Reed-Muller Codes Achieve Capacity on Erasure Channels

Shrinivas Kudekar, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Şaşoğlu, Rüdiger Urbanke

Project presentation, E2 207 – Concentration Inequalities†

January 18, 2018

† *presented by* K. R. Sahasranand, Dept. of Electrical Communication Engg., IISc.

Proof Outline

- Preliminaries
- Key ingredients
  - Reed Muller codes are doubly transitive
  - Symmetric monotone sets have sharp thresholds
  - EXIT† functions satisfy the area theorem
- Conclusion

† EXtrinsic Information Transfer

Preliminaries

Binary Erasure Channel (BEC) and MAP decoder

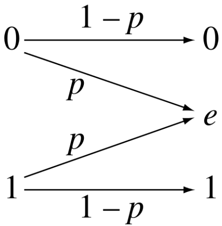


Figure: Denoted BEC(p). If X_i is transmitted over BEC(p_i), referred to as BEC($\underline{p}$)

- $D_i : \mathcal{Y}^N \to \mathcal{X} \cup \{e\}$: bit-MAP decoder for bit i.
- Erasure probability for bit $i \in [N]$, $P_{b,i} \triangleq \mathbb{P}[D_i(\underline{Y}) \neq X_i]$.
  Average bit erasure probability, $P_b \triangleq \frac{1}{N}\sum_{i=1}^{N} P_{b,i}$.
- If bit i is recovered given $\underline{y}$, $H(X_i|\underline{Y} = \underline{y}) = 0$.
  Otherwise, uniform codeword assumption $\Rightarrow H(X_i|\underline{Y} = \underline{y}) = 1$. Thus, $P_{b,i} = H(X_i|\underline{Y})$ and, $P_b = \frac{1}{N}\sum_{i=1}^{N} H(X_i|\underline{Y})$.

Preliminaries

MAP EXIT functions

The vector EXIT function associated with bit i of the (uniformly randomly chosen) codeword

$$h_i(\underline{p}) \triangleq H(X_i|\underline{Y}_{-i}(\underline{p}_{-i})).$$

The average vector EXIT function is defined by

$$h(\underline{p}) \triangleq \frac{1}{N}\sum_{i=1}^{N} h_i(\underline{p}).$$

Scalar EXIT functions defined by choosing $\underline{p} = (p, p, \ldots, p)$.

$$\begin{aligned} H(X_i|\underline{Y}) &= \mathbb{P}(Y_i = e)H(X_i|\underline{Y}_{-i}, Y_i = e) + \mathbb{P}(X_i = Y_i)H(X_i|\underline{Y}_{-i}, Y_i = X_i) \\ &= \mathbb{P}(Y_i = e)H(X_i|\underline{Y}_{-i}). \end{aligned}$$

Therefore, $P_{b,i}(p) = ph_i(p)$ and $P_b(p) = ph(p)$ (3)

Preliminaries

More definitions

Definition 2 - Consider a code $\mathcal{C}$ and the *indirect recovery* of X_i from the subvector $\underline{Y}_{-i}$ (i.e., the bit-MAP decoding of Y_i from $\underline{Y}$ when $Y_i = e$). For $i \in [N]$, the set of erasure patterns that prevent indirect recovery of X_i under bit-MAP decoding is given by

$$\Omega_i \triangleq \{A \subseteq [N]\backslash\{i\} : \exists B \subseteq [N]\backslash\{i\}, B \cup \{i\} \in \mathcal{C}, B \subseteq A\}.$$

For distinct $i, j \in [N]$, the set of erasure patterns where the j-th bit is *pivotal* for the indirect recovery of X_i is given by

$$\partial_j \Omega_i \triangleq \{A \subseteq [N]\backslash\{i\} : A\backslash\{j\} \notin \Omega_i, A \cup \{j\} \in \Omega_i\}$$

These are the erasure patterns where X_i can be recovered from $\underline{Y}_{-i}$ iff $Y_j \neq e$.

Proposition 4

For a code $\mathcal{C}$ and transmission over a BEC, we have the following properties for the EXIT functions.

(a) The EXIT function associated with bit i satisfies

$$h_i(p) = \sum_{A \in \Omega_i} p^{|A|}(1-p)^{N-1-|A|}.$$

(b) For $j \in [N] \backslash \{i\}$, the partial derivative satisfies

$$\left. \frac{\partial h_i(\underline{p})}{\partial p_j} \right|_{\underline{p}=(p,p,\ldots,p)} = \sum_{A \in \partial_j \Omega_i} p^{|A|}(1-p)^{N-1-|A|}.$$

(c) The average EXIT function satisfies the *area theorem*

$$\int_0^1 h(p)dp = \frac{K}{N}.$$

Preliminaries

Permutations of linear codes

S_N, the symmetric group on N elements. The permutation group of a code is defined as the subgroup of S_N whose group action on the bit ordering preserves the set of codewords.

Definition 5 - The permutation group $\mathcal{G}$ of a code $\mathcal{C}$ is defined to be

$$\mathcal{G} = \{\pi \in S_N : \pi(A) \in \mathcal{C} \text{ for all } A \in \mathcal{C}\}.$$

Definition 6 - Suppose $\mathcal{G}$ is a permutation group. Then,

(a) $\mathcal{G}$ is *transitive* if, for any $i, j \in [N]$, there exists a permutation $\pi \in \mathcal{G}$ such that $\pi(i) = j$, and

(b) $\mathcal{G}$ is *doubly transitive* if, for any distinct $i, j, k \in [N]$, there exists a $\pi \in \mathcal{G}$ such that $\pi(i) = i$ and $\pi(j) = k$.

Proposition 7

Suppose the permutation group $\mathcal{G}$ of a code $\mathcal{C}$ is transitive. Then, for any $i \in [N]$,

$$h(p) = h_i(p) \text{ for } 0 \leq p \leq 1.$$

Proposition 8

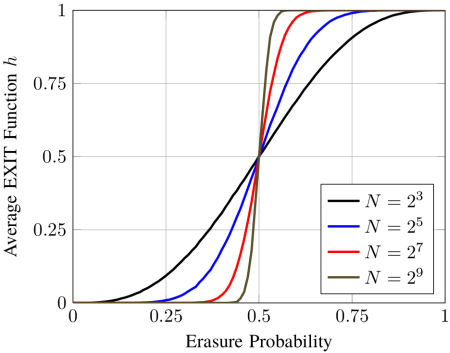
Suppose the permutation group $\mathcal{G}$ of a code $\mathcal{C}$ is doubly transitive. Then, for distinct $i, j, k \in [N]$, and any $0 \leq p \leq 1$,

$$\left.\frac{\partial h_i(\underline{p})}{\partial p'_j}\right|_{\underline{p}=(p,p,\ldots,p)} = \left.\frac{\partial h_i(\underline{p})}{\partial p'_k}\right|_{\underline{p}=(p,p,\ldots,p)}.$$

Capacity achieving codes and the EXIT function

Definition : Suppose $\{\mathcal{C}_n\}$ is a sequence of codes with rates $\{r_n\}$ where $r_n \to r$ for $r \in (0,1)$. $\{\mathcal{C}_n\}$ is said to be capacity achieving on the BEC under bit-MAP decoding, if for any $p \in [0, 1-r)$, the average bit-erasure probabilities satisfy

$$\lim_{n\to\infty} P_b^{(n)}(p) = 0.$$



Proposition 10

Let $\{\mathcal{C}_n\}$ be a seq. of codes with rates $\{r_n\}$, $r_n \to r$ for $r \in (0,1)$. TFAE -

S1: $\{\mathcal{C}_n\}$ is capacity achieving on the BEC under bit-MAP decoding.

S2: The sequence of average EXIT functions satisfies

$$\lim_{n\to\infty} h^{(n)}(p) = \begin{cases} 0 \text{ if } 0 \le p < 1-r \\ 1 \text{ if } 1-r < p \le 1. \end{cases}$$

S3: For any $0 < \epsilon \le 1/2$,

$$\lim_{n\to\infty} p_{1-\epsilon}^{(n)} - p_{\epsilon}^{(n)} = 0.$$

Proof:

- S2 $\Rightarrow$ S1 : $P_b(p) = ph(p)$.
- S1 $\Rightarrow$ S2 : $P_b(p) = ph(p)$ and *Area Theorem* (Proposition 4).
- S2 $\Rightarrow$ S3 : $p_{1-\epsilon}^{(n)} - p_{\epsilon}^{(n)} \sim h^{(n)}$ transitions from ϵ to $1-\epsilon$.
- S3 $\Rightarrow$ S2 : Suffices to show, $\lim_{n\to\infty} p_{\epsilon}^{(n)} = \lim_{n\to\infty} p_{1-\epsilon}^{(n)} = 1 - r$.
  Use Area Theorem.

More definitions

Define

$$[\phi_i(A)] = \begin{cases} \mathbf{1}_A(l) \text{ if } l < i \\ \mathbf{1}_A(l+1) \text{ if } l \geq i. \end{cases}$$

Now define

$$\begin{aligned} \Omega_i' &\triangleq \{\phi_i(A) \in \{0,1\}^{N-1} : A \in \Omega_i\} \\ \partial_j \Omega_i' &\triangleq \{\phi_i(A) \in \{0,1\}^{N-1} : A \in \partial_j \Omega_i\}. \end{aligned} \tag{8}$$

Consider the space $\{0,1\}^M$ with a measure μ_p such that

$$\mu_p(\Omega) = \sum_{\underline{x} \in \Omega} p^{|\underline{x}|}(1-p)^{M-|\underline{x}|}, \text{ for } \Omega \subseteq \{0,1\}^M,$$

where the weight $|\underline{x}| = x_1 + x_2 + \ldots + x_M$ is the number of 1's in $\underline{x}$.
Using proposition 4, $h_i(p) = \mu_p(\Omega_i')$ with $M = N - 1$.

Invoking something we learnt..

Theorem 16

Let Ω be a monotone set and suppose that, for all $0 \leq p \leq 1$, the influences of all bits are equal $I_1^{(p)}(\Omega) = \ldots = I_M^{(p)}(\Omega)$. Then, for any $0 < \epsilon \leq 1/2$,

$$p_{1-\epsilon} - p_\epsilon \leq \frac{2 \log \frac{1-\epsilon}{\epsilon}}{C \log(N-1)},$$

where $p_t = \inf\{p \in [0,1] : \mu_p(\Omega) \geq t\}$ is well defined because $\mu_p(\Omega)$ is strictly increasing in p with $\mu_0(\Omega) = 0$ and $\mu_1(\Omega) = 1$.

Proof: Using Russo's lemma.

... and finally

Wake up folks! It's the main result :)

Theorem 17

Let $\{\mathcal{C}_n\}$ be a sequence of codes where the blocklengths satisfy $N_n \to \infty$, the rates satisfy $r_n \to r$, and the permutation group $\mathcal{G}(n)$ (of $\mathcal{C}_n$) is doubly transitive for each n. If $r \in (0,1)$, then $\{\mathcal{C}_n\}$ is capacity achieving on the BEC under bit-MAP decoding.

Proof:

Let the average EXIT function of $\mathcal{C}_n$ be $h^{(n)}$. Fix some $i \in [N]$. Since $\mathcal{G}$ is transitive, from Proposition 7,

$$h(p) = h_i(p) \text{ for all } p \in [0,1].$$

Consider the sets Ω_i' from Definition 2 and Equation (8), and let $M = N - 1$.

Proof of Theorem 17 (contd.)

Observe that, from Proposition 4,

$$h_i(p) = \mu_p(\Omega'_i), \qquad I_j^p(\Omega'_i) = \left.\frac{\partial h_i(\underline{p})}{\partial p'_j}\right|_{\underline{p}=(p,p,\ldots,p)}$$

where j' is given by

$$j' = \begin{cases} j \text{ if } j < i \\ j+1 \text{ if } j \geq i. \end{cases}$$

Since $\mathcal{G}$ is doubly transitive, from Proposition 8,

$$I_j^p(\Omega'_i) = I_k^p(\Omega'_i) \text{ for all } j, k \in [N-1].$$

Proof of Theorem 17 (contd.)

Using Theorem 16, we have

$$p_{1-\epsilon} - p_{\epsilon} \leq \frac{2\log\frac{1-\epsilon}{\epsilon}}{C\log(N-1)},$$

where p_t is the functional inverse of h as in Theorem 16. Since $N \to \infty$ from the hypothesis,

$$\lim_{n\to\infty}(p_{1-\epsilon} - p_{\epsilon}) = 0.$$

Now, using Proposition 10, $\{\mathcal{C}_n\}$ is capacity achieving on the BEC under bit-MAP decoding.

□

References

(1) S. Kumar and H. D. Pfister, Reed-Muller codes achieve capacity on erasure channels, 2015, [Online]. Available: http://arxiv.org/abs/1505.05123v2.

(2) S. Kudekar, M. Mondelli, E. Şaşŏglu, and R. Urbanke, Reed-Muller codes achieve capacity on the binary erasure channel under MAP decoding, 2015, [Online]. Available: http://arxiv.org/abs/1505.05831v1.

(3) $\equiv$ (1) $\cup$ (2) S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşŏglu, and R. Urbanke, Reed-Muller codes achieve capacity on erasure channels, 2016, [Online]. Available: http://arxiv.org/abs/1601.04689v1.


What people think about during your conference talk
Hee hee! Animated arrows!
Typo on slide 14, line 3, centre-left. Noted.
Hey! That's what I'm working on!
(RANDOM HAPPY THOUGHTS)
I'm up next I'm up next I'm up next
I'm in the wrong session.
©The Upturned Microscope

Thank You!