BERMAN CODES

Achieving the Capacity of the Binary Erasure Channel

Lakshmi Prasad Natarajan

IIT Hyderabad

09 Feb 2024

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

BACKGROUND & MAIN RESULT

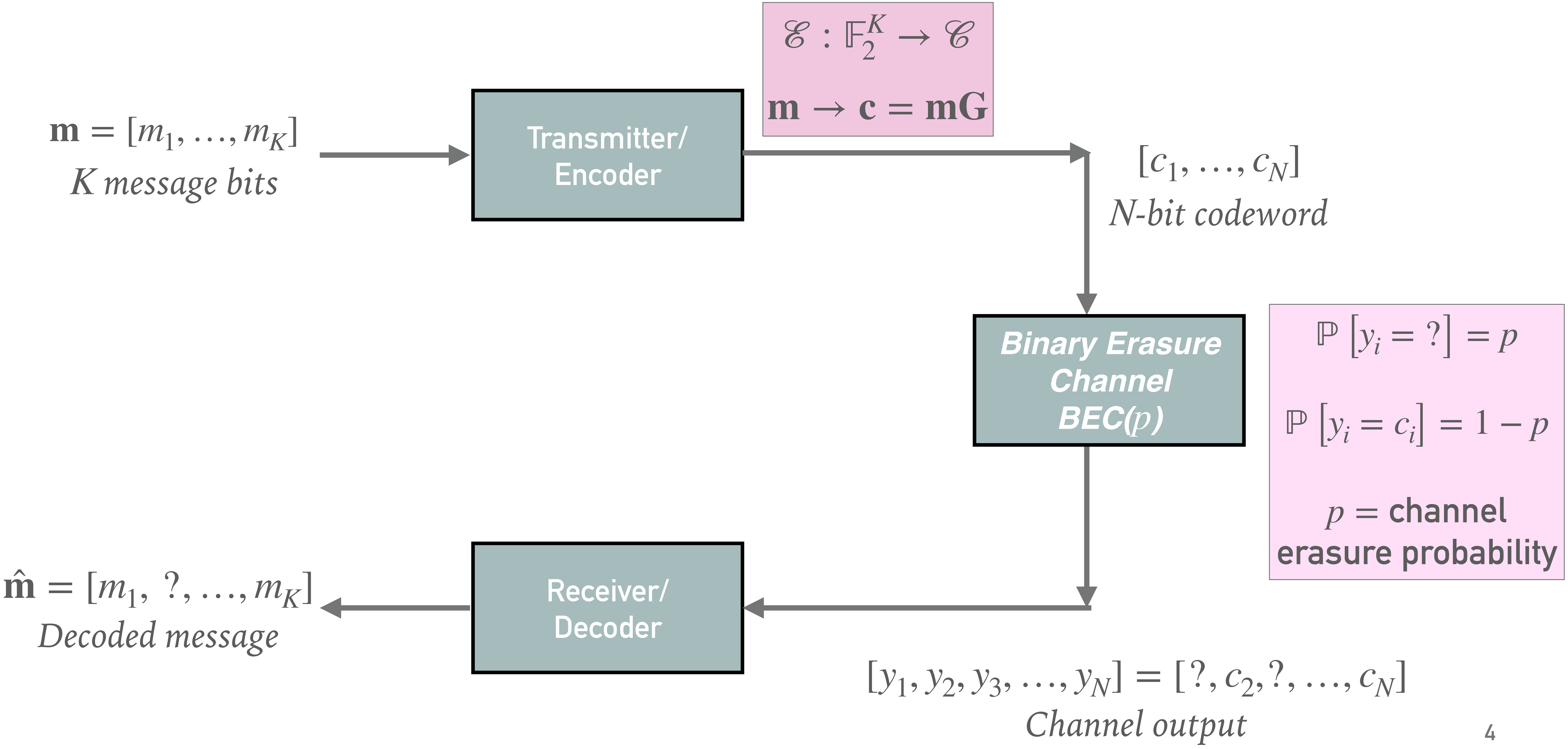
THE BINARY ERASURE CHANNEL (BEC)

- BEC(p) Channel:
  - communication medium with binary input $\{0,1\}$, ternary output $\{0,1,?\}$
  - each transmitted bit is erased with probability p (where $0 < p < 1$)
  - each use of the channel is independent of the other uses

$$\underset{\textit{Transmitted}}{(0,1,0,1,1,0)} \xrightarrow{BEC} \underset{\textit{Received}}{(0,1,?,1,?,0)}$$

$$P\left[(0,1,?,1,?,0) \text{ received} \mid (0,1,0,1,1,0) \text{ transmitted}\right] = p^2(1-p)^4$$

CODES IN DIGITAL COMMUNICATION



CODES / ERASURE CORRECTING CODES / ERROR CORRECTING CODES

$$(m_1, m_2) \xrightarrow{\textit{encoding}} (m_1, m_2, m_1 \oplus m_2) \xrightarrow{\textit{BEC}} (m_1, ?, m_1 \oplus m_2) \xrightarrow{\textit{decoding}} (m_1, m_2)$$

Message — *Transmitted Codeword* — *Received Vector* — *Message*

- **Code $\mathscr{C}$:** set of all possible transmitted sequences

  Single Parity Check Code (of length 3) $\mathscr{C} = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$

- **Codewords:** sequences/vectors in $\mathscr{C}$

- **Parameters of Interest:** **Rate** and **Probability of Decoding Failure**

CODES / ERASURE CORRECTING CODES / ERROR CORRECTING CODES

$$(m_1, m_2) \xrightarrow{\textit{encoding}} (m_1, m_2, m_1 \oplus m_2) \xrightarrow{\textit{BEC}} (m_1, ?, m_1 \oplus m_2) \xrightarrow{\textit{decoding}} (m_1, m_2)$$

Message | *Transmitted Codeword* | *Received Vector* | *Message*

- **Dimension of a (linear) code, K:** number of message bits
  Length of a code, N: number of channel uses (number of bits in the transmitted sequence)

- Robustness is increased at the cost of reduction in communication rate

$$\textbf{Rate } R = \frac{K}{N} = \frac{\text{number of message bits}}{\text{number of channel uses}}$$

BIT ERASURE RATE (BER) & CODEWORD ERASURE RATE (CER)

$$(m_1, m_2) \xrightarrow{\textit{encoding}} (m_1, m_2, m_1 \oplus m_2) \xrightarrow{\textit{BEC}} (m_1, ?, ?) \xrightarrow{\textit{decoding}} (m_1, ?)$$

Message — *Transmitted Codeword* — *Received Vector* — *Message*

- Decoding is not always successful

$$\text{BER} = \frac{1}{\text{num of message bits}} \sum_i P[m_i \text{ is not decodable}]$$

$$\text{CER} = P[\text{ entire message can not be decoded }] \qquad (\text{Note that BER} \le \text{CER})$$

Performance Metrics

$$(m_1, m_2) \xrightarrow{\textit{encoding}} (m_1, m_2, m_1 \oplus m_2) \xrightarrow{\textit{BEC}} (m_1, ?, m_1 \oplus m_2) \xrightarrow{\textit{decoding}} (m_1, m_2)$$

Message — *Transmitted Codeword* — *Received Vector* — *Message*

- ***Rate of the Code***

$$R = \frac{\text{number of messages bits}}{\text{number of code bits}} = \frac{2}{3}$$

- Higher rate ⇒ Faster Communication

- ***Bit Erasure Rate (BER)***

$$\frac{P[\hat{m}_1 = ?] + P[\hat{m}_2 = ?]}{2} = 2p^2 - p^3$$

- Smaller BER ⇒ Better Quality of Communication

A Main Problem in Coding Theory:

For a given $p \in (0,1)$, Design Codes with High Rate and BER, CER ≈ 0

CAPACITY OF THE ERASURE CHANNEL

[Shannon'48] ***Capacity Theorem for the Erasure Channel***

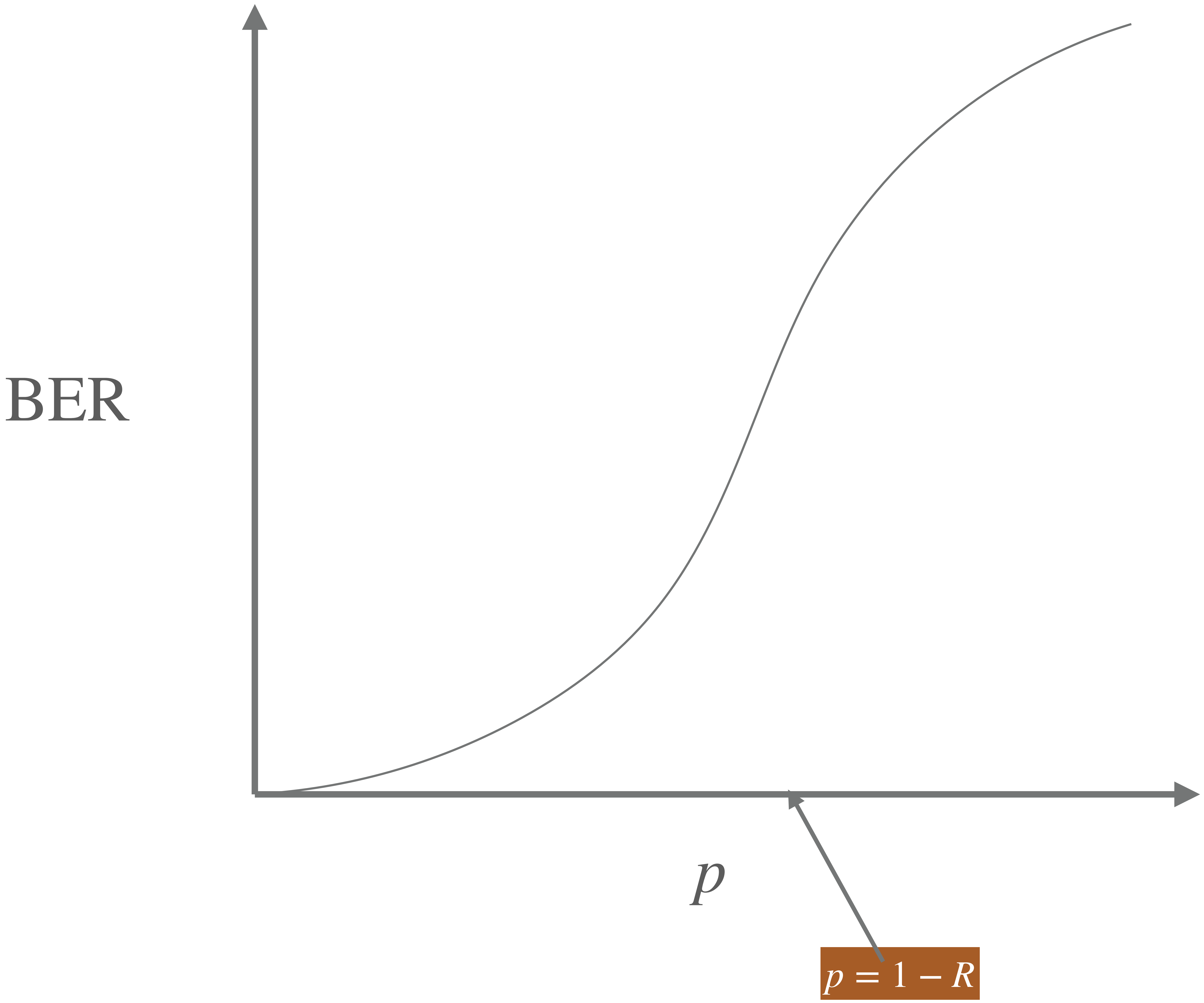
Codes can be designed with $\mathrm{BER}, \mathrm{CER} \to 0$ *if and only if* $R < 1 - p$ and $N \to \infty$

- ***Capacity*** of the binary erasure channel $\mathrm{BEC}(p)$ is $C \triangleq 1 - p$

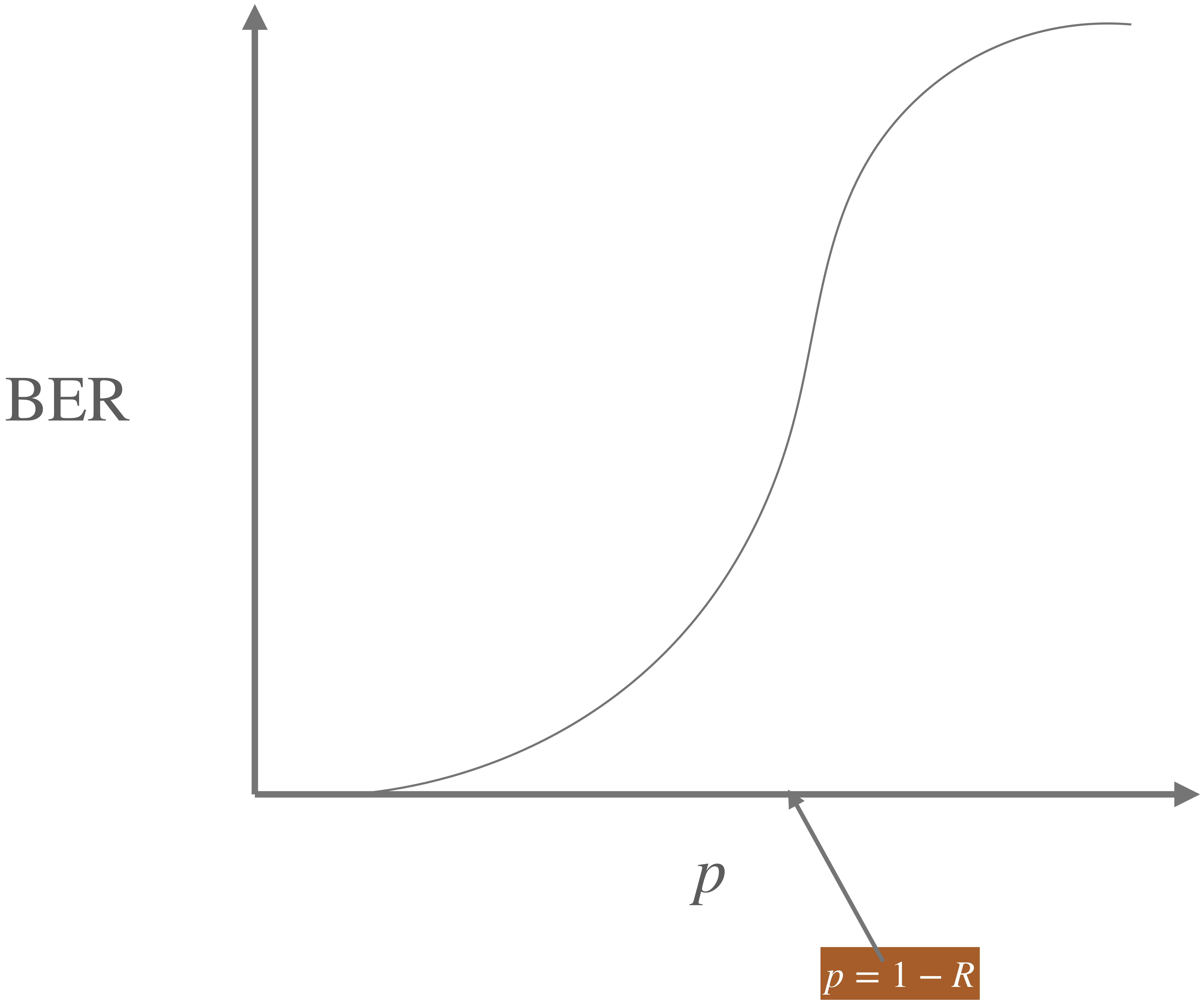
- ***Capacity-Achieving Codes for the Erasure Channel:***

  a sequence of codes for some rate R with increasing values of N such that

$$\mathrm{BER}, \mathrm{CER} \to 0 \quad \text{as} \quad N \to \infty \qquad\qquad \text{for all} \quad p < 1 - R$$



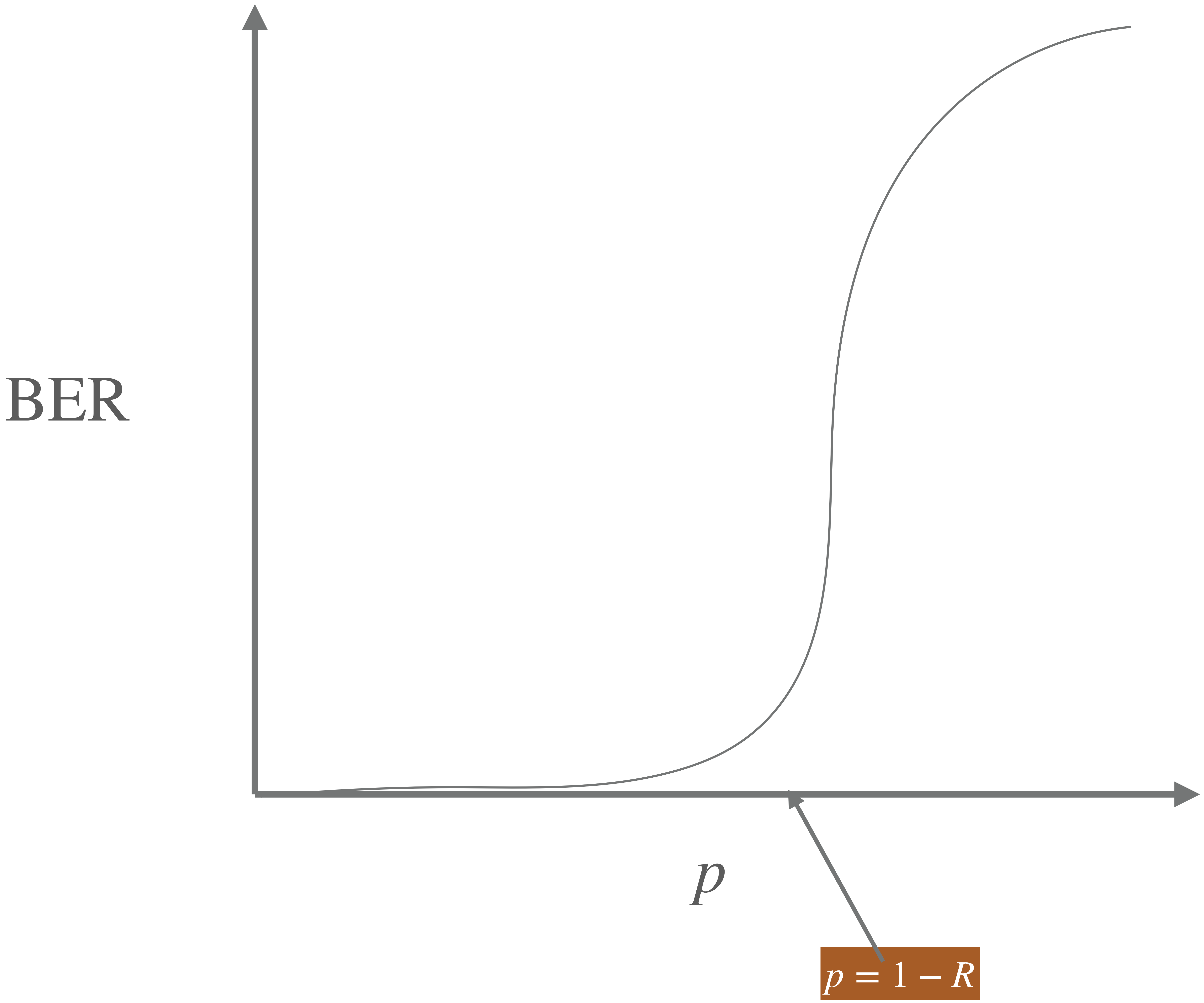
Code $\mathscr{C}_1$
Blocklength N_1
Rate R



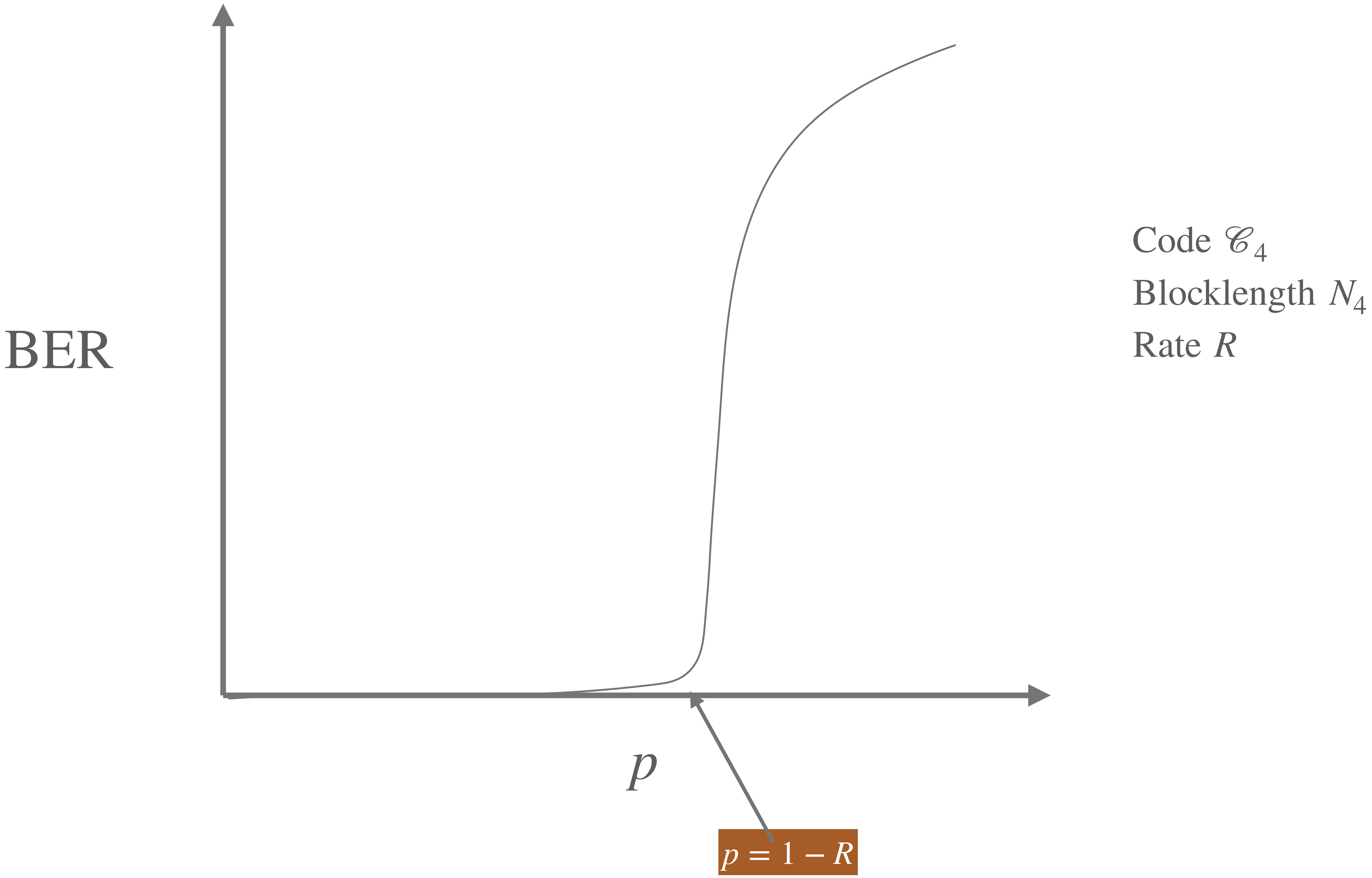
Code $\mathscr{C}_2$

Blocklength N_2

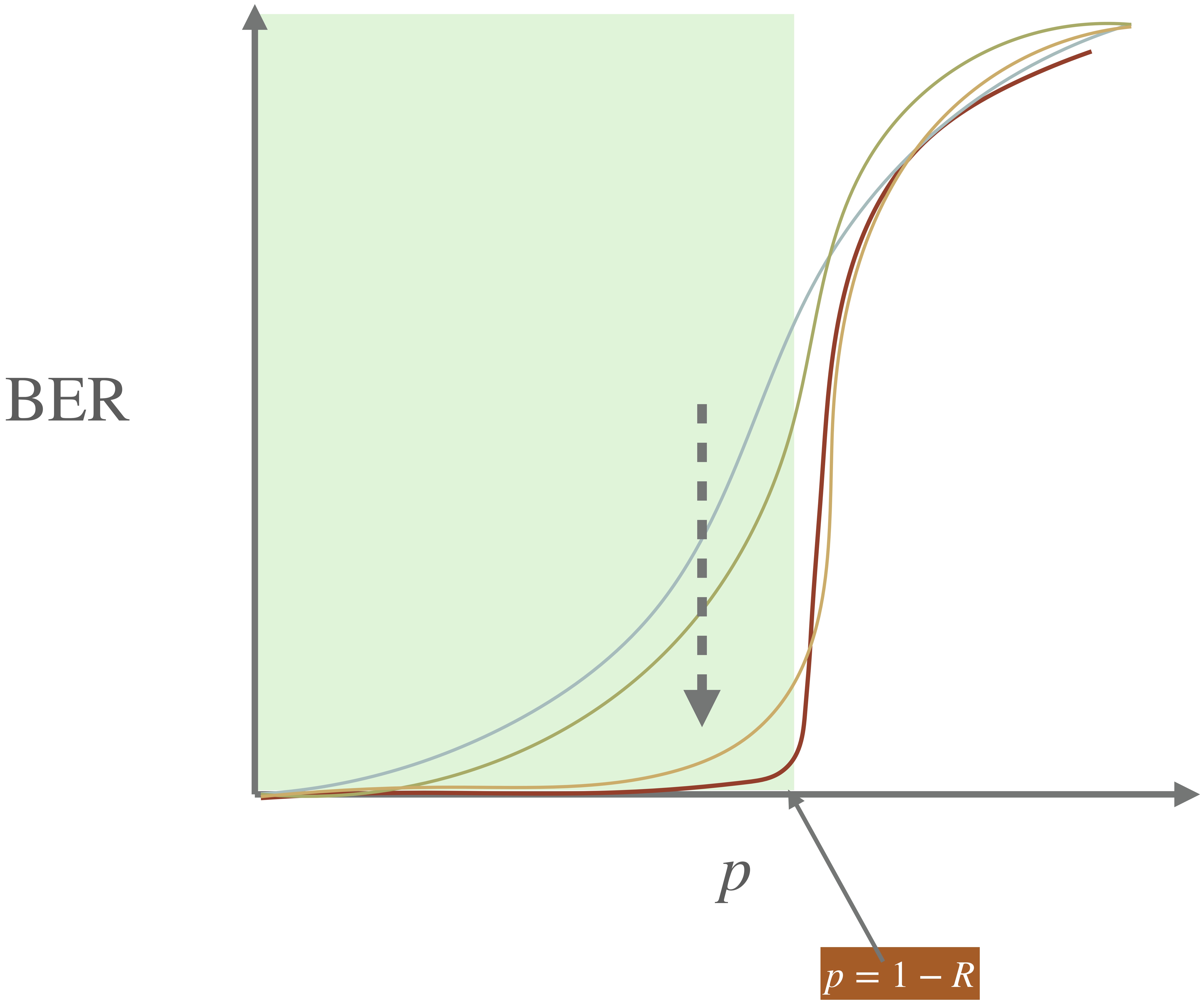
Rate R



Code $\mathscr{C}_3$
Blocklength N_3
Rate R



BER
p
$p = 1 - R$
Code $\mathscr{C}_4$
Blocklength N_4
Rate R



Codes $\mathscr{C}_1, \ldots, \mathscr{C}_4$

Blocklengths $N_1, \ldots, N_4$

Rate R

KNOWN CAPACITY-ACHIEVING CODES

<table>
<tr><td>Irregular LDPC Codes</td><td>1997</td><td>Luby, Mitzenmacher, Shokrollahi, Spielman, Stemann</td><td>BEC</td><td rowspan="5">CER → 0</td></tr>
<tr><td>Polar Codes</td><td>2009</td><td>Arıkan</td><td>BMS</td></tr>
<tr><td>Spatially-Coupled LDPC Codes</td><td>2011</td><td>Kudekar, Richardson, Urbanke</td><td>BMS</td></tr>
<tr><td>Reed-Muller Codes</td><td>2023</td><td>Abbe and Sandon</td><td>BMS</td></tr>
<tr><td>BCH Codes</td><td rowspan="2">2017</td><td rowspan="2">Kudekar, Kumar, Mondelli, Pfister, Şaşoğlu, Urbanke</td><td>BEC</td></tr>
<tr><td>Quadratic Residue Codes</td><td>BEC</td><td rowspan="3">BER → 0</td></tr>
<tr><td>Some more sequences of Cyclic Codes</td><td>2016</td><td>Kumar, Calderbank, Pfister</td><td>BEC</td></tr>
<tr><td>Berman Codes & their duals, A family of Abelian Codes</td><td>2022</td><td>Natarajan, Krishnan</td><td>BEC</td></tr>
</table>

KNOWN CAPACITY-ACHIEVING CODES

Proof is based on code symmetry (automorphism group)

Irregular LDPC Codes	1997	Luby, Mitzenmacher, Shokrollahi, Spielman, Stemann	BEC	
Polar Codes	2009		BMS	
Spatially-Coupled LDPC Codes	2011	Kudekar, Richardson, Urbanke	BMS	CER → 0
Reed-Muller Codes	2023	Abbe and Sandon	BMS	
BCH Codes	2017	Kudekar, Kumar, Mondelli, Pfister, Şaşoğlu, Urbanke	BEC	
Quadratic Residue Codes			BEC	
Some more sequences of Cyclic Codes	2016	Kumar, Calderbank, Pfister	BEC	BER → 0
Berman Codes & their duals, A family of Abelian Codes	2022	Natarajan, Krishnan	BEC	

BERMAN CODES AND THEIR DUALS

- Family of binary linear codes parametrised by 3 integers

$$n \geq 2, \quad m \geq 2, \quad r \in \{0,1,\ldots,m\}$$

- Berman Codes $\quad \mathscr{B}_n(r,m) = \left[n^m,\ \sum_{i=r+1}^{m} \binom{m}{i} (n-1)^i,\ 2^{r+1} \right]$

- Dual Berman Codes $\mathscr{D}_n(r,m) = \mathscr{B}_n(r,m)^\perp = \left[n^m,\ \sum_{i=0}^{r} \binom{m}{i} (n-1)^i,\ n^{m-r} \right]$

  - Reed-Muller codes correspond to $n = 2$: $\quad \mathscr{D}_2(r,m) = \mathrm{RM}(r,m)$

CONSTRUCTION OF BERMAN CODES AND THEIR DUALS

- **Berman Codes for n = odd prime:**
  S.D. Berman, 'Semisimple Cyclic and Abelian Codes,' *Kibernetika,* 1967
  - As ideals in commutative group algebras: *abelian codes*
  - To show that there exist abelian codes with larger min distance than cyclic codes

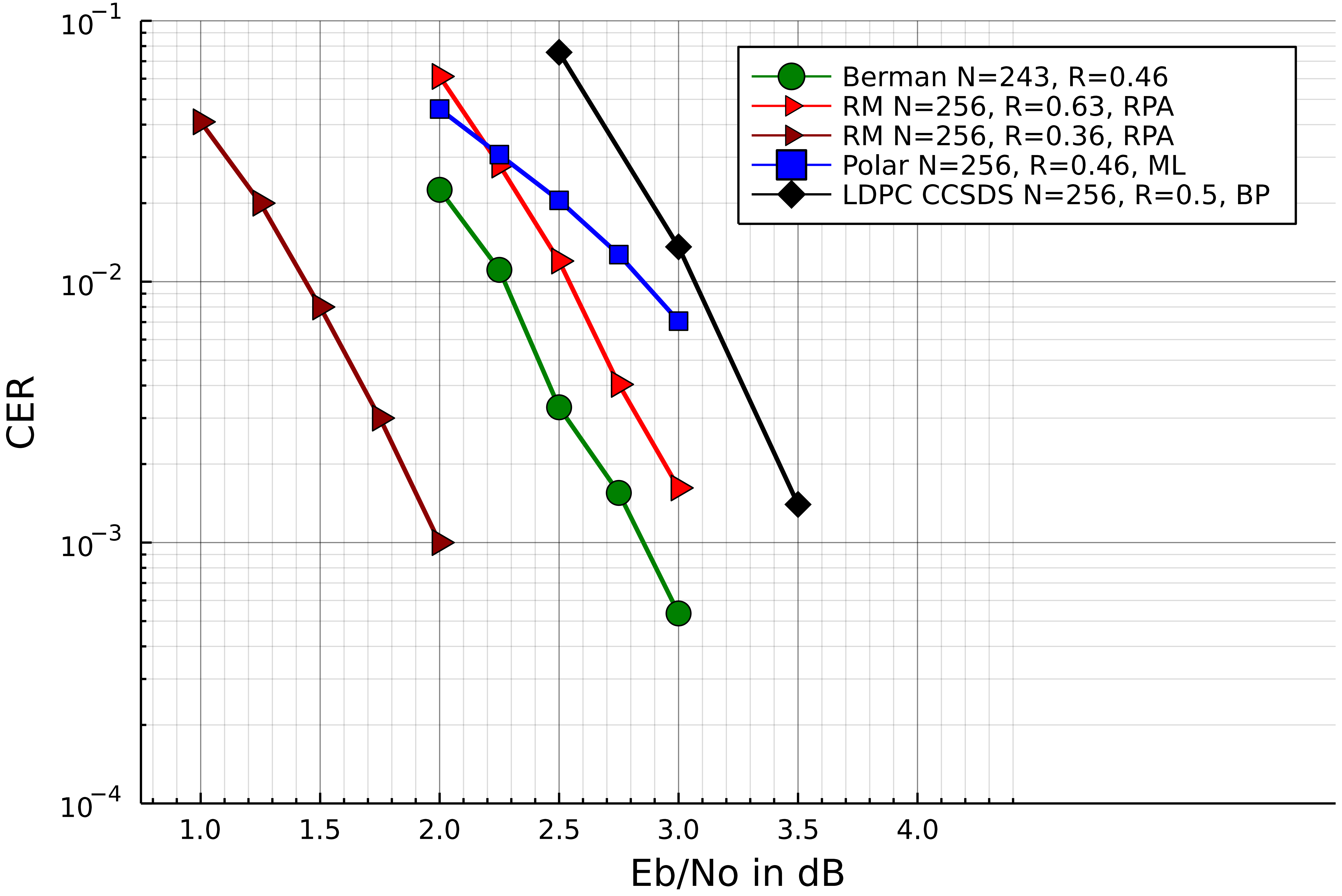
- **Dual Berman Codes**
  Blackmore and Norton, 'On a Family of Abelian Codes and their State Complexities,' *IEEE-IT,* 2001
  - As abelian codes
  - Identify an iterative group algebraic construction that works for all $n \geq 2$
  - Recognise that $n = 2$ yields RM codes

CONSTRUCTION OF BERMAN CODES AND THEIR DUALS

- **Achieve capacity of the binary erasure channel** [N. & Krishnan, *IEEE-IT,* 2023]

  - Simple Plotkin-like construction of Berman codes and their duals (like RM codes)
  - Efficient decoding up to half the minimum distance (like RM codes)
  - Identify some automorphisms
  - Use a result of [Kumar, Calderbank, Pfister, ISIT 2016] that relates automorphism group and capacity-achievability in erasure channels

BERMAN CODE $(n = 3)$ IN ADDITIVE WHITE GAUSSIAN NOISE CHANNEL



$\mathscr{B}_3(3,5)$:

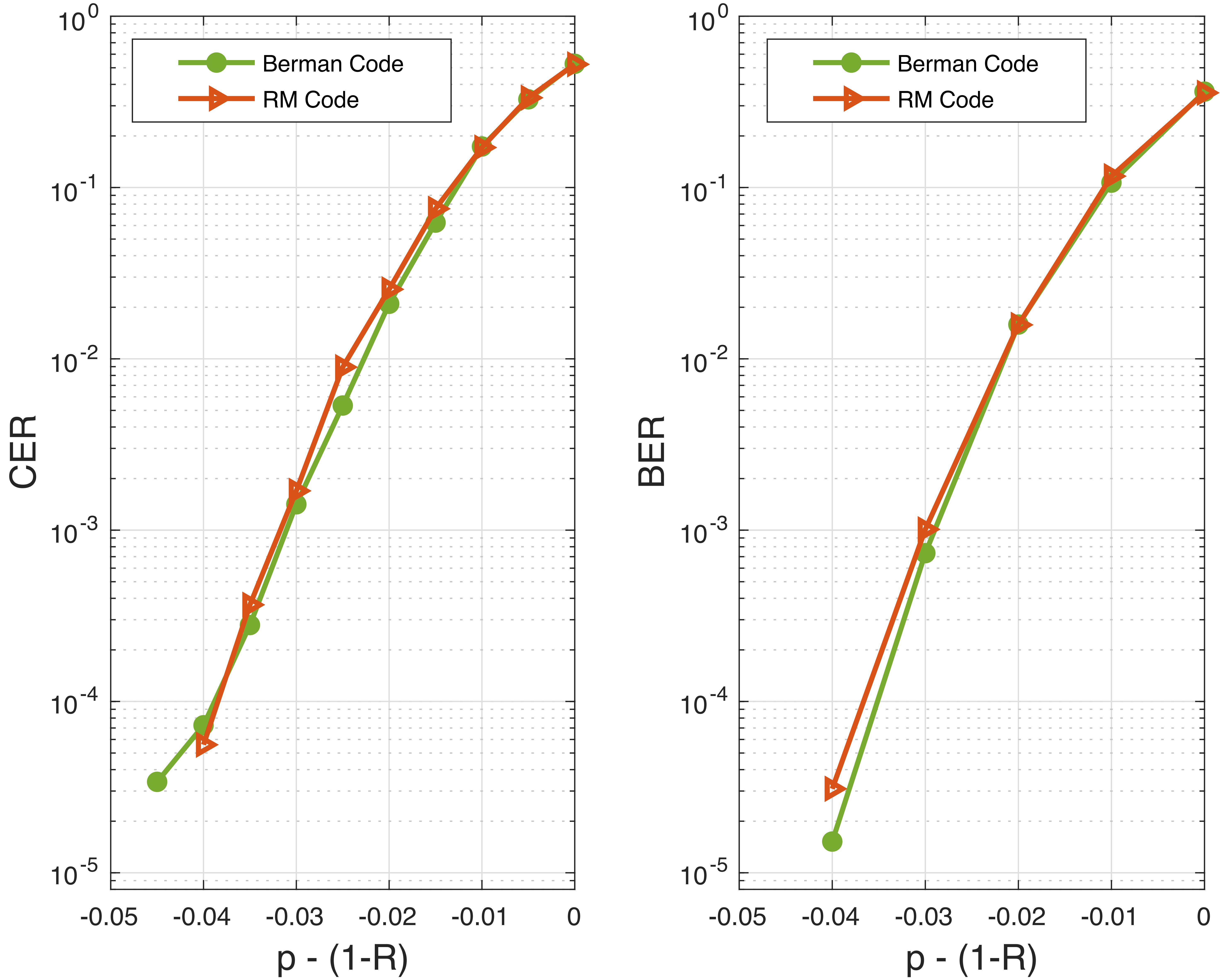
$N = 243,\ R = 0.46,\ d_{\min} = 16$

Compared to RM codes:

- Richer options for rate and length
- Seems to provide graceful trade-off between rate and CER

(Currently working on efficient decoders for Berman codes and their duals)

BERMAN CODE $(n = 3)$ VS. REED-MULLER CODE IN $\mathrm{BEC}(p)$



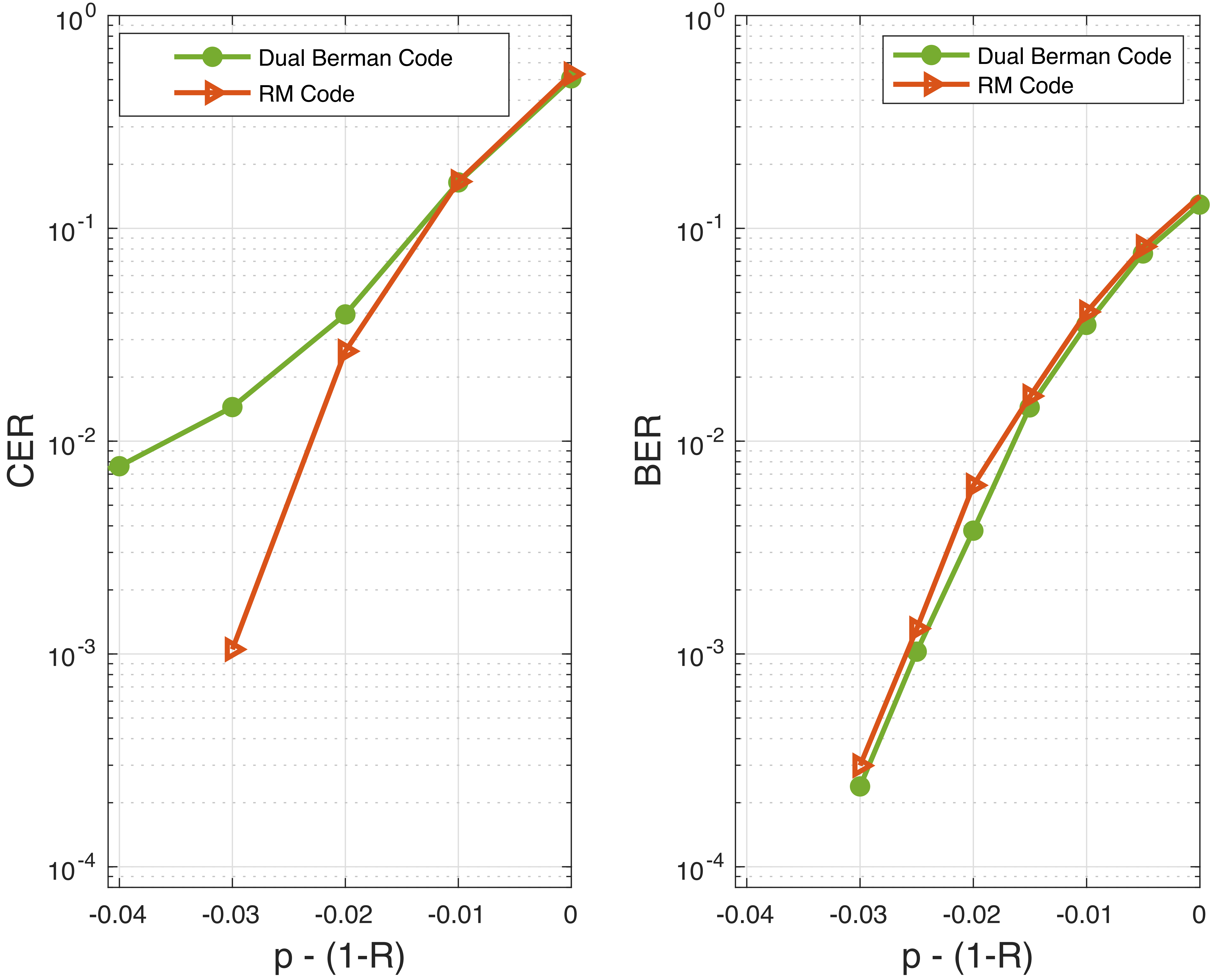
- $\mathscr{B}_3(5,7)$:

  $N = 2187,\ R = 0.26,\ d_{\min} = 64$

- $\mathrm{RM}(4,11)$:

  $N = 2048,\ R = 0.27,\ d_{\min} = 128$

DUAL BERMAN CODE $(n = 3)$ VS. REED-MULLER CODE IN $\mathrm{BEC}(p)$



- $\mathscr{D}_3(5,7)$:

  $N = 2187,\ R = 0.74,\ d_{\min} = 9$

- $\mathrm{RM}(6,11)$:

  $N = 2048,\ R = 0.73,\ d_{\min} = 32$

BERMAN CODES: CONSTRUCTION & PROPERTIES

LINEAR CODES: SUBSPACES OF HAMMING SPACE $\{0,1\}^N$

- $\mathbb{F}_2 = \{0,1\}$ is the binary field
  - addition is XOR, multiplication is AND
- $\mathbb{F}_2^N$ is a vector space
  - Contains 2^N binary vectors of length N
- $\mathscr{C} \subset \mathbb{F}_2^N$ is a **subspace/linear code** if closed under addition
  - $\mathbf{a}, \mathbf{b} \in \mathscr{C} \Rightarrow \mathbf{a} + \mathbf{b} \in \mathscr{C}$
- $|\mathscr{C}| = 2^K$ if dimension of $\mathscr{C}$ is K
  - encode K message bits into a codeword of length N

$$\mathbb{F}_2^3 = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$$

$$\mathscr{C} = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\}$$

EXAMPLES OF LINEAR CODES (BUILDING BLOCKS OF BERMAN CODES)

- Repetition Code of length N

$$\mathscr{C}_{\mathrm{rep},N} = \{(0,\ldots,0),\ (1,\ldots,1)\}$$

- Single Parity Check Code of length N

$$\mathscr{C}_{\mathrm{spc},N} = \left\{\mathbf{a} \in \mathbb{F}_2^N \ :\ a_1 + \cdots + a_N = 0\right\}$$

- Trivial Linear Codes

$$\mathscr{C} = \mathbb{F}_2^N \text{ (no redundancy)}, \qquad \mathscr{C} = \{\ (0,\ldots,0)\ \} \text{ (no information transmission)}$$

ORIGINAL CONSTRUCTION OF BERMAN

- Let n **be an odd prime**, and $m \geq 2$ and $r \in \{0,1,\ldots,m\}$

- Consider the quotient ring $\mathscr{R}_{n,m} = \mathbb{F}_2[X_1, \ldots, X_m] \,/\, \langle X_1^n - 1, \ldots, X_m^n - 1 \rangle$
  - This is the group algebra $\mathbb{F}_2\left[C_n \times \cdots \times C_n\right]$
  - Natural $\mathbb{F}_2$-basis of $\mathscr{R}_{n,m}$: $\left\{ X_1^{i_1} \ldots X_m^{i_m} \;:\; 0 \leq i_1, \ldots, i_m \leq n-1 \right\}$

- Natural $\mathbb{F}_2$-linear map $\rho : \mathscr{R}_{n,m} \rightarrow \mathbb{F}_2^{n^m}$

$$\sum_{i_1=0}^{n-1} \cdots \sum_{i_m=0}^{n-1} a_{(i_1,\ldots,i_m)} X_1^{i_1} \cdots X_m^{i_m} \rightarrow \left(a_{(i_1,\ldots,i_m)} \;:\; 0 \leq i_1, \ldots, i_m \leq n-1 \right)$$

ORIGINAL CONSTRUCTION OF BERMAN

- $\mathscr{R}_{n,m} = \mathbb{F}_2[X_1, \ldots, X_m] \,/\, \langle X_1^n - 1, \ldots, X_m^n - 1 \rangle$

- For any $S \subset \{1,2,\ldots,m\}$ define $u_S \in \mathscr{R}_{n,m}$ as $u_S = \prod_{j \notin S} \frac{X_j^n + 1}{X_j + 1} = \prod_{j \notin S} \left(1 + X_j + X_j^2 + \cdots + X_j^{n-1}\right)$

- Ideal $\mathscr{I}_n(r,m) = \langle u_S : |S| = r \rangle$

  its annihilator $\mathscr{A}_n(r,m) = \left\{y \in \mathscr{R}_{n,m} \ : \ yz = 0 \ \forall z \in \mathscr{I}_n(r,m)\right\}$

Berman

Berman Code $\mathscr{B}_n(r,m) = \rho\left(\mathscr{A}_n(r,m)\right)$

Blackmore & Norton

Dual Berman Code $\mathscr{D}_n(r,m) = \rho\left(\mathscr{I}_n(r,m)\right)$

PLOTKIN-LIKE CONSTRUCTION OF BERMAN CODES

- Let $n \geq 2, \quad m \geq 2, \quad r \in \{0,1,\ldots,m\}$

- When $r = m$: $\quad \mathscr{B}_n(r = m, m) = \{(0,\ldots,0)\}$

- When $r = 0$: $\quad \mathscr{B}_n(r = 0, m) = \left\{ (a_1, \ldots, a_{n^m}) \; : \; \sum_i a_i = 0 \right\}$

- When $1 \leq r \leq m-1$:

$$\mathscr{B}_n(r, m) = \left\{ (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n) \; : \; \mathbf{v}_i \in \mathscr{B}_n(r-1, m-1), \sum_i \mathbf{v}_i \in \mathscr{B}_n(r, m-1) \right\}$$

EXAMPLE: $n = 3, r = 1, m = 2$

- $\mathscr{B}_n(r,m) \subset \mathbb{F}^9$ $\quad\mathscr{B}_n(r-1, m-1) = \mathscr{C}_{\text{spc},3}$ $\quad\mathscr{B}_n(r, m-1) = \{\,(0,0,0)\,\}$

- $\mathscr{B}_3(1,2) = \left\{(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \;:\; \mathbf{v}_i \in \mathscr{C}_{\text{spc},3},\;\; \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = (0,0,0)\right\}$

- (1,0,1, 0,1,1, 1,1,0) is a codeword of $\mathscr{B}_3(1,2)$:

  $(1,0,1)\,,\,(0,1,1),\;(1,1,0)\;\in \mathscr{C}_{\text{spc},3}$

  $(1,0,1) + (0,1,1) + (1,1,0) = (0,0,0) \in \mathscr{B}_3(1,1) = \{(0,0,0)\}$

PLOTKIN-LIKE CONSTRUCTION OF DUAL BERMAN CODES

- Let $n \geq 2, \quad m \geq 2, \quad r \in \{0,1,\ldots,m\}$
- When $r = m$: $\quad \mathcal{D}_n(r = m, m) = \mathbb{F}_2^{n^m}$
- When $r = 0$: $\quad \mathcal{D}_n(r = 0, m) = \{(0,\ldots,0), (1,\ldots,1)\}$
- When $1 \leq r \leq m-1$:

$$\mathcal{D}_n(r,m) = \Big\{ (\mathbf{u}+\mathbf{u}_1, \mathbf{u}+\mathbf{u}_2, \ldots, \mathbf{u}+\mathbf{u}_{n-1}, \mathbf{u}) \ : \ \mathbf{u}_i \in \mathcal{D}_n(r-1, m-1), \mathbf{u} \in \mathcal{D}_n(r, m-1) \Big\}$$

WHEN $n = 2$ DUAL BERMAN CODES ARE RM CODES (PLOTKIN CONSTRUCTION)

- Use $n = 2$
- When $r = m$: $\quad \mathscr{D}_2(r = m, m) = \mathbb{F}_2^{2^m}$
- When $r = 0$: $\quad \mathscr{D}_2(r = 0, m) = \{(0,\ldots,0), (1,\ldots,1)\}$
- When $1 \leq r \leq m - 1$:

$$\mathscr{D}_2(r, m) = \left\{ (\mathbf{u} + \mathbf{u}_1, \mathbf{u}) \ : \ \mathbf{u}_1 \in \mathscr{D}_2(r-1, m-1), \mathbf{u} \in \mathscr{D}_2(r, m-1) \right\}$$

BASE-n INDEXING OF ENTRIES OF A CODEWORD

- Replace natural indexing that uses $i \in \{1,2,\ldots,n^m\}$ with
  the base-n expansion of $(i-1) \in \{1,\ldots,n^m\}$

$$(i-1) \;=\; \sum_{k=1}^{m} i_k\, n^{(k-1)}, \quad \text{where } i_k \in [n] = \{0,1,\ldots,n-1\}$$

- Use the vector $\mathbf{i} = (i_1, i_2, \ldots, i_m)$ as an index instead of the integer i
  (note that $\mathbf{i} \in \{0,1,\ldots,n-1\}^m = [n]^m$)

- Codeword $\mathbf{a} = (\, a_{\mathbf{i}} \;:\; \mathbf{i} \in [n]^m\,)$, where each $a_{\mathbf{i}} \in \mathbb{F}_2$

BASES FOR BERMAN AND DUAL BERMAN CODES

- Recall: $[n] = \{0,1,\ldots,n-1\}$, $[n]^m = \{0,1,\ldots,n-1\}^m$

  Index the n^m coordinates of a codeword using elements of $[n]^m$

- Define a partial order on $[n]^m$

  $$(i_1, \ldots, i_m) \preceq (j_1, \ldots, j_m) \quad \text{if and only if} \quad i_k \in \{j_k\} \cup \{0\} \quad \text{for all } k$$

  Example: $(0,0,1) \preceq (0,2,1) \preceq (1,2,1)$

- Define the Hamming weight $w\big((i_1, \ldots, i_m)\big)$ as usual.

BASES FOR BERMAN AND DUAL BERMAN CODES

- Recall partial order: $(i_1, \ldots, i_m) \preceq (j_1, \ldots, j_m)$ iff $i_k \in \{j_k\} \cup \{0\}$ for all k.

- For each $(j_1, \ldots, j_m) \in [n]^m$ define $\mathbf{b}(j_1, \ldots, j_m), \mathbf{d}(j_1, \ldots, j_m) \in \mathbb{F}_2^{n^m}$

$$\text{Support of } \mathbf{b}(j_1, \ldots, j_m) = \text{set of all } (i_1, \ldots, i_m) \preceq (j_1, \ldots, j_m)$$

$$\text{Support of } \mathbf{d}(j_1, \ldots, j_m) = \text{set of all } (i_1, \ldots, i_m) \succeq (j_1, \ldots, j_m)$$

An $\mathbb{F}_2$-basis for $\mathscr{B}_n(r, m) = \left\{ \mathbf{b}(j_1, \ldots, j_m) \ : \ w\left((j_1, \ldots, j_m)\right) \geq r + 1 \right\}$

An $\mathbb{F}_2$-basis for $\mathscr{D}_n(r, m) = \left\{ \mathbf{d}(j_1, \ldots, j_m) \ : \ w\left((j_1, \ldots, j_m)\right) \leq r \right\}$

BASES FOR BERMAN AND DUAL BERMAN CODES

Consider $A_n^{\otimes m}$, where $A_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{bmatrix} \in \mathbb{F}_2^{n \times n}$

Rows of $A_n^{\otimes m}$ with Hamming weight $\geq 2^{r+1}$ generate $\mathscr{B}_n(r, m)$

Columns of $A_n^{\otimes m}$ with Hamming weight $\geq n^{m-r}$ generate $\mathscr{D}_n(r, m)$

SPECTRAL DESCRIPTION (ODD n)

- Use $[n]^m$ to index the coordinates of n^m-length codewords

$$\mathbf{c} = \left(c_{(i_1,\ldots,i_m)} \; : \; (i_1, \ldots, i_m) \in [n]^m \right)$$

- Let α be a primitive n^{th} root of unity (from the appropriate field extension of $\mathbb{F}_2$)

- The m-dimensional discrete Fourier transform of $\mathbf{c}$ is

$$\hat{\mathbf{c}} = \left(\hat{c}_{(j_1,\ldots,j_m)} \; : \; (j_1, \ldots, j_m) \in [n]^m \right), \quad \text{where } \hat{c}_{(j_1,\ldots,j_m)} = \sum_{(i_1,\ldots,i_m)} c_{(i_1,\ldots,i_m)} \, \alpha^{i_1 j_1 + \cdots + i_m j_m}$$

SPECTRAL DESCRIPTION (ODD n)

- Recall: $\hat{c}_{(j_1,\ldots,j_m)} = \sum_{(i_1,\ldots,i_m)} c_{(i_1,\ldots,i_m)} \alpha^{i_1 j_1 + \cdots + i_m j_m}$

- Berman Code $\mathscr{B}_n(r,m) = \left\{ \mathbf{c} \in \mathbb{F}_2^{n^m} \ : \ \hat{c}_{(j_1,\ldots,j_m)} = 0, \ \ w((j_1,\ldots,j_m)) \le r \right\}$

- Dual Berman Code. $\mathscr{D}_n(r,m) = \left\{ \mathbf{c} \in \mathbb{F}_2^{n^m} \ : \ \hat{c}_{(j_1,\ldots,j_m)} = 0, \ \ w((j_1,\ldots,j_m)) > r \right\}$

AUTOMORPHISMS & CAPACITY-ACHIEVABILITY

AUTOMORPHISMS OF A CODE

- Suppose $\pi : [n]^m \to [n]^m$ is a permutation (an invertible map)

- Apply π on the indices of a codeword to permute its coordinates:

$$\pi(\mathbf{a}) = (a_{\pi(\mathbf{i})} \ : \ \mathbf{i} \in [n]^m)$$

$$\mathbf{i}^{\text{th}} \text{ entry of } \pi(\mathbf{a}) = \pi(\mathbf{i})^{\text{th}} \text{ entry of } \mathbf{a}$$

Automorphism Group of a Code $\mathscr{C}$

$$\mathrm{Aut}(\mathscr{C}) \triangleq \{ \pi \ : \ \pi(\mathbf{a}) \in \mathscr{C} \text{ for all } \mathbf{a} \in \mathscr{C} \}$$

EXAMPLE: AN AUTOMORPHISM OF $\mathscr{B}_3(1,2)$

$\pi(\mathbf{i}) =$

0	2	1	0	2	1	0	2	1
1	1	1	2	2	2	0	0	0

$\mathbf{i} =$

0	1	2	0	1	2	0	1	2
0	0	0	1	1	1	2	2	2

$\mathbf{a} =$

1	0	1	0	1	1	1	1	0

$\in \mathscr{B}_3(1,2)$

$\pi(\mathbf{a}) =$

0	1	1	1	0	1	1	1	0

$\in \mathscr{B}_3(1,2)$

AUTOMORPHISMS OF $\mathscr{B}_n(r,m)$ AND $\mathscr{D}_n(r,m)$

- **Theorem:** The following maps are automorphisms of Berman codes and their duals

  - for any permutations $\sigma_1, \ldots, \sigma_m$ of the set $[n] = \{0,1,\ldots,n-1\}$

$$(i_1, i_2, \ldots, i_m) \rightarrow \left(\sigma_1(i_1), \sigma_2(i_2), \ldots, \sigma_m(i_m)\right)$$

  - for any permutation γ of the set $\{1,\ldots,m\}$

$$(i_1, i_2, \ldots, i_m) \rightarrow \left(i_{\gamma(1)}, i_{\gamma(2)}, \ldots, i_{\gamma(m)}\right)$$

ALL SUFFICIENTLY SYMMETRIC CODES ACHIEVE BEC CAPACITY

➤ [Kumar, Calderbank & Pfister, 2016] showed that code sequences with rich-enough automorphism groups achieve BEC capacity (BER $\to$ 0)

1. Codes must be ***transitive***

   for every $\mathbf{i} \neq \mathbf{j}$ there must exist a $\pi \in \mathrm{Aut}(\mathscr{C})$ such that $\pi(\mathbf{i}) = \mathbf{j}$

2. Minimum orbit size under a specific subgroup of automorphisms must grow unboundedly as $N \to \infty$

$$\mathcal{O}_{\min}(\mathscr{C}) = \min_{\mathbf{i} \neq \mathbf{0}} \left| \left\{ \pi(\mathbf{i}) \ : \ \pi \in \mathrm{Aut}(\mathscr{C}),\ \pi(\mathbf{0}) = \mathbf{0} \right\} \right|$$

1. BERMAN CODES ARE TRANSITIVE

- Suppose $(i_1, \ldots, i_m) \neq (j_1, \ldots, j_m)$

- Pick any $\sigma_1, \ldots, \sigma_m$ (permutations on $[n]$) such that

$$\sigma_1(i_1) = j_1, \;\; \ldots, \; \sigma_m(i_m) = j_m$$

- Consider the automorphism

$$\pi \;:\; \left(i_1, i_2, \ldots, i_m \right) \;\rightarrow\; \left(\sigma_1\left(i_1\right), \sigma_2\left(i_2\right), \ldots, \sigma_m\left(i_m\right) \right)$$

- Then $\pi(\mathbf{i}) = \mathbf{j}$

2. ORBIT UNDER AUTOMORPHISMS THAT FIX $(0,\ldots,0)$

Consider $\mathbf{i} = (i_1, \ldots, i_m) \neq (0,\ldots,0)$

1. Apply all $\pi : \left(i_1, i_2, \ldots, i_m\right) \to \left(\sigma_1\left(i_1\right), \sigma_2\left(i_2\right), \ldots, \sigma_m\left(i_m\right)\right)$ such that
   - $\sigma_1(0) = 0, \ \ldots, \sigma_m(0) = 0$

   ➤ All vectors with the same support as $\mathbf{i}$ are in the orbit of $\mathbf{i}$

2. Apply all $\pi : \left(i_1, i_2, \ldots, i_m\right) \to \left(i_{\gamma(1)}, i_{\gamma(2)}, \ldots, i_{\gamma(m)}\right)$

   ➤ All vectors with the same Hamming weight as $\mathbf{i}$ are in the orbit of $\mathbf{i}$

2. ORBIT UNDER AUTOMORPHISMS THAT FIX $(0,\ldots,0)$

Consider $\mathbf{i} = (i_1, \ldots, i_m) \neq (0,\ldots,0)$

The size of the orbit of $\mathbf{i}$ under this subgroup of automorphisms:

$$\left| \left\{ \pi(\mathbf{i}) \ : \ \pi \in \mathrm{Aut}(\mathscr{C}),\ \pi(\mathbf{0}) = \mathbf{0} \right\} \right| \ \geq \ \#\text{vectors with weight } w(\mathbf{i}) = \binom{m}{w(\mathbf{i})}(n-1)^{w(\mathbf{i})}$$

$$\mathcal{O}_{\min} \geq \min_{\mathbf{i} \neq \mathbf{0}} \binom{m}{w(\mathbf{i})}(n-1)^{w(\mathbf{i})} = (n-1)m \geq 2m \qquad \text{if } n \geq 3.$$

ALGEBRAIC CRITERION TO ACHIEVE CAPACITY OF BEC (BER $\to 0$)

Consider a sequence of codes with strictly increasing block lengths

[Kumar, Calderbank, Pfister, 2016]: If the sequence of codes satisfies

1. The rate of this sequence of codes $\to R$
2. Each code in this sequence has a transitive group of automorphisms
3. $\mathcal{O}_{\min} \to \infty$

As long as $R < 1 - p$, then for this sequence of codes:

the probability of recovering each codeword bit in $\mathrm{BEC}(p) \to 1$.

APPLYING [KUMAR, CALDERBANK, PFISTER, 2016]

- Pick any $n \geq 3$.

- Choose any desired code rate $R \in (0,1)$.

- Construct sequence of Berman codes

  for each $m \geq 2$, choose order $r_m \in \{0,1,\ldots,m\}$ to be the integer closest to

$$m\left(\frac{n-1}{n}\right) + Q^{-1}(R)\sqrt{m\frac{(n-1)}{n^2}}$$

  where $Q(x) = \int_{t=x}^{+\infty} (2\pi)^{-1/2} e^{-t^2/2}\, dt$.

BERMAN CODES ACHIEVE VANISHING BER IN BEC FOR RATES UP TO CAPACITY

For $n \geq 3$, consider the sequence of Berman codes $\mathscr{B}_n(r_m, m)$, $m = 2,3,\ldots$

This sequence of codes satisfies the criteria of [Kumar, Calderbank, Pfister, 2016]

1. The rate of this sequence of codes $\rightarrow$ R
2. Each code in this sequence has a transitive group of automorphisms
3. $\mathscr{O}_{\min} \geq 2m \rightarrow \infty$

If $R < 1 - p$ then as $m \rightarrow \infty$,

the probability of recovering each codeword bit in BEC(p) $\rightarrow$ 1.

(a similar result holds for dual Berman codes)

ACKNOWLEDGMENT

భారతీయ సాంకేతిక విజ్ఞాన సంస్థ హైదరాబాద్
भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

शिक्षा मंत्रालय
MINISTRY OF
EDUCATION

सत्यमेव जयते

SERB
iNDIA

THANK YOU!

REFERENCES

- [Shannon'48]
  Shannon, Claude Elwood. "A mathematical theory of communication." *The Bell system technical journal* 27, no. 3 (1948): 379-423.

- [Dobrushin'63]
  Dobrushin, R. L. "Asymptotic optimality of group and systematic codes for some channels." *Theory of Probability & Its Applications* 8, no. 1 (1963): 47-60.

- [Gallager'68]
  Gallager, Robert G. *Information theory and reliable communication.* Vol. 588. New York: Wiley, 1968.

- [LMSSS’97]
  Luby, Michael G., Michael Mitzenmacher, M. Amin Shokrollahi, Daniel A. Spielman, and Volker Stemann. "Practical loss-resilient codes." In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 150-159. 1997.

- [Arikan’09]
  Arikan, Erdal. "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels." *IEEE Transactions on information Theory* 55, no. 7 (2009): 3051-3073.

- [KRU’11]
  Kudekar, Shrinivas, Thomas J. Richardson, and Rüdiger L. Urbanke. "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC." *IEEE Transactions on Information Theory* 57, no. 2 (2011): 803-834.

- [KSMPSU'17]
  Kudekar, Shrinivas, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Şaşoğlu, and Rüdiger L. Urbanke. "Reed–Muller codes achieve capacity on erasure channels." *IEEE Transactions on information theory* 63, no. 7 (2017): 4298-4316.

- [KCP'16]
  Kumar, Santhosh, Robert Calderbank, and Henry D. Pfister. "Beyond double transitivity: Capacity-achieving cyclic codes on erasure channels." In *2016 IEEE Information Theory Workshop (ITW)*, pp. 241-245. IEEE, 2016.

- [NK'22]
  L. P. Natarajan and P. Krishnan, "Berman Codes: A Generalization of Reed-Muller Codes that Achieve BEC Capacity," in *IEEE Transactions on Information Theory*, doi: 10.1109/TIT.2023.3299287.

- [RS’92]
  Rajan, B. Sundar, and M. U. Siddiqi. "Transform domain characterization of abelian codes." *IEEE transactions on information theory* 38, no. 6 (1992): 1817-1821.

- [Camion’71]
  P. Camion, “Abelian codes,” *Math. Res. Ctr., Univ. Wisconsin*, Madison, Tech. Rep. 1059, 1971.

- [MacWilliams’70]
  F.J.M.Williams,“Binary codes which are ideals in the group algebra of an abelian group,” *The Bell System Technical Journal*, vol.49, no. 6, pp. 987–1011, 1970.

- [MS'77]
  F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977, vol. 16.

- [Blahut'03]
  R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge University Press, 2003.

- [Berman'67]
  S. Berman, "On the theory of group codes," *Cybernetics*, vol. 3, no. 1, pp. 25–31, 1967.

- [Berman'67]
  Berman, S. D. "Semisimple cyclic and Abelian codes. II." *Cybernetics,* vol. 3, no. 3, pp. 17-23, 1967.

- [Abbe & Sandon'23]
  Emmanuel Abbe and Colin Sandon, *"A proof that Reed-Muller codes achieve Shannon capacity on symmetric channels."* arXiv preprint arXiv:2304.02509 (2023).

- [Reeves & Pfister]
  G. Reeves and H. D. Pfister, "Reed–Muller Codes on BMS Channels Achieve Vanishing Bit-Error Probability for all Rates Below Capacity," in *IEEE Transactions on Information Theory*, vol. 70, no. 2, pp. 920-949, Feb. 2024.

- [Talagrand'92]
  Talagrand, Michel. "On Russo's approximate zero-one law." *The Annals of Probability* (1994): 1576-1587.

- Ehud Friedgut and Gil Kalai. "Every monotone graph property has a sharp threshold." *Proceedings of the American mathematical Society* 124, no. 10 (1996): 2993-3002.