an arbitrary order). The Hamming code $V$ is defined as $V = \text{null}(H)$.

(a) Find the dimension of $V$.

(b) Find the minimum distance of $V$.

REMARK. The most famous Hamming code is the one with $r = 3$. This is a $[7,4,3]$ code, i.e., it is a classical linear code with $n = 7$, $k = 4$, $d = 3$. All Hamming codes are single-error correcting.

8. Show that the $[7,4,3]$ Hamming code $V$ satisfies $V^\perp \subset V$. This particular subspace or linear code $V^\perp$ is called the *simplex code*. List all the codewords of the code $V^\perp$. Can you identify its minimum distance?

9. **The Steane code is a CSS code.** Use the description of the Hamming and simplex codes (with parameter $r = 3$) from the previous questions to answer the following.

(a) Write the check matrix of the Steane code.

REMARK. Do you see any connections to the Hamming code $V$ and the simplex code $V^\perp$? As a CSS code, what are $V_1$ and $V_2$ here?

(b) Let $S$ be the stabilizer of the Steane code and $W = \tau(S)$. Describe the vectors in $W$ and the vectors in $W^{\perp_s}$ using the Hamming code $V$ and the simplex code $V^{\perp}$.

(c) Use this connection to Hamming codes/simplex codes and the properties of these classical codes to show that

$$\min\{\mathrm{swt}(v) : v \in W^{\perp_s} \setminus W\} = 3.$$

10. **Exact distance of CSS codes.** In general, for a CSS code that uses the classical codes $V_1$ and $V_2$, show that the exact distance of the quantum code is

$$\min\{\tilde{d}_1, \tilde{d}_2\},$$

where

$$\tilde{d}_1 = \min\{w_H(v) : v \in V_1 \setminus V_2^{\perp}\} \text{ and } \tilde{d}_2 = \min\{w_H(v) : v \in V_2 \setminus V_1^{\perp}\}.$$

Note that $\tilde{d}_i \geq d(V_i)$ for $i = 1, 2$ (simply follows from the fact $0 \in V_1^{\perp}$ and $0 \in V_2^{\perp}$). Thus, we see that the distance of the CSS code is lower bounded by $\min\{d(V_1), d(V_2)\}$.

11. Use the CSS construction and the family of Reed-Muller codes to construct a 2-error correcting quantum code. Identify the number of physical and logical qubits of your quantum code.

12. **Decoding CSS codes.** Consider a CSS code that is constructed using the classical codes $V_1$ and $V_2$. One can build a decoder for the CSS code by using the syndrome decoders of the classical codes $V_1$ and $V_2$. As in Lecture 29, consider the check matrix of the CSS code

$$H = \begin{bmatrix} 0 & H_1 \\ H_2 & 0 \end{bmatrix}.$$

Let the number of rows in $H_i$ be $r_i = n - k_i$, where $k_i = \dim(V_i)$ for $i = 1, 2$. Assume that we want to correct all Pauli errors of weight at the most $t$, and that $2t + 1 \leq d$, where $d$ is the distance of the CSS code. Let the Pauli error be

$$E = \mu X^{x_1} Z^{z_1} \otimes \cdots \otimes X^{x_n} Z^{z_n}, \ \ \mu \in \{\pm 1, \pm i\}.$$

(a) Which Paulis occur as Kronecker factors in the first $r_1$ generators of the stabilizer? What about the last $r_2$ generators?

(b) To compute the syndrome for quantum error correction we measure the observables $M_1, \ldots, M_r$ of the erroneous quantum codeword where $r = r_1 + r_2$. Let the resulting syndrome be $s \in \{\pm 1\}^{r_1 + r_2}$. Now, split this quantum syndrome into two parts, of length $r_1$ and length $r_2$, and replace the $\pm 1$ entries with $\{0, 1\} = \mathbb{F}_2$,

$$+1 \to 0 \ \text{ and } \ -1 \to 1.$$

Call these two binary vectors $s_1 \in \mathbb{F}_2^{r_1}$ and $s_2 \in \mathbb{F}_2^{r_2}$. Argue that

$$s_1 = H_1 x^T \ \text{ and } \ s_2 = H_2 z^T$$

where $x = (x_1, \ldots, x_n)$ and $z = (z_1, \ldots, z_n)$.

(c) If $2t + 1 \leq d$, where $d$ is the distance of the quantum CSS code, can we use the syndrome decoders of $V_1$ and $V_2$ to identify $x$ and $z$? Does this identify the error $E$ completely (including the phase $\mu$)? Can we recover from this error even if we do not know $\mu$?

(d) Suppose we use the syndrome decoders of $V_1$ and $V_2$ to correct $E$. Apart from all Paulis of weight less than or equal to $t$, are there any other Paulis that this decoder corrects?