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 Şasoğlu
Outline

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

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

**uniform codeword:** $X = (X_0, \ldots, X_{N-1}) \in \{0, 1\}^N$

**Bernoulli-$p$ erasures:** $Z = (Z_0, \ldots, Z_{N-1}) \in \{0, 1\}^N$

**BEC($p$) observation of $X$:** $Y_i = \begin{cases} X_i & \text{if } Z_i = 0 \\ ? & \text{if } Z_i = 1 \end{cases}$
Problem Setup

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

uniform codeword: $X = (X_0, \ldots, X_{N-1}) \in \{0, 1\}^N$

Bernoulli-$p$ erasures: $Z = (Z_0, \ldots, Z_{N-1}) \in \{0, 1\}^N$

BEC($p$) observation of $X$: $Y_i = \begin{cases} X_i & \text{if } Z_i = 0 \\ ? & \text{if } Z_i = 1 \end{cases}$

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

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

where $h_i(p)$ is the MAP EXIT function of bit-$i$. 
Recently, it was shown that symmetry alone is sufficient for a code sequence to achieve capacity on erasure channels [KKMPSU16]

Theorem 1: Let \( \{C_n\} \) 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 \( C_n \) is doubly transitive.

Then, \( \{C_n\} \) achieves capacity on the \( q \)-ary erasure channel (QEC) under symbol-MAP decoding.
Recently, it was shown that symmetry alone is sufficient for a code sequence to achieve capacity on erasure channels [KKMPSU16]

**Theorem 1:** Let \( \{C_n\} \) 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 \( C_n \) 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: $b = \pi(a) \iff b\pi(i) = a_i$
- The permutation group of $\mathcal{A}$ is defined to be

$$G \triangleq \{ \pi \in S_N \mid \pi(a) \in \mathcal{A} \ \forall \ a \in \mathcal{A} \}$$
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: $b = \pi(a) \iff b_{\pi(i)} = a_i$
- The permutation group of $\mathcal{A}$ is defined to be

$$\mathcal{G} \triangleq \{ \pi \in S_N \mid \pi(a) \in \mathcal{A} \ \forall \ a \in \mathcal{A} \}$$

Permutation group of $\mathcal{A}$

$$\mathcal{A} = \begin{cases} (0\ 0\ 0\ 0) \\ (0\ 0\ 1\ 1) \\ (1\ 1\ 0\ 0) \\ (1\ 1\ 1\ 1) \end{cases} \quad \Longrightarrow \quad \mathcal{G} = \begin{cases} \ (0\ 1\ 2\ 3) & (0\ 1\ 2\ 3) \\ \ (0\ 1\ 2\ 3) & (1\ 0\ 2\ 3) \\ \ (0\ 1\ 3\ 2) & (0\ 1\ 2\ 3) \\ \ (0\ 1\ 2\ 3) & (0\ 1\ 2\ 3) \\ \ (0\ 1\ 2\ 3) & (0\ 1\ 2\ 3) \\ \ (2\ 3\ 0\ 1) & (3\ 2\ 0\ 1) \\ \ (2\ 3\ 1\ 0) & (3\ 2\ 1\ 0) \end{cases}$$
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: $b = \pi(a) \iff b_{\pi(i)} = a_i$
  - The permutation group of $\mathcal{A}$ is defined to be
    \[
    \mathcal{G} \triangleq \{ \pi \in S_N | \pi(a) \in \mathcal{A} \ \forall \ a \in \mathcal{A} \}
    \]
  - 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

\[
\mathcal{A} = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \right\} \quad \implies \quad \mathcal{G} = \left\{ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix} \right\}
\]
The Permutation Group of a Set of Vectors

For a set \( A \subseteq \mathcal{X}^N \) of vectors

- Permutations \( \pi \in S_N \) act on \( \mathcal{X}^N \) via: \( b = \pi(a) \iff b_{\pi(i)} = a_i \)
- The permutation group of \( A \) is defined to be
  \[
  G \triangleq \{ \pi \in S_N \mid \pi(a) \in A \ \forall \ a \in A \}
  \]
- A permutation group \( G \) is transitive if, for all \( i, j \in \mathbb{Z}_N \), there exists \( \pi \in G \) such that \( \pi(i) = j \)
- \( G \) is doubly transitive if, for any \( i, j, k, l \in \mathbb{Z}_N \) with \( i \neq j \) and \( k \neq l \), there exists \( \pi \in G \) such that \( \pi(i) = k \) and \( \pi(j) = l \).

Permutation group of \( A \) is transitive but not doubly transitive

\[
A = \begin{Bmatrix}
(0 \ 0 \ 0 \ 0 \\
0 \ 0 \ 1 \ 1 \\
1 \ 1 \ 0 \ 0 \\
1 \ 1 \ 1 \ 1
\end{Bmatrix} \quad \implies \quad G = \begin{Bmatrix}
(0 \ 1 \ 2 \ 3) & (0 \ 1 \ 2 \ 3) \\
(0 \ 1 \ 2 \ 3) & (1 \ 0 \ 2 \ 3) \\
(0 \ 1 \ 2 \ 3) & (0 \ 1 \ 2 \ 3) \\
(0 \ 1 \ 2 \ 3) & (1 \ 0 \ 3 \ 2) \\
(0 \ 1 \ 2 \ 3) & (0 \ 1 \ 2 \ 3) \\
(2 \ 3 \ 0 \ 1) & (3 \ 2 \ 0 \ 1) \\
(2 \ 3 \ 1 \ 0) & (0 \ 1 \ 2 \ 3)
\end{Bmatrix}
\]
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

$$h(p) \triangleq \frac{1}{N} \sum_{i=0}^{N-1} H(X_i | Y_{\sim i}(p))$$

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

\[
h(p) \triangleq \frac{1}{N} \sum_{i=0}^{N-1} H(X_i|\underline{Y}_i(p)) \]

- EXIT Area Theorem [ABK04]

\[
\int_{0}^{1} h(p) dp = R \quad \text{(code rate)}
\]

Note: \(\underline{Y}_i \triangleq (Y_0, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_{N-1})\)
Properties of the MAP EXIT Function

- For linear codes, the recovery of $X_i$ from $Y_{\sim i} = y_{\sim i}$
  - is independent of the transmitted codeword $X$
  - only depends on erasure indicator $z_i = 1_{\{?\}}(y_i)$
  - is a zero-one boolean function of $z_{\sim i}$
Properties of the MAP EXIT Function

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

- Bit-\textit{i} EXIT function is a monotone boolean function $f_i$ of $Z_{\sim i}$

\[
H(X_i | Y_{\sim i} = y_{\sim i}, Z_{\sim i} = z_{\sim i}) = f_i(z_{\sim i}) \in \{0, 1\},
\]

where $z_{\sim i} \triangleq (z_0, \ldots, z_{i-1}, z_{i+1}, \ldots, z_{N-1})$
Properties of the MAP EXIT Function

- For linear codes, the recovery of $X_i$ from $Y_{\sim i} = y_{\sim i}$
  - is independent of the transmitted codeword $X$
  - only depends on erasure indicator $z_i = 1_{\{\cdot\}}(y_i)$
  - is a zero-one boolean function of $z_{\sim i}$

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

$$H(X_i | Y_{\sim i} = y_{\sim i}, Z_{\sim i} = z_{\sim i}) = f_i(z_{\sim i}) \in \{0, 1\},$$

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

- “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
$h^{-1}(1-\delta) - h^{-1}(\delta) = \text{transition width}$ where $\delta \leq h(p) \leq 1-\delta$
The MAP EXIT Curve of a Capacity-Achieving Code

\[ h^{-1}(1 - \delta) - h^{-1}(\delta) = \text{transition width} \quad \text{where} \quad \delta \leq h(p) \leq 1 - \delta \]

Area Theorem implies sharp transition iff capacity achieving
The MAP EXIT Curve of a Capacity-Achieving Code

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

\[ \text{Area Theorem implies sharp transition iff capacity achieving} \]
The MAP EXIT Curve of a Capacity-Achieving Code

\[
\begin{align*}
\text{Average EXIT Function } h \\
\text{Erasure Probability } p
\end{align*}
\]

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

\[\text{Area Theorem implies sharp transition iff capacity achieving}\]
Theorem 1: Outline of Proof

1. **Permutation group** of code is **transitive** implies

   \[ h_i(p) \triangleq H(X_i | Y_{\sim i}) = \mathbb{E} [f_i(Z_{\sim i})] = h(p) \quad \forall i \]

   Thus, EXIT Area Theorem says \( \int_0^1 h(p) \, dp = R \)
Theorem 1: Outline of Proof

1. Permutation group of code is transitive implies

\[ h_i(p) \triangleq H(X_i|Y_{\sim i}) = \mathbb{E}[f_i(Z_{\sim i})] = h(p) \quad \forall i \]

Thus, EXIT Area Theorem says \( \int_0^1 h(p) \, dp = R \)

2. Permutation group of code is doubly transitive implies

\[ f_i(z_1, z_2, \ldots, z_{N-1}) = f_i(z_{\pi(1)}, z_{\pi(2)}, \ldots, z_{\pi(N-1)}) \quad \forall \pi \in G_i \]

where \( G_i \) is a transitive group of permutations
Theorem 1: Outline of Proof

1. Permutation group of code is transitive implies

\[ h_i(p) \triangleq H(X_i|Y_{\sim i}) = \mathbb{E}[f_i(Z_{\sim i})] = h(p) \quad \forall i \]

Thus, EXIT Area Theorem says \( \int_0^1 h(p) \, dp = R \)

2. Permutation group of code is doubly transitive implies

\[ f_i(z_1, z_2, \ldots, z_{N-1}) = f_i(z_{\pi(1)}, z_{\pi(2)}, \ldots, z_{\pi(N-1)}) \quad \forall \pi \in G_i \]

where \( G_i \) 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 $A_{i,j} \triangleq |\{(\pi(i), \pi(j)) | \pi \in \mathcal{G}\}|$
  - 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 $i \neq j$
For a group $G$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is

$$O_i \triangleq \{j \in \mathbb{Z}_N \mid \exists \pi \in G, \pi(i) = j\}.$$ 

Note that for $i, j \in \mathbb{Z}_N$, either $O_i = O_j$ or $O_i \cap O_j = \emptyset$. Thus, the set of orbits, $\{O_\ell\}$, partitions the set $\mathbb{Z}_N$. 

For $G_i$, let the size of the smallest non-trivial orbit be $O_{\min}(G_i) = \min_{j \in \mathbb{Z}_N \setminus \{i\}} |O_j(G_i)|$. 
For a group $G$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is

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

Note that for $i, j \in \mathbb{Z}_N$, either $O_i = O_j$ or $O_i \cap O_j = \emptyset$. Thus, the set of orbits, $\{O_\ell\}$, partitions the set $\mathbb{Z}_N$.

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

$$G_i \triangleq \{ \pi \in G | \pi(i) = i \}.$$
For a group $G$ acting on $\mathbb{Z}_N$, the orbit of $i \in \mathbb{Z}_N$ is

$$O_i \triangleq \{ j \in \mathbb{Z}_N \mid \exists \pi \in G, \pi(i) = j \} .$$

Note that for $i, j \in \mathbb{Z}_N$, either $O_i = O_j$ or $O_i \cap O_j = \emptyset$. Thus, the set of orbits, $\{O_\ell\}$, partitions the set $\mathbb{Z}_N$.

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

$$G_i \triangleq \{ \pi \in G \mid \pi(i) = i \} .$$

For $G_i$, let the size of the smallest non-trivial orbit be

$$O_{\text{min}}(G_i) \triangleq \min_{j \in \mathbb{Z}_N \setminus \{i\}} |O_j(G_i)| .$$
The previous result also holds with less symmetry [KCP16].

**Theorem 2:** Let \( \{C_n\} \) be a sequence of codes over \( \mathbb{F}_q \) with

- transitive perm. groups \( G^{(n)} \) and rates \( R_n \to R \in (0, 1) \),
- where the sequence \( a_n = O_{\text{min}}(G_0^{(n)}) \) satisfies \( a_n \to \infty \).

Then, \( \{C_n\} \) achieves capacity on the \( q \)-ary erasure channel (QEC) under symbol-MAP decoding.
The previous result also holds with less symmetry [KCP16].

**Theorem 2:** Let \( \{C_n\} \) be a sequence of codes over \( \mathbb{F}_q \) with
- transitive perm. groups \( G^{(n)} \) and rates \( R_n \rightarrow R \in (0, 1) \),
- where the sequence \( a_n = \mathcal{O}_{\min}(G_0^{(n)}) \) satisfies \( a_n \rightarrow \infty \).

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

<table>
<thead>
<tr>
<th>(0, 0)</th>
<th>(0, 1)</th>
<th>(0, 2)</th>
<th>(0, 3)</th>
<th>(0, 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1, 0)</td>
<td>(1, 1)</td>
<td>(1, 2)</td>
<td>(1, 3)</td>
<td>(1, 4)</td>
</tr>
<tr>
<td>(2, 0)</td>
<td>(2, 1)</td>
<td>(2, 2)</td>
<td>(2, 3)</td>
<td>(2, 4)</td>
</tr>
</tbody>
</table>

**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, $O_{\text{min}}(G_0) \geq \min\{M - 1, N - 1\}$
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 $\lim_{n \to \infty} R_n \to e^{-1}$
For $m$-D product of $(n, k)$ codes, we index bits by $v \in \mathbb{Z}_n^m$

- 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 $O_{\text{min}}(G_0)$

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 $O_{\text{min}}(G_0) \geq m$

$n$-D product of $(n, n-1)$ SPCs achieves capacity as $n \to \infty$

Some prior work on SPC product codes [CTB95, RG01]
Multi-Dimensional Product Codes (2)

- For $m$-D product of $(n, k)$ codes, we index bits by $v \in \mathbb{Z}_n^m$
  - 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 $O_{\text{min}}(G_0)$
  - 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 $O_{\text{min}}(G_0) \geq m$
Multi-Dimensional Product Codes (2)

- For $m$-D product of $(n, k)$ codes, we index bits by $\mathbf{v} \in \mathbb{Z}_n^m$
  - 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 $O_{\text{min}}(G_0)$
  - 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 $O_{\text{min}}(G_0) \geq m$

- $n$-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

MAP Performance for the $n$-D Product of $(n, n - 1)$ SPC Codes

- $n = 3$, $R = 0.30$, $N = 3^3 = 27$
- $n = 4$, $R = 0.32$, $N = 4^4 = 256$
- $n = 5$, $R = 0.33$, $N = 5^5 = 3125$
- $n = 6$, $R = 0.34$, $N = 6^6 = 46656$
- Capacity for $R = 0.34$

Erasure Probability $p$

Decoder Erasure Rate $P_b$
Let $f : \{0, 1\}^M \rightarrow \{0, 1\}$ be a monotone boolean function and $Z$ be an iid Bernoulli-$p$ random vector.

- The expected value of $f$ is defined to be

$$\mu_p(f) \triangleq \mathbb{E}[f(Z)] = \mathbb{P}(f(Z) = 1)$$
Let $f : \{0, 1\}^M \rightarrow \{0, 1\}$ be a monotone boolean function and $Z$ be an iid Bernoulli-$p$ random vector

- The expected value of $f$ is defined to be
  \[
  \mu_p(f) \triangleq \mathbb{E} [f(Z)] = \mathbb{P} (f(Z) = 1)
  \]

- The symmetry group of $f$ is defined to be
  \[
  G(f) \triangleq \left\{ \pi \in S_M \mid f(Z) = f(\pi(Z)) \text{ for all } Z \in \{0, 1\}^M \right\}
  \]

Let $m_f$ be the size of the smallest orbit of $G(f)$
Let \( f : \{0, 1\}^M \rightarrow \{0, 1\} \) be a monotone boolean function and \( Z \) be an iid Bernoulli-\( p \) random vector

▶ The expected value of \( f \) is defined to be

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

▶ The symmetry group of \( f \) is defined to be

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

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

▶ BKKL implies transition width satisfies

\[
\leq A \frac{M}{m_f \ln M}
\]
Let $f : \{0, 1\}^M \to \{0, 1\}$ be a monotone boolean function and $Z$ be an iid Bernoulli-$p$ random vector.

- The expected value of $f$ is defined to be
  \[
  \mu_p(f) \triangleq \mathbb{E} [f(Z)] = \mathbb{P}(f(Z) = 1)
  \]

- The symmetry group of $f$ is defined to be
  \[
  \mathcal{G}(f) \triangleq \left\{ \pi \in S_M \mid f(z) = f(\pi(z)) \text{ for all } z \in \{0, 1\}^M \right\}
  \]
  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 $\leq A \frac{1}{\ln m_f}$
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)

(128,64) Reed-Muller RM(3,7) Code

Word Error Rate vs. $E_b/N_0$ for different decoding methods and error rates.
For a length-$N$ cyclic code over $\mathbb{F}_q$, the perm. group contains
\[ \pi_q(i) \triangleq qi \mod N, \quad i \in \mathbb{Z}_N \]
Cyclic Codes and the Frobenius Automorphism

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

- The orbit of $i \in \mathbb{Z}_N$ under $\pi_q$ is the $q$-cyclotomic coset mod $N$:
  \[ C_i \triangleq \{ i, iq, iq^2, \ldots, iq^{s-1} \} \mod N \]
Cyclic Codes and the Frobenius Automorphism

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

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

- Lemma: \( \exists i \in \mathbb{Z}_N \setminus \{0\}, \ |C_i| = s \text{ iff } \gcd(q^s - 1, N) > 1 \text{ and } \)
  \[ |C_i| \geq \min\{s \in \mathbb{N} | \gcd(q^s - 1, N) > 1\} \]
Cyclic Codes and the Frobenius Automorphism

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

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

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

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

▶ 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 $C^{(n)}$ 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, $O_{\min}(G^{(n)}_0) \geq s_n$ and Theorem 2 applies if $s_n \to \infty$
Example: Orbits Induced by $\pi_q : N = 35, q = 2$

- Each orbit colored with a different color
- $N = 5 \times 7 \Rightarrow O_{\text{min}} = \min\{s \in \mathbb{N} \mid \gcd(2^s - 1, N) > 1\} = 3$
- This defines $G_0$ exactly for (35,16) binary code with

$$g(x) = x^{19} + x^{17} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + 1$$
Combining the Frobenius automorphism with Theorem 2 gives:

**Theorem 3:** Let \( \{C_n\} \) 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.
Combining the Frobenius automorphism with Theorem 2 gives:

**Theorem 3:** Let \( \{C_n\} \) 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
- \( s_n = \min\{s \in \mathbb{N} | \gcd(q^s - 1, N_n) > 1\} \) 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 \( \text{prime} \ N_n \) achieve capacity
- for example, \( r \)-th power residue codes of prime length
Cyclic Codes Without Double Transitive Symmetry

- Codes have \( \min\{s \in \mathbb{N} \mid \gcd(q^s - 1, N) > 1\} = \{4, 10, 12, 18\} \)
- \( G_0 \) orbits = Frobenius \( \pi_q \) 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 $H(X_i|Y_i = y_i) \in \{0, 1\}$
  - (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 $H(X_i|\underline{Y}_i = \underline{y}_i) \in \{0, 1\}$
  - (ii) Need to show binary symmetry (stronger than $\mathbb{Z}_4$ case)

- Binary images of extended Reed-Solomon codes on the BEC
  - $G_0$ transitive on blocks associated with RS symbols
  - But, $G_0$ 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 $H(X_i|Y \sim_i = y \sim_i) \in \{0, 1\}$
  - (ii) Need to show binary symmetry (stronger than $\mathbb{Z}_4$ case)

- Binary images of extended Reed-Solomon codes on the BEC
  - $G_0$ transitive on blocks associated with RS symbols
  - But, $G_0$ 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

Erasure Probability $p$

Average EXIT Function $h$

- eRS(128,64)
- eRS(64,32)
- eRS(32,16)
- eRS(16,8)
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!
The influence of variables in product spaces.

[CTB95] Giuseppe Caire, Giorgio Taricco, Gérard Battail.
Weight distribution and performance of the iterated product of single-parity-check codes.

[FK96] Ehud Friedgut, Gil Kalai.
Every monotone graph property has a sharp threshold.

[HHML10] Thorsten Hehn, Johannes B Huber, Olgica Milenkovic, Stefan Laendner.
Multiple-bases belief-propagation decoding of high-density cyclic codes.
References II


On Russo's approximate zero-one law.