Capacity via Symmetry: Extensions and Practical Consequences

Henry D. Pfister

MIT LIDS Seminar Series
April 4th, 2017

Acknowledgments

- Thanks to my collaborators
  - **Santhosh Kumar**
  - Robert Calderbank
  - Elia Santi

- And to everyone involved with the original result
  - Marco Mondelli
  - Rüdiger Urbanke
  - Shrinivas Kudekar
  - Eren Şaşoğlu

Outline

- Capacity via Symmetry
- Beyond Double Transitivity
- Product Codes and Cyclic Codes
- Leveraging Symmetry in Practice
- Open Problems
- Summary

Problem Setup

$$\text{Msg.} \longrightarrow \boxed{\text{Rate-}R \text{ code } \mathcal{C}} \longrightarrow \underline{X} \longrightarrow \boxed{\mathrm{BEC}(p)} \longrightarrow \underline{Y}$$

- Binary linear code $\mathcal{C} \subseteq \{0,1\}^N$ is a RN-dim. subspace of $\mathbb{F}_2^N$

uniform codeword:	$\underline{X} = (X_0, \ldots, X_{N-1}) \in \{0,1\}^N$
Bernoulli-p erasures:	$\underline{Z} = (Z_0, \ldots, Z_{N-1}) \in \{0,1\}^N$
BEC(p) observation of $\underline{X}$:	$Y_i = \begin{cases} X_i & \text{if } Z_i = 0 \\ ? & \text{if } Z_i = 1 \end{cases}$

Problem Setup

$$\text{Msg.} \longrightarrow \boxed{\text{Rate-}R \text{ code } \mathcal{C}} \longrightarrow \underline{X} \longrightarrow \boxed{\text{BEC}(p)} \longrightarrow \underline{Y}$$

- Binary linear code $\mathcal{C} \subseteq \{0,1\}^N$ is a RN-dim. subspace of $\mathbb{F}_2^N$

uniform codeword:	$\underline{X} = (X_0, \ldots, X_{N-1}) \in \{0,1\}^N$
Bernoulli-p erasures:	$\underline{Z} = (Z_0, \ldots, Z_{N-1}) \in \{0,1\}^N$
BEC(p) observation of $\underline{X}$:	$Y_i = \begin{cases} X_i & \text{if } Z_i = 0 \\ ? & \text{if } Z_i = 1 \end{cases}$

- The MAP erasure rate $P_{b,i}(p)$ of bit-i satisfies

$$P_{b,i}(p) = \mathbb{P}(Y_i = ?)\,\underbrace{H(X_i | \underline{Y}, Y_i = ?)}_{h_i(p)} = p h_i(p),$$

where $h_i(p)$ is the MAP EXIT function of bit-i.

Capacity via Symmetry

Recently, it was shown that symmetry alone is sufficient for a code sequence to achieve capacity on erasure channels [KKMPSU16]

Theorem 1: Let $\{\mathcal{C}_n\}$ be a sequence of $\mathbb{F}_q$-linear codes with

- blocklengths $N_n \to \infty$ and rates $R_n \to R \in (0, 1)$, where
- the permutation group of each $\mathcal{C}_n$ is doubly transitive.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Capacity via Symmetry

Recently, it was shown that symmetry alone is sufficient for a code sequence to achieve capacity on erasure channels [KKMPSU16]

Theorem 1: Let $\{\mathcal{C}_n\}$ be a sequence of $\mathbb{F}_q$-linear codes with

- blocklengths $N_n \to \infty$ and rates $R_n \to R \in (0,1)$, where
- the permutation group of each $\mathcal{C}_n$ is doubly transitive.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Some consequences are:

- Reed-Muller codes achieve capacity
- Linear affine-invariant codes over $\mathbb{F}_q$ achieve capacity
- Primitive narrow-sense BCH codes achieve capacity

The Permutation Group of a Set of Vectors

- For a set $\mathcal{A} \subseteq \mathcal{X}^N$ of vectors
  - Permutations $\pi \in S_N$ act on $\mathcal{X}^N$ via: $\underline{b} = \pi(\underline{a}) \Leftrightarrow b_{\pi(i)} = a_i$
  - The permutation group of $\mathcal{A}$ is defined to be

$$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{a}) \in \mathcal{A} \; \forall \; \underline{a} \in \mathcal{A}\}$$

The Permutation Group of a Set of Vectors

- For a set $\mathcal{A} \subseteq \mathcal{X}^N$ of vectors
  - Permutations $\pi \in S_N$ act on $\mathcal{X}^N$ via: $\underline{b} = \pi(\underline{a}) \Leftrightarrow b_{\pi(i)} = a_i$
  - The permutation group of $\mathcal{A}$ is defined to be

$$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{a}) \in \mathcal{A} \;\forall\; \underline{a} \in \mathcal{A}\}$$

- Permutation group of $\mathcal{A}$

$$\mathcal{A} = \left\{ \begin{matrix} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{matrix} \right\} \quad \Longrightarrow \quad \mathcal{G} = \left\{ \begin{matrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix} \end{matrix} \right\}$$

The Permutation Group of a Set of Vectors

- For a set $\mathcal{A} \subseteq \mathcal{X}^N$ of vectors
  - Permutations $\pi \in S_N$ act on $\mathcal{X}^N$ via: $\underline{b} = \pi(\underline{a}) \Leftrightarrow b_{\pi(i)} = a_i$
  - The permutation group of $\mathcal{A}$ is defined to be

$$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{a}) \in \mathcal{A} \;\forall\; \underline{a} \in \mathcal{A}\}$$

  - A permutation group $\mathcal{G}$ is transitive if, for all $i, j \in \mathbb{Z}_N$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = j$

- Permutation group of $\mathcal{A}$ is transitive

$$\mathcal{A} = \left\{ \begin{matrix} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{matrix} \right\} \quad \Longrightarrow \quad \mathcal{G} = \left\{ \begin{matrix} \begin{pmatrix} 0&1&2&3 \\ 0&1&2&3 \end{pmatrix} & \begin{pmatrix} 0&1&2&3 \\ 1&0&2&3 \end{pmatrix} \\ \begin{pmatrix} 0&1&2&3 \\ 0&1&3&2 \end{pmatrix} & \begin{pmatrix} 0&1&2&3 \\ 1&0&3&2 \end{pmatrix} \\ \begin{pmatrix} 0&1&2&3 \\ 2&3&0&1 \end{pmatrix} & \begin{pmatrix} 0&1&2&3 \\ 3&2&0&1 \end{pmatrix} \\ \begin{pmatrix} 0&1&2&3 \\ 2&3&1&0 \end{pmatrix} & \begin{pmatrix} 0&1&2&3 \\ 3&2&1&0 \end{pmatrix} \end{matrix} \right\}$$

The Permutation Group of a Set of Vectors

- For a set $\mathcal{A} \subseteq \mathcal{X}^N$ of vectors
  - Permutations $\pi \in S_N$ act on $\mathcal{X}^N$ via: $\underline{b} = \pi(\underline{a}) \Leftrightarrow b_{\pi(i)} = a_i$
  - The permutation group of $\mathcal{A}$ is defined to be

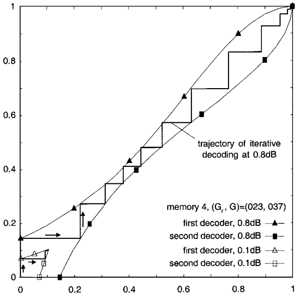
$$\mathcal{G} \triangleq \{\pi \in S_N \,|\, \pi(\underline{a}) \in \mathcal{A} \;\forall\; \underline{a} \in \mathcal{A}\}$$

  - A permutation group $\mathcal{G}$ is transitive if, for all $i, j \in \mathbb{Z}_N$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = j$
  - $\mathcal{G}$ is doubly transitive if, for any $i, j, k, l \in \mathbb{Z}_N$ with $i \neq j$ and $k \neq l$, there exists $\pi \in \mathcal{G}$ such that $\pi(i) = k$ and $\pi(j) = l$.
- Permutation group of $\mathcal{A}$ is transitive but not doubly transitive

$$\mathcal{A} = \left\{ \begin{array}{cccc} (0 & 0 & 0 & 0) \\ (0 & 0 & 1 & 1) \\ (1 & 1 & 0 & 0) \\ (1 & 1 & 1 & 1) \end{array} \right\} \implies \mathcal{G} = \left\{ \begin{array}{cc} \binom{0\,1\,2\,3}{0\,1\,2\,3} & \binom{0\,1\,2\,3}{1\,0\,2\,3} \\ \binom{0\,1\,2\,3}{0\,1\,3\,2} & \binom{0\,1\,2\,3}{1\,0\,3\,2} \\ \binom{0\,1\,2\,3}{2\,3\,0\,1} & \binom{0\,1\,2\,3}{3\,2\,0\,1} \\ \binom{0\,1\,2\,3}{2\,3\,1\,0} & \binom{0\,1\,2\,3}{3\,2\,1\,0} \end{array} \right\}$$

EXtrinsic Information Transfer (EXIT) Curves

- Defined by ten Brink in 1999 to explain iterative decoding

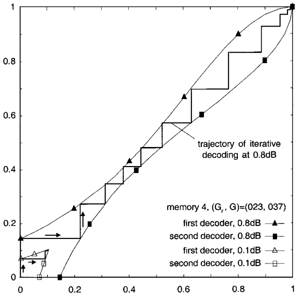


EXtrinsic Information Transfer (EXIT) Curves

- Defined by ten Brink in 1999 to explain iterative decoding

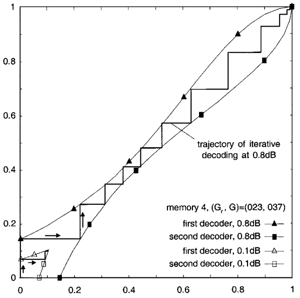
- For the BEC(p), the average MAP EXIT function is

$$h(p) \triangleq \frac{1}{N}\sum_{i=0}^{N-1} \underbrace{H(X_i|\underline{Y}_{\sim i}(p))}_{h_i(p)}$$



Note: $\underline{Y}_{\sim i} \triangleq (Y_0, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_{N-1})$

EXtrinsic Information Transfer (EXIT) Curves



- Defined by ten Brink in 1999 to explain iterative decoding
- For the BEC(p), the average MAP EXIT function is

$$h(p) \triangleq \frac{1}{N} \sum_{i=0}^{N-1} \underbrace{H(X_i | \underline{Y}_{\sim i}(p))}_{h_i(p)}$$

- EXIT Area Theorem [ABK04]

$$\int_0^1 h(p) \mathrm{d}p = R \qquad \text{(code rate)}$$

Note: $\underline{Y}_{\sim i} \triangleq (Y_0, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_{N-1})$

Properties of the MAP EXIT Function

- For linear codes, the recovery of X_i from $\underline{Y}_{\sim i} = \underline{y}_{\sim i}$
  - is independent of the transmitted codeword $\underline{X}$
  - only depends on erasure indicator $z_i = \mathbf{1}_{\{?\}}(y_i)$
  - is a zero-one boolean function of $\underline{z}_{\sim i}$

Properties of the MAP EXIT Function

- For linear codes, the recovery of X_i from $\underline{Y}_{\sim i} = \underline{y}_{\sim i}$
  - is independent of the transmitted codeword $\underline{X}$
  - only depends on erasure indicator $z_i = \mathbf{1}_{\{?\}}(y_i)$
  - is a zero-one boolean function of $\underline{z}_{\sim i}$

- Bit-i EXIT function is a monotone boolean function f_i of $\underline{Z}_{\sim i}$

$$H(X_i | \underline{Y}_{\sim i} = \underline{y}_{\sim i}, \underline{Z}_{\sim i} = \underline{z}_{\sim i}) = f_i(\underline{z}_{\sim i}) \in \{0, 1\},$$

where $\underline{z}_{\sim i} \triangleq (z_0, \ldots, z_{i-1}, z_{i+1}, \ldots, z_{N-1})$

Properties of the MAP EXIT Function

- For linear codes, the recovery of X_i from $\underline{Y}_{\sim i} = \underline{y}_{\sim i}$
  - is independent of the transmitted codeword $\underline{X}$
  - only depends on erasure indicator $z_i = \mathbf{1}_{\{?\}}(y_i)$
  - is a zero-one boolean function of $\underline{z}_{\sim i}$

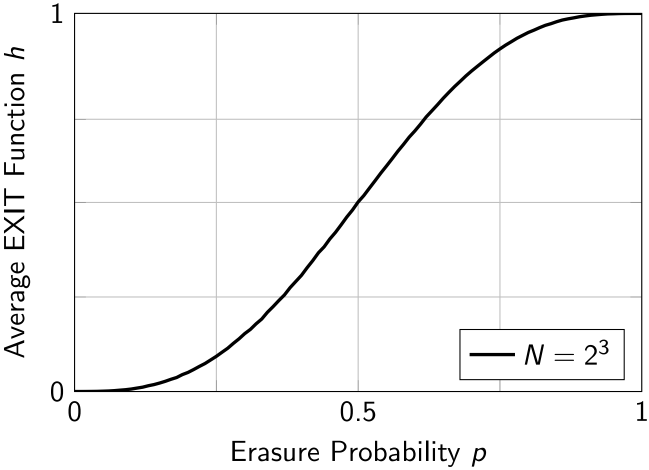
- Bit-i EXIT function is a monotone boolean function f_i of $\underline{Z}_{\sim i}$

$$H(X_i|\underline{Y}_{\sim i} = \underline{y}_{\sim i}, \underline{Z}_{\sim i} = \underline{z}_{\sim i}) = f_i(\underline{z}_{\sim i}) \in \{0, 1\},$$

  where $\underline{z}_{\sim i} \triangleq (z_0, \ldots, z_{i-1}, z_{i+1}, \ldots, z_{N-1})$

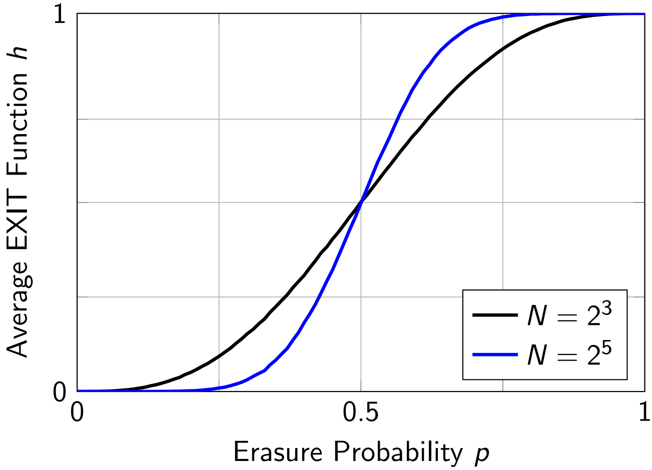
- "Sequence of rate-R codes achieves capacity" is equivalent to:
  - $P_b(p) \to 0$ for all $p < 1 - R$
  - $h(p) \to 0$ for all $p < 1 - R$ (since $P_b(p) = ph(p)$)
  - $h(p)$ transitions sharply from 0 to 1

The MAP EXIT Curve of a Capacity-Achieving Code



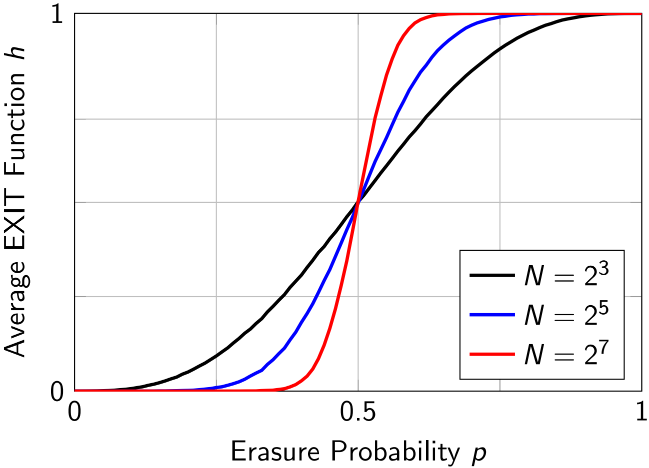
- $h^{-1}(1-\delta)-h^{-1}(\delta) =$ transition width where $\delta \leq h(p) \leq 1-\delta$

The MAP EXIT Curve of a Capacity-Achieving Code



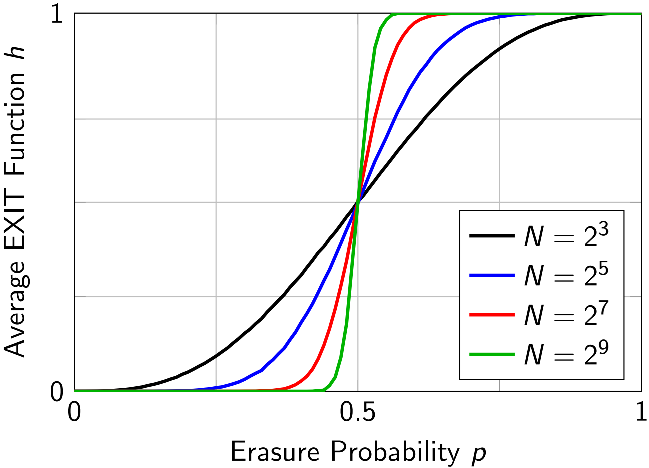
- $h^{-1}(1-\delta) - h^{-1}(\delta) =$ transition width where $\delta \le h(p) \le 1-\delta$
- Area Theorem implies sharp transition iff capacity achieving

The MAP EXIT Curve of a Capacity-Achieving Code



- $h^{-1}(1-\delta) - h^{-1}(\delta) =$ transition width where $\delta \leq h(p) \leq 1-\delta$
- Area Theorem implies sharp transition iff capacity achieving

The MAP EXIT Curve of a Capacity-Achieving Code



- $h^{-1}(1-\delta) - h^{-1}(\delta) =$ transition width where $\delta \leq h(p) \leq 1-\delta$
- Area Theorem implies sharp transition iff capacity achieving

Theorem 1: Outline of Proof

1. Permutation group of code is transitive implies

$$h_i(p) \triangleq H(X_i|\underline{Y}_{\sim i}) = \mathbb{E}\left[f_i(\underline{Z}_{\sim i})\right] = h(p) \quad \forall i$$

   Thus, EXIT Area Theorem says $\int_0^1 h(p)\mathrm{d}p = R$

Theorem 1: Outline of Proof

1. Permutation group of code is transitive implies

$$h_i(p) \triangleq H(X_i | \underline{Y}_{\sim i}) = \mathbb{E}\left[f_i(\underline{Z}_{\sim i})\right] = h(p) \quad \forall i$$

   Thus, EXIT Area Theorem says $\int_0^1 h(p)\mathrm{d}p = R$

2. Permutation group of code is doubly transitive implies

$$f_i\big(z_1, z_2, \ldots, z_{N-1}\big) = f_i\big(z_{\pi(1)}, z_{\pi(2)}, \ldots, z_{\pi(N-1)}\big) \;\; \forall \pi \in \mathcal{G}_i$$

   where $\mathcal{G}_i$ is a transitive group of permutations

Theorem 1: Outline of Proof

1. Permutation group of code is transitive implies

$$h_i(p) \triangleq H(X_i|\underline{Y}_{\sim i}) = \mathbb{E}\left[f_i(\underline{Z}_{\sim i})\right] = h(p) \quad \forall i$$

   Thus, EXIT Area Theorem says $\int_0^1 h(p)\mathrm{d}p = R$

2. Permutation group of code is doubly transitive implies

$$f_i\big(z_1, z_2, \ldots, z_{N-1}\big) = f_i\big(z_{\pi(1)}, z_{\pi(2)}, \ldots, z_{\pi(N-1)}\big) \ \ \forall \pi \in \mathcal{G}_i$$

   where $\mathcal{G}_i$ is a transitive group of permutations

3. Thus, f_i is a symmetric monotone boolean function and (B)KKL/FK implies the EXIT function has a sharp threshold!

$$h^{-1}(1-\delta) - h^{-1}(\delta) < C\frac{\ln N}{N} \quad \text{for all } \delta \in (0, 1/2)$$

Beyond Double Transitivity

- Possible extensions of Theorem 1
  - to more general (e.g., BMS) channels
  - to more codes based on minimum distances (d and $d^{\perp}$)
  - to more codes by using less symmetry (this talk)

Beyond Double Transitivity

- Possible extensions of Theorem 1
  - to more general (e.g., BMS) channels
  - to more codes based on minimum distances (d and $d^{\perp}$)
  - to more codes by using less symmetry (this talk)
- Quantifying Symmetry
  - Transitive symmetry is not enough ($\exists$ counterexample)
  - Fix $i, j \in \mathbb{Z}_N$ and compute $A_{i,j} \triangleq \left| \left\{ \left(\pi(i), \pi(j) \right) \,\middle|\, \pi \in \mathcal{G} \right\} \right|$
  - If $\mathcal{G}$ transitive, then $N \mid A_{i,j}$ and $A_{i,j} = A_{0,j'}$ for some j'
  - New condition equivalent to $A_{i,j}/N \to \infty$ for all $i \neq j$

Orbits and Stabilizers

- For a group $\mathcal{G}$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is

$$\mathcal{O}_i \triangleq \{j \in \mathbb{Z}_N \,|\, \exists \pi \in \mathcal{G}, \pi(i) = j\}\,.$$

- Note that for $i, j \in \mathbb{Z}_N$, either $\mathcal{O}_i = \mathcal{O}_j$ or $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$. Thus, the set of orbits, $\{\mathcal{O}_\ell\}$, partitions the set $\mathbb{Z}_N$.

Orbits and Stabilizers

- For a group $\mathcal{G}$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is
$$\mathcal{O}_i \triangleq \{j \in \mathbb{Z}_N \,|\, \exists \pi \in \mathcal{G}, \pi(i) = j\}\,.$$
- Note that for $i, j \in \mathbb{Z}_N$, either $\mathcal{O}_i = \mathcal{O}_j$ or $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$. Thus, the set of orbits, $\{\mathcal{O}_\ell\}$, partitions the set $\mathbb{Z}_N$.

- For group $\mathcal{G}$ acting on $\mathbb{Z}_N$, the stabilizer subgroup of $i \in \mathbb{Z}_N$ is
$$\mathcal{G}_i \triangleq \{\pi \in \mathcal{G} \,|\, \pi(i) = i\}\,.$$

Orbits and Stabilizers

- For a group $\mathcal{G}$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is

$$\mathcal{O}_i \triangleq \{j \in \mathbb{Z}_N \,|\, \exists \pi \in \mathcal{G}, \pi(i) = j\}\,.$$

- Note that for $i, j \in \mathbb{Z}_N$, either $\mathcal{O}_i = \mathcal{O}_j$ or $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$. Thus, the set of orbits, $\{\mathcal{O}_\ell\}$, partitions the set $\mathbb{Z}_N$.

- For group $\mathcal{G}$ acting on $\mathbb{Z}_N$, the stabilizer subgroup of $i \in \mathbb{Z}_N$ is

$$\mathcal{G}_i \triangleq \{\pi \in \mathcal{G} \,|\, \pi(i) = i\}\,.$$

- For $\mathcal{G}_i$, let the size of the smallest non-trivial orbit be

$$\mathcal{O}_{\min}(\mathcal{G}_i) \triangleq \min_{j \in \mathbb{Z}_N \setminus \{i\}} |\mathcal{O}_j(\mathcal{G}_i)|\,.$$

Capacity via Weak Symmetry for Erasure Channels

The previous result also holds with less symmetry [KCP16].

Theorem 2: Let $\{\mathcal{C}_n\}$ be a sequence of codes over $\mathbb{F}_q$ with

- transitive perm. groups $\mathcal{G}^{(n)}$ and rates $R_n \to R \in (0, 1)$,
- where the sequence $a_n = \mathcal{O}_{\min}\big(\mathcal{G}_0^{(n)}\big)$ satisfies $a_n \to \infty$.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Capacity via Weak Symmetry for Erasure Channels

The previous result also holds with less symmetry [KCP16].

Theorem 2: Let $\{\mathcal{C}_n\}$ be a sequence of codes over $\mathbb{F}_q$ with

- transitive perm. groups $\mathcal{G}^{(n)}$ and rates $R_n \to R \in (0,1)$,
- where the sequence $a_n = \mathcal{O}_{\min}\left(\mathcal{G}_0^{(n)}\right)$ satisfies $a_n \to \infty$.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Proof Idea

- Same as Theorem 1 except that we use a new sharp threshold result for weakly symmetric boolean functions

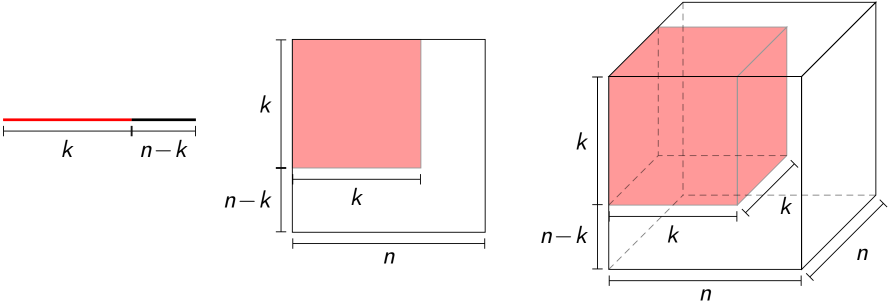
Example: Product Codes

$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$
$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$
$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$

Setup

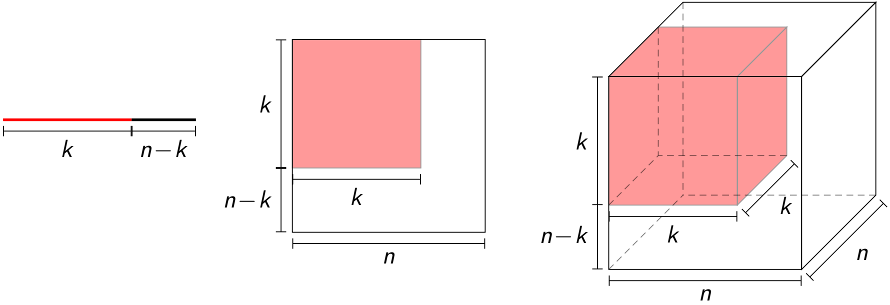
- $M \times N$ product code with doubly transitive component codes
- Permutations fixing $(0,0)$ are transitive on other rows/cols
- Each orbit has a distinct color, $\mathcal{O}_{\min}(\mathcal{G}_0) \geq \min\{M-1, N-1\}$

Multi-Dimensional Product Codes (1)



- Codeword of *m-dimensional product code* is array of n^m bits
- Axis-aligned 1D subarrays are codewords of (n, k) linear code
- Overall Rate: $R_m = (k/n)^m$

Multi-Dimensional Product Codes (1)



- Codeword of *m*-dimensional product code is array of n^m bits
- Axis-aligned 1D subarrays are codewords of (n, k) linear code
- Overall Rate: $R_m = (k/n)^m$

- If (n, k) code is $(n, n-1)$ single parity-check (SPC) code
  - Rate $R_m = \left(\frac{n-1}{n}\right)^m$ satisfies $\lim_{n\to\infty} R_n \to e^{-1}$

Multi-Dimensional Product Codes (2)

- For m-D product of (n, k) codes, we index bits by $\underline{v} \in \mathbb{Z}_n^m$
  - If (n, k) code transitive, then product code transitive
  - We permute code bits by permuting code dimensions
  - Code is preserved because component codes identical

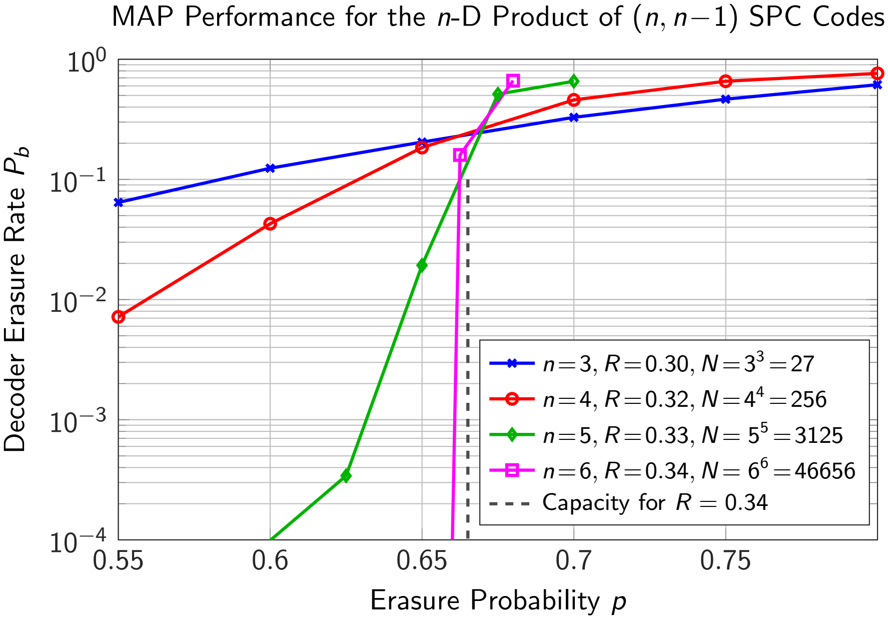
Multi-Dimensional Product Codes (2)

- For m-D product of (n, k) codes, we index bits by $\underline{v} \in \mathbb{Z}_n^m$
  - If (n, k) code transitive, then product code transitive
  - We permute code bits by permuting code dimensions
  - Code is preserved because component codes identical
- Consider size of the smallest non-trivial orbit $\mathcal{O}_{\min}(\mathcal{G}_0)$
  - Assume bit 0 associated with index $(0, \ldots, 0)$
  - Then, permuting code dimensions maps bit 0 to bit 0
  - Permuting code dimensions induces orbits defined by the empirical distribution of the index vector
  - Minimal orbits have one non-zero entry and $\mathcal{O}_{\min}(\mathcal{G}_0) \geq m$

Multi-Dimensional Product Codes (2)

- For m-D product of (n, k) codes, we index bits by $\underline{v} \in \mathbb{Z}_n^m$
  - If (n, k) code transitive, then product code transitive
  - We permute code bits by permuting code dimensions
  - Code is preserved because component codes identical
- Consider size of the smallest non-trivial orbit $\mathcal{O}_{\min}(\mathcal{G}_0)$
  - Assume bit 0 associated with index $(0, \ldots, 0)$
  - Then, permuting code dimensions maps bit 0 to bit 0
  - Permuting code dimensions induces orbits defined by the empirical distribution of the index vector
  - Minimal orbits have one non-zero entry and $\mathcal{O}_{\min}(\mathcal{G}_0) \geq m$
- n-D product of $(n, n-1)$ SPCs achieves capacity as $n \to \infty$!
  - Some prior work on SPC product codes [CTB95, RG01]

High-Dimensional SPC Product Codes



Let $f\colon \{0,1\}^M \to \{0,1\}$ be a monotone boolean function and $\underline{Z}$ be an iid Bernoulli-p random vector

- The expected value of f is defined to be

$$\mu_p(f) \triangleq \mathbb{E}\left[f(\underline{Z})\right] = \mathbb{P}\left(f(\underline{Z}) = 1\right)$$

Sharp Thresholds for Monotone Boolean Functions

Let $f\colon \{0,1\}^M \to \{0,1\}$ be a monotone boolean function and $\underline{Z}$ be an iid Bernoulli-p random vector

- The expected value of f is defined to be

$$\mu_p(f) \triangleq \mathbb{E}\left[f(\underline{Z})\right] = \mathbb{P}\left(f(\underline{Z}) = 1\right)$$

- The symmetry group of f is defined to be

$$\mathcal{G}(f) \triangleq \left\{\pi \in S_M \mid f(\underline{z}) = f(\pi(\underline{z})) \text{ for all } \underline{z} \in \{0,1\}^M\right\}$$

Let m_f be the size of the smallest orbit of $\mathcal{G}(f)$

Sharp Thresholds for Monotone Boolean Functions

Let $f\colon \{0,1\}^M \to \{0,1\}$ be a monotone boolean function
and $\underline{Z}$ be an iid Bernoulli-p random vector

- The expected value of f is defined to be

$$\mu_p(f) \triangleq \mathbb{E}\left[f(\underline{Z})\right] = \mathbb{P}\left(f(\underline{Z}) = 1\right)$$

- The symmetry group of f is defined to be

$$\mathcal{G}(f) \triangleq \left\{\pi \in S_M \mid f(\underline{z}) = f(\pi(\underline{z})) \text{ for all } \underline{z} \in \{0,1\}^M\right\}$$

Let m_f be the size of the smallest orbit of $\mathcal{G}(f)$

- BKKL implies transition width satisfies $\leq A\frac{M}{m_f \ln M}$

Sharp Thresholds for Monotone Boolean Functions

Let $f\colon \{0,1\}^M \to \{0,1\}$ be a monotone boolean function and $\underline{Z}$ be an iid Bernoulli-p random vector

- The expected value of f is defined to be

$$\mu_p(f) \triangleq \mathbb{E}\left[f(\underline{Z})\right] = \mathbb{P}\left(f(\underline{Z}) = 1\right)$$

- The symmetry group of f is defined to be

$$\mathcal{G}(f) \triangleq \left\{\pi \in S_M \mid f(\underline{z}) = f(\pi(\underline{z})) \text{ for all } \underline{z} \in \{0,1\}^M\right\}$$

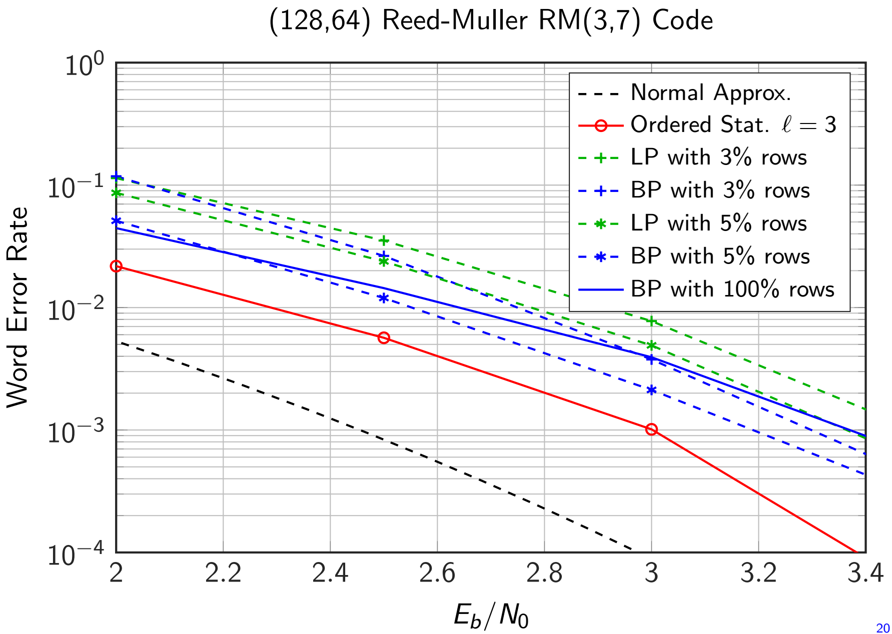
Let m_f be the size of the smallest orbit of $\mathcal{G}(f)$

- BKKL implies transition width satisfies $\leq A\frac{M}{m_f \ln M}$
- We improve this to transition width $\leq A\frac{1}{\ln m_f}$

Leveraging Symmetry in Practice (1)

- Can the symmetry group allow efficient decoding in practice?
  - A single low-weight parity-check generates many others
  - Thus, one can form a large overcomplete parity-check matrix and use iterative or LP decoding
  - For example, the (32,16) RM code has 620 parity checks and the (128,64) RM code has $\geq 90,000$ parity checks
- Reducing complexity
  - Decoding performance is good, but too many checks
  - Can we adaptively choose good checks?
  - For an (r, m) Reed-Muller code, minimum weight parity-checks are defined by $(r+1)$-dimensional affine subspaces of $\mathbb{F}_2^m$
  - Using bit soft-information, we can choose "good" checks!
- See also overcomplete decoding by Hehn et al. [HHML10]

Leveraging Symmetry in Practice (2)



Cyclic Codes and the Frobenius Automorphism

- For a length-N cyclic code over $\mathbb{F}_q$, the perm. group contains

$$\pi_q(i) \triangleq qi \bmod N, \quad i \in \mathbb{Z}_N$$

Cyclic Codes and the Frobenius Automorphism

- For a length-N cyclic code over $\mathbb{F}_q$, the perm. group contains

$$\pi_q(i) \triangleq qi \bmod N, \quad i \in \mathbb{Z}_N$$

- The orbit of $i \in \mathbb{Z}_N$ under π_q is the q-cyclotomic coset mod N:

$$C_i \triangleq \{i, iq, iq^2, \ldots, iq^{s-1}\} \bmod N$$

Cyclic Codes and the Frobenius Automorphism

- For a length-N cyclic code over $\mathbb{F}_q$, the perm. group contains

$$\pi_q(i) \triangleq qi \bmod N, \quad i \in \mathbb{Z}_N$$

- The orbit of $i \in \mathbb{Z}_N$ under π_q is the q-cyclotomic coset mod N:

$$C_i \triangleq \{i, iq, iq^2, \ldots, iq^{s-1}\} \bmod N$$

- Lemma: $\exists i \in \mathbb{Z}_N \setminus \{0\}$, $|C_i| = s$ iff $\gcd(q^s - 1, N) > 1$ and

$$|C_i| \geq \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N) > 1\}$$

Cyclic Codes and the Frobenius Automorphism

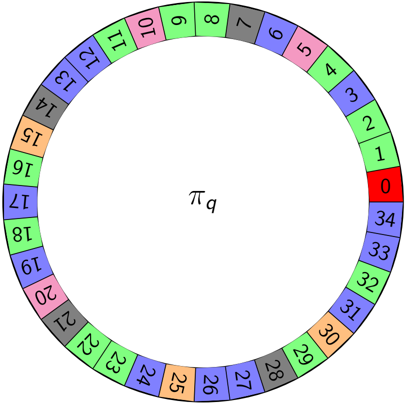
- For a length-N cyclic code over $\mathbb{F}_q$, the perm. group contains
$$\pi_q(i) \triangleq qi \bmod N, \quad i \in \mathbb{Z}_N$$

- The orbit of $i \in \mathbb{Z}_N$ under π_q is the q-cyclotomic coset mod N:
$$C_i \triangleq \{i, iq, iq^2, \ldots, iq^{s-1}\} \bmod N$$

- Lemma: $\exists i \in \mathbb{Z}_N \setminus \{0\}$, $|C_i| = s$ iff $\gcd(q^s - 1, N) > 1$ and
$$|C_i| \geq \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N) > 1\}$$

- If $\mathcal{C}^{(n)}$ is a sequence of length-N_n cyclic codes over $\mathbb{F}_q$ where
$$s_n = \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N_n) > 1\}$$
Then, $\mathcal{O}_{\min}(\mathcal{G}_0^{(n)}) \geq s_n$ and Theorem 2 applies if $s_n \to \infty$

Example: Orbits Induced by π_q : $N = 35$, $q = 2$



- Each orbit colored with a different color
- $N = 5\times 7 \;\Rightarrow\; \mathcal{O}_{\min} = \min\{s \in \mathbb{N} \mid \gcd(2^s - 1, N) > 1\} = 3$
- This defines $\mathcal{G}_0$ exactly for (35,16) binary code with

$$g(x) = x^{19} + x^{17} + x^{13} + x^{12} + x^{10} + x^{9} + x^{7} + x^{6} + x^{5} + x^{4} + 1$$

Capacity via Symmetry for Cyclic Codes

Combining the Frobenius automorphism with Theorem 2 gives:

Theorem 3: Let $\{\mathcal{C}_n\}$ be a seq. of cyclic codes over $\mathbb{F}_q$ with

- blocklengths $N_n \to \infty$ and rates $r_n \to r \in (0,1)$, where
- $s_n = \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N_n) > 1\}$ satisfies $s_n \to \infty$.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Capacity via Symmetry for Cyclic Codes

Combining the Frobenius automorphism with Theorem 2 gives:

Theorem 3: Let $\{\mathcal{C}_n\}$ be a seq. of cyclic codes over $\mathbb{F}_q$ with

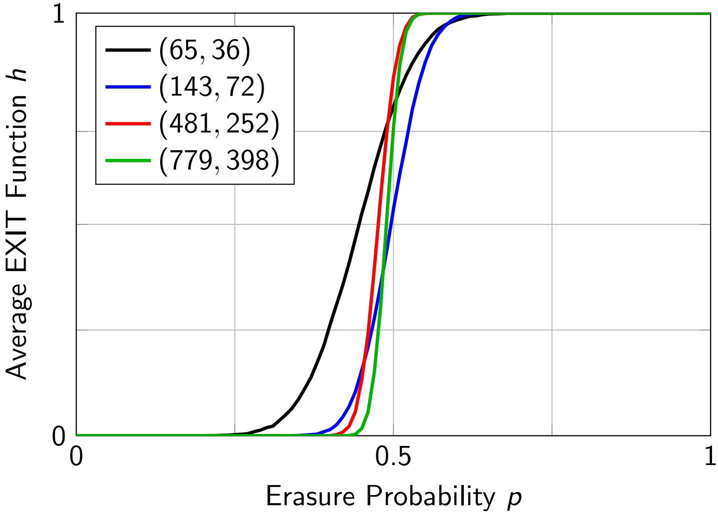
- blocklengths $N_n \to \infty$ and rates $r_n \to r \in (0,1)$, where
- $s_n = \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N_n) > 1\}$ satisfies $s_n \to \infty$.

Then, $\{C_n\}$ achieves capacity on the q-ary erasure channel (QEC) under symbol-MAP decoding.

Consequences and Details

- sequences of cyclic codes with prime N_n achieve capacity
- for example, r-th power residue codes of prime length

Cyclic Codes Without Double Transitive Symmetry



- Codes have $\min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N) > 1\} = \{4, 10, 12, 18\}$
- $\mathcal{G}_0$ orbits $=$ Frobenius π_q orbits (for $N = 65, 143$ via MAGMA)

Open Problems

- Non-linear codes on the BEC
  - For example, gray map images of $\mathbb{Z}_4$ linear codes
  - (i) Need to show $H(X_i|\underline{Y}_{\sim i} = \underline{y}_{\sim i}) \in \{0, 1\}$
  - (ii) Need to show binary symmetry (stronger than $\mathbb{Z}_4$ case)

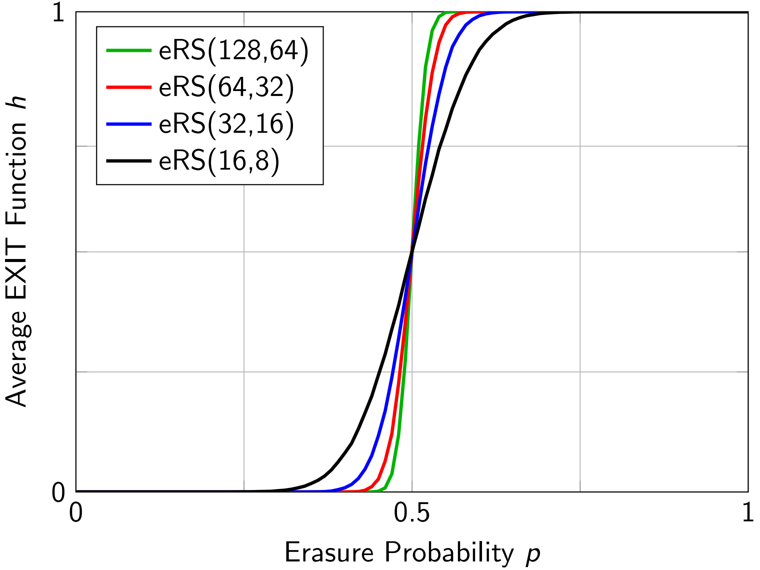
Open Problems

- Non-linear codes on the BEC
  - For example, gray map images of $\mathbb{Z}_4$ linear codes
  - (i) Need to show $H(X_i|\underline{Y}_{\sim i} = \underline{y}_{\sim i}) \in \{0, 1\}$
  - (ii) Need to show binary symmetry (stronger than $\mathbb{Z}_4$ case)
- Binary images of extended Reed-Solomon codes on the BEC
  - $\mathcal{G}_0$ transitive on blocks associated with RS symbols
  - But, $\mathcal{G}_0$ cannot move other bits in symbol 0
  - Problem similar to symmetry for $\mathbb{Z}_4$ codes

Open Problems

- Non-linear codes on the BEC
  - For example, gray map images of $\mathbb{Z}_4$ linear codes
  - (i) Need to show $H(X_i|\underline{Y}_{\sim i} = \underline{y}_{\sim i}) \in \{0, 1\}$
  - (ii) Need to show binary symmetry (stronger than $\mathbb{Z}_4$ case)
- Binary images of extended Reed-Solomon codes on the BEC
  - $\mathcal{G}_0$ transitive on blocks associated with RS symbols
  - But, $\mathcal{G}_0$ cannot move other bits in symbol 0
  - Problem similar to symmetry for $\mathbb{Z}_4$ codes
- More general (e.g., BMS) channels
  - Still have symmetry and GEXIT area theorem
  - But, GEXIT function is neither monotone nor boolean

Binary Images of Extended Reed-Solomon Codes



Summary and Open Questions

Main Results

- Product codes (under simple conditions) achieve capacity
- Cyclic codes with the right numerology achieve capacity!
- Sharp thresholds for monotone boolean fun. w/o transitivity
  - Proof relies on [Tal94] and a simple Fourier estimate

Open Questions

- Can this be extended to some non-linear codes on the BEC (e.g., grey mapping of $\mathbb{Z}_4$ linear codes)?
- Do all simple-root cyclic codes achieve capacity?
  - Implied by [KKMPSU] conjecture and Szemerédi's Theorem
- Is the sharp threshold extension useful for other problems?

Thank You!

References I

[BKK$^+$92] Jean Bourgain, Jeff Kahn, Gil Kalai, Yitzhak Katznelson, Nathan Linial.
The influence of variables in product spaces.
Israel Journal of Mathematics, 77(1-2):55–64, 1992.

[CTB95] Giuseppe Caire, Giorgio Taricco, Gérard Battail.
Weight distribution and performance of the iterated product of single-parity-check codes.
Annales Des Télécommunications, 50(9-10):752–761, 1995.

[FK96] Ehud Friedgut, Gil Kalai.
Every monotone graph property has a sharp threshold.
Proc. Amer. Math. Soc., 124(10):2993–3002, 1996.

[HHML10] Thorsten Hehn, Johannes B Huber, Olgica Milenkovic, Stefan Laendner.
Multiple-bases belief-propagation decoding of high-density cyclic codes.
IEEE Trans. Commun., 58(1):1–8, 2010.

References II

[KCP16] Santhosh Kumar, Robert Calderbank, Henry D. Pfister.
Beyond double transitivity: Capacity-achieving cyclic codes on erasure channels.
Proc. IEEE Inform. Theory Workshop, strony 241–245, Sept 2016.

[KKL88] J. Kahn, G. Kalai, N. Linial.
The influence of variables on boolean functions.
Proc. IEEE Symp. on the Found. of Comp. Sci., strony 68–80, Oct 1988.

[KKM+] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, R. L. Urbanke.
Reed-Muller codes achieve capacity on erasure channels.
Submitted to *IEEE Trans. Inform. Theory*, 2016. [Online]. Available: http://arxiv.org/pdf/1601.04689.pdf.

[RG01] David M Rankin, T Aaron Gulliver.
Single parity check product codes.
IEEE Trans. Inform. Theory, 49(8):1354–1362, 2001.

References III

[Tal94] Michel Talagrand.
On Russo's approximate zero-one law.
The Ann. of Prob., strony 1576–1587, 1994.