Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels

Erdal Arikan

presented by Tomáš Gavenčiak

Binary channels

Binary input channel W: Input alphabet $\mathcal{X} = \{0, 1\}$, output alphabet $\mathcal{Y}$ arbitrary. Given known transition probabilities $W(y \in \mathcal{Y}|x \in \mathcal{X})$.

Symmetric channel (BSC) has a permutation ϖ on $\mathcal{Y}$ such that $\varpi = \varpi^{-1}$ and $W(y|0) = W(\varpi(y)|1)$ for all y. An **erasure channel** (BEC) is a code such that either $W(y|0)W(y|1) = 0$ or $W(y|0) = W(y|1)$ (y is then an erasure symbol).

Symmetric capacity and Bhattacharyya coefficient.

$$I(W) = I(Y; X) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \frac{1}{2} W(y|x) \log \frac{2W(y|x)}{W(y|1) + W(y|0)}$$

$$Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$$

Proposition 1. For any channel W: $1 - \log(1 + Z(W)) \leq I(W) \leq \sqrt{1 - Z(W)^2}$

Polarization

Channel combining. Let $W_N(y_1^N|u_1^N) = W^N(y_1^N|G_N x_1^N)$ be a channel $\mathcal{X}^N \to \mathcal{Y}^N$ where $G_N = B_N F^{\otimes N}$ and with B_N bit-reversal permutation.

Channel splitting. Let $W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \sum_{u_{i+1}^N} 2^{1-N} W_N(y_1^N, u_1^N)$, considering it as a channel $\mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{i-1}$.

Single-step transformation of two copies of channel $W : \mathcal{X} \to \mathcal{Y}$ to channels $W' : \mathcal{X} \to \mathcal{Y}'$ and $W'' : \mathcal{X} \to \mathcal{Y}' \times \mathcal{X}$ as $(W, W) \to (W', W'')$:

$$W'((y_1, y_2)|u_1) = \sum_{u_2'} 1/2 W(y_1|u_1 + u_2')W(y_2|u_2')$$

$$W''((y_1, y_2), u_1|u_2) = 1/2 W(y_1|u_1 + u_2)W(y_2|u_2)$$

PROPOSITION 4. For $(W, W) \to (W', W'')$ we have $I(W') + I(W'') = 2I(W)$ and $I(W') \leq I(W'')$.

PROPOSITION 5. For $(W, W) \to (W', W'')$ we have $Z(W'') = Z(W)^2$, $Z(W') \leq 2Z(W) - Z(W)^2$.

Decoding. Let $h_i(y_1^N, u_1^{i-1}) = \text{argmax}_{u_i \in \mathcal{X}} W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)$ be the estimate for u_i with u_1^{i-1} already decoded.

G_N-coset code with parameters (N, K, A, u_{A^c}) where $A \subseteq \{1, \ldots N\}$ and $|A| = K$ is encoded as $x_1^N = (u_A + u_{A^c})G_N$.

Code performance $P_e(N, K, A, u_{A^c})$ is the probability of decoding error. $P_e(N, K, A) = \mathbb{E}_{u_{A^c}} P_e(N, K, A, u_{A^c})$.

PROPOSITION 2. For any N, K, A, we have $P_e(N, K, A) \leq \sum_{i \in A} Z(W_N^{(i)})$

Polar code has A chosen to include the indices i with largest $Z(W_N^{(i)})$. ($I(W_N^{(i)})$ would also work.) Let $P_e(N, R) = P_e(N, \lfloor RN \rfloor, A)$ with A chosen as above and $|A| = \lfloor RN \rfloor$.

Analysis

THEOREM 1. For fixed W and $\delta \in (0, 1)$, as $N = 2^k$ goes to infinity, the fraction of indices i with $I(W_N^{(i)}) \geq 1 - \delta$ goes to $I(W)$ and the fraction of indices i with $I(W_N^{(i)}) \leq \delta$ goes to $1 - I(W)$.

THEOREM 2. For any $0 < R < I(W)$ there is a sequence of subsets $A_N \subseteq \{1, \ldots N\}$ for $N = 2^k$ going to infinity with $|A_N| \geq NR$ and $Z(W_N^{(i)}) = O(N^{-5/4})$ for all $i \in A_N$.

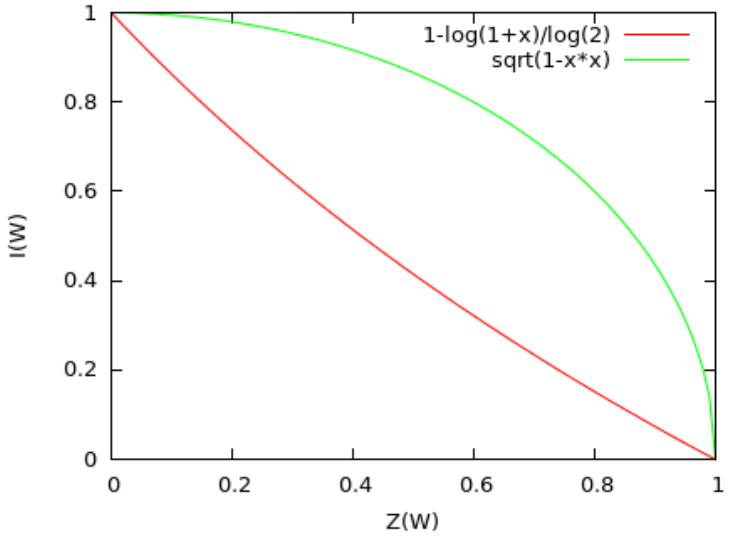
PROPOSITION 18. [IMPROVED T2] For any $0 < R < I(W)$ and any $\beta < 1/2$ there is a sequence of subsets $A_N \subseteq \{1, \ldots N\}$ for $N = 2^k$ going to infinity with $|A_N| \geq NR$ and $\sum_{i \in A_N} Z(W_N^{(i)}) = o(2^{-N^\beta})$.

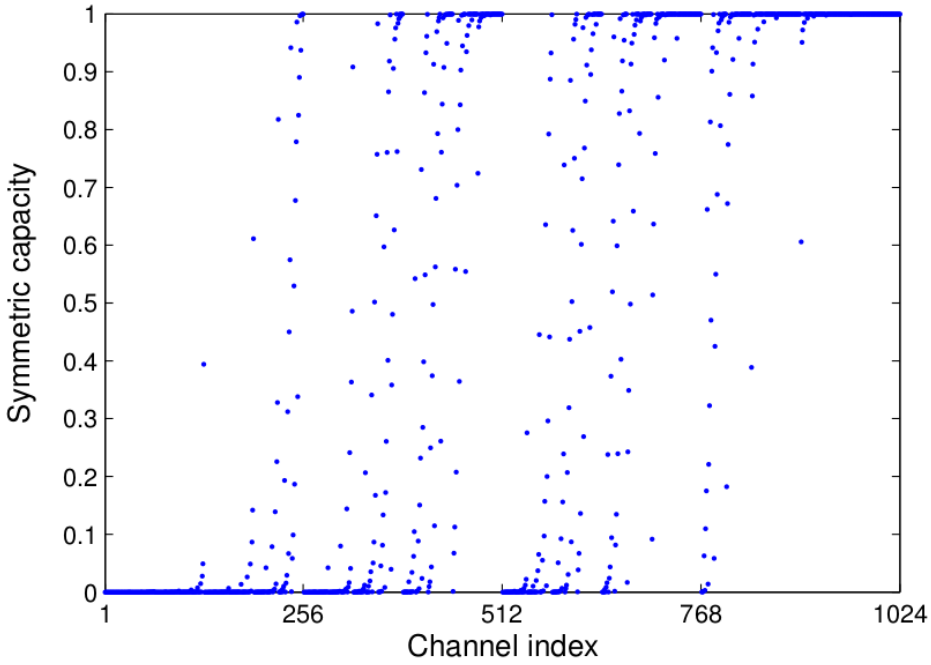
THEOREM 3. For any $R < I(W)$ we have $P_e(N, R) = O(N^{-1/4})$.

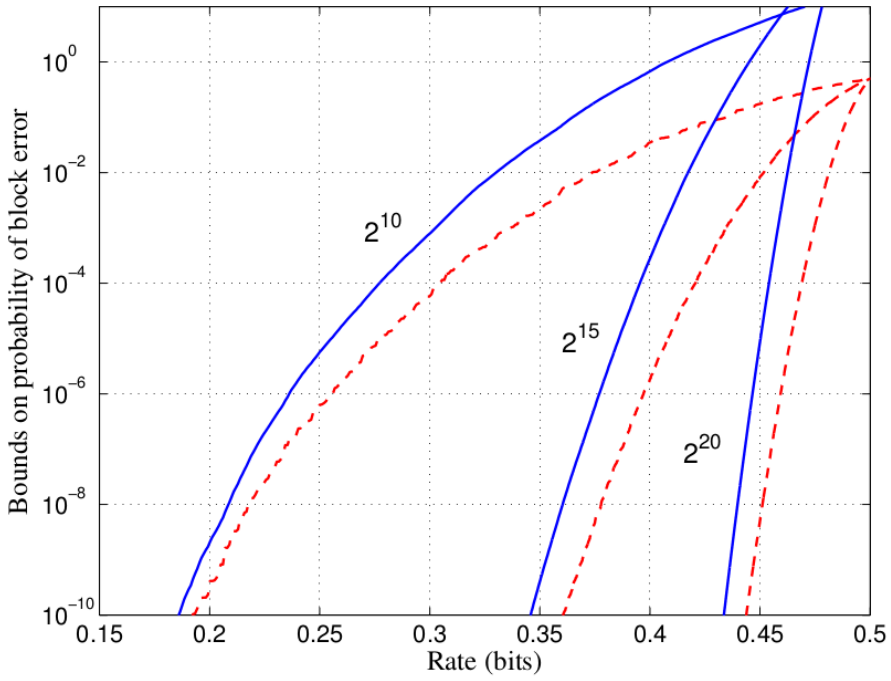
PROPOSITION 19. [IMPROVED T3] For any $R < I(W)$ and $\beta < 1/2$ we have $P_e(N, R) = o(2^{-N^\beta})$.

THEOREM 4. For a symmetric channel W and any $R < I(W)$ we have $P_e(N, K, A, u_{A^c}) = O(N^{-1/4})$ with any u_{A^c}.

THEOREM 5. The complexity of encoding and decoding of a given polar code is $O(N \log N)$.


1-log(1+x)/log(2)
sqrt(1-x*x)
I(W)
Z(W)
0
0.2
0.4
0.6
0.8
1


Symmetric capacity
Channel index
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
1
256
512
768
1024


Bounds on probability of block error
Rate (bits)
10^{0}
10^{-2}
10^{-4}
10^{-6}
10^{-8}
10^{-10}
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
2^{10}
2^{15}
2^{20}