Capacity Via Symmetry I - A New Proof for an Old Code

[ H. Mondelli, S. Kudekar, S. Kumar, H.D. Pfister, E. Sasoglu, R. Urbanke]

Basic question of coding theory: how to achieve channel capacity?

1. **Random Codes**
   - Create ensemble with pairwise independent codewords.
   - Use typically decoders.
   - Several classical proofs of this by Feinstein, Elias, Wolfowitz, and Gallager.
   - Weight distribution sufficiently close to random one.
   - [Polyanskiy, Shoklma, Feder 09]

2. **Sparse Graph Codes**
   - Explicitly write down evolution of the decoding process when block length $\to \infty$ (density evolution).
   - [Kudekar, Richardson, Urbanke 13]

3. **Polar Codes**
   - Concept of channel polarization.
   - Proof "backwards" into the construction of the code.
   - [Arikan 09]

4. **Symmetry**
Thresholds in Coding Theory

\( P_e(n, \varepsilon) \) = error probability for our code of block length \( n \) transmitted over a channel with parameter \( \varepsilon \).

Think to \( \varepsilon \) as channel quality (e.g., \( \text{BEC}(\varepsilon) \))

\( P_e(n, \varepsilon) \) increasing in \( \varepsilon \).

Define \( \varepsilon(n, \delta) \) as the channel parameter s.t. \( P_e(n, \varepsilon(n, \delta)) = \delta \).

Then, we want that \( \varepsilon(n, 1-\delta) - \varepsilon(n, \delta) \to 0 \) \((\ast)\).

**Note:** If we want a code that is capacity-achieving, then the threshold must be at capacity. This follows both from the strong converse of coding theory and from one of our basic techniques.

[Tillich - Tewod 00] Let \( C \) be a binary, linear code of minimum distance \( d \). Consider transmission over the \( \text{BEC}(\varepsilon) \) or the \( \text{BSC}(\varepsilon) \) and optimal MAP decoding.

\[ \varepsilon(n, 1-\delta) - \varepsilon(n, \delta) \leq \frac{c(\delta)}{\sqrt{d}} \]

where \( c(\delta) \) is an explicit universal constant depending only on \( \delta \).
If the code sequence has linear minimum distance \( d = \alpha n \), then the transinformation occurs in \( O\left(\frac{1}{\sqrt{n}}\right) \).

This is as sharp as it can be since the channel variances are already of order \( \frac{1}{\sqrt{n}} \) (e.g., the typical number of erasures is \( n e \pm c \sqrt{n} \)).

EXIT Function and Area Theorem

1) Introduced as a visual tool to understand iterative decoding for the BEC [Ashikhmin-Kramer-Ten Brink 04]

2) Connect to entropy for general channels [Yassaee-Houtanari 08; Richardson-Urbanke 08]

EXIT FUNCTION

\[
\hat{p}(E) = \frac{1}{n} \frac{d}{d E} \frac{H(X|Y)}{H(X)}
\]

\[
H(X) = n R
\]

\[
\int_0^1 \hat{p}(E) = \frac{1}{n} \left[ H(X|Y(E=1)) - H(X|Y(E=0)) \right] = R
\]

The area under the EXIT function is a preserved quantity and does not depend on the code.

Claim

\[
\hat{p}(E) = \frac{1}{n} \sum_{i=1}^{n} P \left( \hat{X}_{i} \mid Y_{i} = ? , Y_{i-1}, Y_{i+1}, \ldots, Y_{n} \right)
\]

\( \hat{X}_{i} \) is an estimator of \( \cdot \)th code bit given observation \( Y_{i} \).
Proof [Perhaps to be omitted if there is no true]

\[ n \mathbf{p}(\varepsilon) = \frac{1}{\varepsilon} \sum_{i=1}^{n} \mathbf{H}(X_i | Y_i(\varepsilon), \ldots, Y_n(\varepsilon)) \]

\[ = \sum_{i=1}^{n} \mathbf{H}(X_i | Y_i(\varepsilon), Y_i) \]

\[ \text{chain rule} \]

\[ = \sum_{i=1}^{n} \mathbf{H}(X_i | Y_{\pi_i}, Y_i) \]

\[ \text{does not depend on } \varepsilon_i \quad \forall \varepsilon \in [n] \]

\[ \varepsilon_i = \varepsilon \quad \forall i \in [n] \]

\[ \mathbb{P}(X_{i}^{\text{MAP}}(Y_{\pi_i}) = ?) = \sum_{i=1}^{n} f_i(\varepsilon) \]
The Proof!

Ingredients:
1. Symmetry - 2-transitivity
2. Monotone symmetric sets have sharp thresholds
3. EXIT function & Area theorem

\[\begin{align*}
\{ & x_1, \ldots, x_n \\ & x_{21}, \ldots, x_{2n} \\ & \vdots \\ & x_{n1}, \ldots, x_{nn} \} \\
& \text{N codewords}
\end{align*}\]

\[\begin{align*}
\forall a, b, c, d & \in [n] \text{ s.t. } a \neq c, \ b \neq d, \\
\exists \pi: & [n] \rightarrow [n] \text{ so that} \\
& \pi(a) = c \\
& \pi(b) = d \\
& \pi(c) = c
\end{align*}\]

"For any \( a \neq c, \ b \neq d \), there exists a permutation mapping \( a \) in \( c \) and \( b \) in \( d \) that leaves the code invariant."

Claim [Kasami - Lin - Peterson 68]:
RH codes are 2-transitive.
\[ \Omega \leq \binom{N}{10} \]

\[ \Omega \text{ MONOTONE } \quad \text{if} \quad \omega \triangleright \omega' \implies \| \omega \|_2 \geq \| \omega' \|_2 \]

"By adding more 1s, we remain in \( \Omega \)."

\[ \Omega \text{ SYMMETRIC } \quad \text{if} \quad \Omega \text{ is 1-transitive} \]

"For any \( a, b \), there exists a permutation mapping \( a \mapsto b \) that leaves \( \Omega \) invariant."

This ensures that no single variable has too much influence.

\[
\mu_\varepsilon(\Omega) = \sum_{\omega \in \Omega} \mu_\varepsilon(\omega) = \sum_{\omega \in \Omega} \varepsilon^{W_0(\omega)} (1-\varepsilon)^{N-W_0(\omega)}
\]

Bernoulli product measure with parameter \( \varepsilon \).

"\( \mu_\varepsilon(\Omega) \) is the probability that an i.i.d. \( \text{Bern}(\varepsilon) \) vector is \( \omega \in \Omega \)."

Friedgut-Kalai '96 \[ \text{Claim} \]

Let \( \Omega \leq \binom{N}{10} \) be monotone and symmetric and pick \( \varepsilon > 0 \). Then, \( \mu_\varepsilon(\Omega) \) goes from \( \delta \) to \( 1-\delta \) in a window of size \[ \frac{\log(1/\delta)}{\log N} \]
Transmission over \( \text{BEC}(\epsilon) \).

\( \mathcal{E}_i \) is the set of "bad" erasure patterns for bit \( i \).

"No erasure" given \( Y_i \), it is not possible to recover \( x_i \).

**Example:** we receive \( 0 \ ? \ 1 \ ? \ 0 \ ? \ ? \).

Pick \( i = 2 \), then \( w = 0 \ 0 \ 1 \ 0 \ 1 \).

By definition \( \mathcal{I}_i(\epsilon) = \Pr(\hat{x} \neq x | Y_{\text{err}} = \epsilon) = \mu_e(\mathcal{E}_i) \).

\( \mathcal{I}_i \) monotone "more erasures can only hurt"

Proof: \( w \) has more erasures than \( w' \)

\( w \succ w' \)

If I cannot decode under \( w' \), I will certainly not be able to decode under \( w \)

\( \mathcal{I}_i(w) \geq \mathcal{I}_i(w') \).

\( \mathcal{I}_i \) symmetric follows from 2-taunhnty of the code

Proof: [Perhaps to be omitted if there is no time]

Fix \( a, b \), then \( \exists \ \bar{a}' \) s.t. \( \bar{a}'(a) = b \) and \( \bar{a}'(w) \in \mathcal{I}_i \) for \( \forall w \in \mathcal{I}_i \).

This is the claim.

Code is 2-taunhnte \( \Rightarrow \exists \ \bar{a}' \) s.t.

\[ \bar{a}'(a) = b \]
\[ \bar{a}'(i) = i \]

Idea: construct \( \bar{u} \) from \( \bar{a}' \) by removing \( i \) position.

\( w \in \mathcal{I}_i \Rightarrow \) there are two compatible codewords \( c_1, c_2 \) differing in position \( i \) under erasure pattern \( w \Rightarrow \bar{a}'(c_1) \), \( \bar{a}'(c_2) \) are two compatible codewords differing in position \( i \) under erasure pattern \( \bar{a}(w) \Rightarrow \bar{a}(w) \in \mathcal{I}_i \).
INDEPENDENCE

\[ \mu_E(\omega_i) = \mu_E(\omega_j) \quad \forall i, j \in [n] \]
follows from

Proof: Perhaps to be omitted if there is no hint. 

There exists \( \tilde{u} \) such that \( \tilde{u}(i) = i \) and \( \tilde{u}(j) = j \).

\[ \omega \in \Omega_i \Rightarrow \text{there are two compatible codewords } c_1, c_2 \text{ differing in position } i \text{ under erasure pattern } \omega \Rightarrow \tilde{u}(c_1), \tilde{u}(c_2) \text{ compatible codewords differing in position } j \text{ under an erasure pattern } \omega \in \Omega_j \text{ with the same weight as } \omega. \]

Thus \( \mu_E(\omega_i) \leq \mu_E(\omega_j) \), since different elements of \( \Omega_i \) are mapped into different elements of \( \Omega_j \).

Revers the role of \( i \) and \( j \) in the previous argument and we obtain

INDEPENDENCE \[ \Rightarrow \quad f(\epsilon) = f_i(\epsilon) \quad \forall i \in [n] \]

\( \Omega \): MONOTONE + SYMMETRIC \[ \Rightarrow \quad f(c) \mid \text{SHARP THRESHOLD} \]

\[ f(\epsilon) = \begin{cases} 0 & \epsilon < s \\ A & \epsilon = 1 \\ 1 - s & \epsilon > 1 \\ \log(1/\sqrt{\log(n)}) & \text{for } \epsilon \approx 1 - R \\ \end{cases} \]

Area theorem \[ \Rightarrow \quad \text{Threshold is at } 1 - R \]

Reliable transmission possible IFF \( R < 1 - R \)

\[ R < 1 - \epsilon = C \]

\[ \Downarrow \]

RSC codes achieve capacity!