Polar codes – a new paradigm in communication

Alexander Barg

Dept of ECE/Inst. for Systems Research University of Maryland, College Park, MD 20742

Dec. 12, 2012



- Introduction: Transmission over channels
- Binary Polar Codes
- Nonbinary Polar Codes
- Improved decoding: Approaching optimal performance



 $\mathcal X$ - finite set, $|\mathcal X| = q$

Entropy

 $\mathcal X$ - finite set, $|\mathcal X| = q$

Elements of \mathcal{X} can be labelled using log q bits

Entropy

 $\mathcal X$ - finite set, $|\mathcal X| = q$

Elements of \mathcal{X} can be labelled using log q bits

Uniform distrubtion $P_X(x) = \frac{1}{q}$ log $q = \log \frac{1}{P_X(x)}$ bits suffice to identify x

Entropy

 \mathcal{X} - finite set, $|\mathcal{X}| = q$

Elements of \mathcal{X} can be labelled using log q bits

Uniform distrubtion $P_X(x) = \frac{1}{q}$ log $q = \log \frac{1}{P_X(x)}$ bits suffice to identify x

Suppose $P_X = (P_X(x), x \in \mathcal{X})$ is a pmf

The expected number of bits is $H(X) = \sum_{x \in \mathcal{X}} P_X(x) \log \frac{1}{P_X(x)}$ H(X) is called Shannon entropy

Let $W : \mathcal{X} \to \mathcal{Y}$ be a stochastic mapping, $|\mathcal{Y}| < \infty$ $W(y|x) = \Pr(Y = y|X = x)$ Conditional entropy (residual uncertainty about *X* given *Y*)

$$H(X|Y) = E_{XY} \log \frac{1}{P_{X|Y}(x|y)}$$

Mutual information I(X; Y) := H(X) - H(X|Y)

Let $W : \mathcal{X} \to \mathcal{Y}$ be a stochastic mapping, $|\mathcal{Y}| < \infty$ $W(y|x) = \Pr(Y = y|X = x)$ Conditional entropy (residual uncertainty about X given Y)

$$H(X|Y) = E_{XY} \log \frac{1}{P_{X|Y}(x|y)}$$

Mutual information I(X; Y) := H(X) - H(X|Y)

Theorem (Shannon '48)

There exists a subset $D \subset \mathcal{X}^n$ such that its images in \mathcal{Y}^n under W can be distinguished with high probability as long as $|D| < 2^{nl(W)}$.

Let $W : \mathcal{X} \to \mathcal{Y}$ be a stochastic mapping, $|\mathcal{Y}| < \infty$ $W(y|x) = \Pr(Y = y|X = x)$ Conditional entropy (residual uncertainty about *X* given *Y*)

$$H(X|Y) = E_{XY} \log \frac{1}{P_{X|Y}(x|y)}$$

Mutual information I(X; Y) := H(X) - H(X|Y)

Theorem (Shannon '48)

There exists a subset $D \subset \mathcal{X}^n$ such that its images in \mathcal{Y}^n under W can be distinguished with high probability as long as $|D| < 2^{nl(W)}$.

$$I(W) = \max_{P_X} I(X; Y)$$
 is called Channel Capacity

Let $W : \mathcal{X} \to \mathcal{Y}$ be a stochastic mapping, $|\mathcal{Y}| < \infty$ $W(y|x) = \Pr(Y = y|X = x)$ Conditional entropy (residual uncertainty about X given Y)

$$H(X|Y) = E_{XY} \log \frac{1}{P_{X|Y}(x|y)}$$

Mutual information $I(X; Y) := H(X) - H(X|Y) = \log q - H(X|Y)$

Theorem (Shannon '48)

There exists a subset $D \subset \mathcal{X}^n$ such that its images in \mathcal{Y}^n under W can be distinguished with high probability as long as $|D| < 2^{nl(X;Y)}$.

 $I(W) = \log q - H(X|Y)$ (uniform) Channel Capacity

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)

$$u_1 \longrightarrow W \longrightarrow y_1$$

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



 $2I(W) = I(U_1 U_2; Y_1 Y_2) = I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 | U_1)$ = I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 U_1)

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



 $2I(W) = I(U_1 U_2; Y_1 Y_2) = I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 | U_1)$ = $I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 U_1)$

$$W^{-}(y_1y_2|u_1) = rac{1}{2}\sum_{u_2=0}^{1}W(y_1|u_1\oplus u_2)W(y_2|u_2)$$

 $W^{+}(y_1y_2, u_1|u_2) = rac{1}{2}W(y_1|u_1\oplus u_2)W(y_2|u_2).$

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



$$2I(W) = I(U_1; Y_1Y_2) + I(U_2; Y_1Y_2, U_1)$$
$$W^{-}(y_1y_2|u_1) = \frac{1}{2} \sum_{u_2=0}^{1} W(y_1|u_1 \oplus u_2) W(y_2|u_2)$$
$$W^{+}(y_1y_2, u_1|u_2) = \frac{1}{2} W(y_1|u_1 \oplus u_2) W(y_2|u_2)$$
$$I(W^{+}) \ge I(W) \ge I(W^{-})$$

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



 $W^{++}, W^{+-}, W^{-+}, W^{--}$

Discrete memoryless channel $W : \mathcal{X} \to \mathcal{Y}$ with capacity I(W)



 $W^{+++}, W^{++-}, \dots, W^{---}$

Binary Polar Codes

Binary polar codes, BEC(0.5)

I(W) = 0.5

Alexander Barg (UMD)

Binary polar codes, BEC(0.5)

$$I(W) = 0.5$$

 $I(W^{-}) = 0.25, I(W^{+}) = 0.75$

Binary polar codes, BEC(0.5)

$$I(W) = 0.5$$

 $I(W^{-}) = 0.25, I(W^{+}) = 0.75$
 $I(W^{--}) = 0.0625, I(W^{-+}) = 0.4375, I(W^{+-}) = 0.5625, I(W^{++}) = 0.9375$

Binary Polar Codes



Binary Polar Codes



Binary Polar Codes



Binary Polar Codes



Binary Polar Codes



Binary Polar Codes



Binary Polar Codes



Binary Polar Codes

Binary polar codes: ordered bits ($N = 2^4$)


















Binary polar codes: ordered bits



Binary polar codes: ordered bits, $N = 2^{15}$



Binary polar codes: ordered bits



Binary Polar Codes

Encoding map

 $C(W_i)$ 0.0039 0.1211 0.1914 0.6836 0.3164 0.8086 0.8789



Alexander Barg (UMD)

0.9961

Binary Polar Codes

| $C(W_i)$ | rank |
|----------|------|
| 0.0039 | 8 |
| 0.1211 | 7 |
| 0.1914 | 6 |
| 0.6836 | 4 |
| 0.3164 | 5 |
| 0.8086 | 3 |
| 0.8789 | 2 |
| 0.9961 | 1 |



Binary Polar Codes

Encoding map

| $C(W_i)$ | rank |
|----------|------|
| 0.0039 | 8 |
| 0.1211 | 7 |
| 0.1914 | 6 |
| 0.6836 | 4 |
| 0.3164 | 5 |
| 0.8086 | 3 |
| 0.8789 | 2 |
| 0.9961 | 1 |



data

Binary Polar Codes

Encoding map

| $C(W_i)$ | rank |
|----------|------|
| 0.0039 | 8 |
| 0.1211 | 7 |
| 0.1914 | 6 |
| 0.6836 | 4 |
| 0.3164 | 5 |
| 0.8086 | 3 |
| 0.8789 | 2 |
| 0.9961 | 1 |



data

data

data

data

data

Binary Polar Codes

| $C(W_i)$ | rank |
|----------|------|
| 0.0039 | 8 |
| 0.1211 | 7 |
| 0.1914 | 6 |
| 0.6836 | 4 |
| 0.3164 | 5 |
| 0.8086 | 3 |
| 0.8789 | 2 |
| 0.9961 | 1 |



Binary Polar Codes

| $C(W_i)$ | rank | |
|----------|------|------|
| 0.0039 | 8 | |
| 0.1211 | 7 | |
| 0.1914 | 6 | |
| 0.6836 | 4 | data |
| 0.3164 | 5 | |
| 0.8086 | 3 | data |
| 0.8789 | 2 | data |
| 0.9961 | 1 | data |



Binary Polar Codes



Binary Polar Codes

Encoding map



У₁

 y_2

У3

У4

У₅

У6

У7

 y_8

w

W

W

W

w

W

W

W

Alexander Barg (UMD)

Binary Polar Codes



Encoding map

 $(u_1, u_2)H_2 = (x_1, x_2)^t$, where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Encoding map

 $(u_1, u_2)H_2 = (x_1, x_2)^t$, where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$$x_1^4 = u_1^4 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$



Encoding map

 $(u_1, u_2)H_2 = (x_1, x_2)^t$, where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.



Generally $x_1^N = u_1^N H_N$, where $H_N = H_2^{\otimes n}$, $N = 2^n$

The set $\{1, \ldots, N\}$ contains NI(W) indices such that $I(W^s) \approx 1$.

Binary polar codes: Convergence

Why this works:

$$I(W^-) + I(W^+) = 2I(W)$$

After *n* steps we obtain 2^n values $\mathcal{I}_n = \{I^b, b \in \{+, -\}^n\}$

Binary polar codes: Convergence

Why this works:

$$I(W^{-}) + I(W^{+}) = 2I(W)$$

After *n* steps we obtain 2^n values $\mathcal{I}_n = \{I^b, b \in \{+, -\}^n\}$

Introduce a uniform distribution on \mathcal{I}_n : $P_n(I^b) = 2^{-n}$ for all *b* Consider the random process $I_n, n \ge 1$.

The sequence I_n forms a bounded martingale: $E(I_{n+1}|\mathcal{F}_n) = I_n$

$$I_n \stackrel{\text{a.s.}}{\to} I_{\infty}$$
$$I_{\infty} \in \{0,1\}, \ EI_{\infty} = I(W)$$

Binary polar codes: Convergence

For any $\epsilon > 0$

$$\lim_{n\to\infty}\frac{|\{b\in\{+,-\}^n:I(W^b)\in(\epsilon,1-\epsilon)\}|}{2^n}=0.$$

Decoding of polar codes

Let $A_N \subset \{1, \dots, N\}$ be the set of bits used to transmit data

Successive cancellation (SC decoding, Arikan '09)

$$\hat{u}_i = \begin{cases} \arg\max_{z \in \{0,1\}} W(y_1^N, \hat{u}_1^{i-1} | z) & \text{if } i \in F_N^c \\ 0 & \text{if } i \in F_N. \end{cases}$$

Decoding of polar codes

Let $A_N \subset \{1, \dots, N\}$ be the set of bits used to transmit data

Successive cancellation (SC decoding, Arikan '09)

$$\hat{u}_i = \begin{cases} \arg\max_{z \in \{0,1\}} W(y_1^N, \hat{u}_1^{i-1} | z) & \text{if } i \in F_N^c \\ 0 & \text{if } i \in F_N. \end{cases}$$

Rate of polarization (Arikan-Telatar '09) The decline rate of BER is given by $O(2^{-\sqrt{N}})$

q-ary polar codes, $q = 2^r$

Arikan's kernel: $(x_1, x_2) = (u_1, u_2)H_2$ where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

q-ary polar codes, $q = 2^r$

Arikan's kernel: $(x_1, x_2) = (u_1, u_2)H_2$ where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$$(x_1, x_2, \dots, x_N) = (u_1, u_2, \dots, u_N)(H_2)^{\otimes n}, \quad N = 2^n$$

q-ary polar codes

q-ary polar codes, $q = 2^r$

Arikan's kernel: $(x_1, x_2) = (u_1, u_2)H_2$ where $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$$(x_1, x_2, \dots, x_N) = (u_1, u_2, \dots, u_N)(H_2)^{\otimes n}, \quad N = 2^n$$

$$(x_1, x_2, \dots, x_8) = (u_1, u_2, \dots, u_8) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Polar codes for *q*-ary alphabets, $q = 2^r$

Let W_n be the random channel at step n,

$$Pr(W_n = W^B, B \in \{+, -\}^n) = 2^{-n}$$

 $I_n = I(W_n)$ – symmetric capacity

Theorem

 $I_n \to I_\infty$ a.e., where I_∞ is supported on the set $\{0, 1, \dots, r\}$ and $EI_\infty = I(W)$.

Extremal configurations

The virtual channels converge to one of r + 1 possibilities:

| 1 | 1 | 1 | 1 | 1 |
|---|---|---|-------|---|
| 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 |
| ÷ | | ÷ | | ÷ |
| 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 |

Extremal configurations

Define the channel "for the last k bits":

$$W^{[k]}(y|u) = \frac{1}{2^{r-k}} \sum_{x \in \mathcal{X}: x_{r-k+1}^r = u} W(y|x), \qquad u \in \{0,1\}^k$$

Theorem

For any DMC $W : \mathcal{X} \to \mathcal{Y}$ the channels $W_N^{(i)}$ polarize to one of the r + 1 extremal configurations. Namely, let $V_i = W_N^{(i)}$ and

$$\pi_{k,N} = \frac{|\{i \in [N] : |I(V_i) - k| < \delta \land |I(V_i^{[k]}) - k| < \delta\}|}{N},$$

where $\delta > 0$, then $\lim_{N\to\infty} \pi_{k,N} = P(I_{\infty} = k)$ for all k = 0, 1, ..., r. Consequently

$$\sum_{k=1}^{\prime} k\pi_k \to I(W).$$

Extremal configurations: Example



Extremal configurations: Example



A.B, W. Park, Polar codes for q-ary channels, $q = 2^r$, IEEE Trans, Inform. Theory, in press, arXiv:1107.4965v3 Notes for polar codes: http://www.ece.umd.edu/~abarg/627/polar.pdf

Polar codes are related to classical Reed-Muller codes RM(*m*, *r*) a code of length $N = 2^n$, $k = \sum_{i=0}^r {m \choose i}$ data symbols, distance 2^{m-r}

Polar codes are related to classical Reed-Muller codes RM(*m*, *r*) a code of length $N = 2^n$, $k = \sum_{i=0}^r {m \choose i}$ data symbols, distance 2^{m-r}

Polar codes are related to classical Reed-Muller codes RM(*m*, *r*) a code of length $N = 2^n$, $k = \sum_{i=0}^{r} {m \choose i}$ data symbols, distance 2^{m-r}

RM (0,4)

Polar

| 1000 0000 0000 0000 | 1000 0000 0000 0000 |
|---------------------|---------------------|
| 1100 0000 0000 0000 | 1100 0000 0000 0000 |
| 1010 0000 0000 0000 | 1010 0000 0000 0000 |
| 1111 0000 0000 0000 | 1111 0000 0000 0000 |
| 1000 1000 0000 0000 | 1000 1000 0000 0000 |
| 1100 1100 0000 0000 | 1100 1100 0000 0000 |
| 1010 1010 0000 0000 | 1010 1010 0000 0000 |
| 1111 1111 0000 0000 | 1111 1111 0000 0000 |
| 1000 0000 1000 0000 | 1000 0000 1000 0000 |
| 1100 0000 1100 0000 | 1100 0000 1100 0000 |
| 1010 0000 1010 0000 | 1010 0000 1010 0000 |
| 1111 0000 1111 0000 | 1111 0000 1111 0000 |
| 1000 1000 1000 1000 | 1000 1000 1000 1000 |
| 1100 1100 1100 1100 | 1100 1100 1100 1100 |
| 1010 1010 1010 1010 | 1010 1010 1010 1010 |
| 1111 1111 1111 1111 | 1111 1111 1111 1111 |

Polar codes are related to classical Reed-Muller codes RM(*m*, *r*) a code of length $N = 2^n$, $k = \sum_{i=0}^{r} {m \choose i}$ data symbols, distance 2^{m-r}

RM (1,4)

Polar

| 1000 0000 0000 0000 | 1000 0000 0000 0000 |
|---------------------|---------------------|
| 1100 0000 0000 0000 | 1100 0000 0000 0000 |
| 1010 0000 0000 0000 | 1010 0000 0000 0000 |
| 1111 0000 0000 0000 | 1111 0000 0000 0000 |
| 1000 1000 0000 0000 | 1000 1000 0000 0000 |
| 1100 1100 0000 0000 | 1100 1100 0000 0000 |
| 1010 1010 0000 0000 | 1010 1010 0000 0000 |
| 1111 1111 0000 0000 | 1111 1111 0000 0000 |
| 1000 0000 1000 0000 | 1000 0000 1000 0000 |
| 1100 0000 1100 0000 | 1100 0000 1100 0000 |
| 1010 0000 1010 0000 | 1010 0000 1010 0000 |
| 1111 0000 1111 0000 | 1111 0000 1111 0000 |
| 1000 1000 1000 1000 | 1000 1000 1000 1000 |
| 1100 1100 1100 1100 | 1100 1100 1100 1100 |
| 1010 1010 1010 1010 | 1010 1010 1010 1010 |
| 1111 1111 1111 1111 | 1111 1111 1111 1111 |

Polar codes are related to classical Reed-Muller codes RM(*m*, *r*) a code of length $N = 2^n$, $k = \sum_{i=0}^{r} {m \choose i}$ data symbols, distance 2^{m-r}

Polar

RM (2,4)

| 1000 0000 0000 0000 | 1000 0000 0000 0000 |
|---------------------|---------------------|
| 1100 0000 0000 0000 | 1100 0000 0000 0000 |
| 1010 0000 0000 0000 | 1010 0000 0000 0000 |
| 1111 0000 0000 0000 | 1111 0000 0000 0000 |
| 1000 1000 0000 0000 | 1000 1000 0000 0000 |
| 1100 1100 0000 0000 | 1100 1100 0000 0000 |
| 1010 1010 0000 0000 | 1010 1010 0000 0000 |
| 1111 1111 0000 0000 | 1111 1111 0000 0000 |
| 1000 0000 1000 0000 | 1000 0000 1000 0000 |
| 1100 0000 1100 0000 | 1100 0000 1100 0000 |
| 1010 0000 1010 0000 | 1010 0000 1010 0000 |
| 1111 0000 1111 0000 | 1111 0000 1111 0000 |
| 1000 1000 1000 1000 | 1000 1000 1000 1000 |
| 1100 1100 1100 1100 | 1100 1100 1100 1100 |
| 1010 1010 1010 1010 | 1010 1010 1010 1010 |
| | |

Decoding of polar codes and RM codes

Goal: Fill the void for moderate block length: $200 \le N \le 2000$

Decoding of polar codes and RM codes

Goal: Fill the void for moderate block length: $200 \le N \le 2000$

Problem: Relatively slow convergence

Decoding of polar codes and RM codes

Goal: Fill the void for moderate block length: $200 \le N \le 2000$

Problem: Relatively slow convergence

Enhancements of Decoding Algorithms: List decoding Gradient-like decoding Easier logic by quantizing SC decoding

A.B. and I. Dumer (UC Riverside), work in progress

I. Dumer, papers on decoding RM codes, *IEEE Transactions on Information Theory*, 2006,2008.
List decoding of polar codes

SC decoding:

$$\hat{u}_{i} = (\arg\max_{z \in \{0,1\}} W(y_{1}^{N}, \hat{u}_{1}^{i-1} | z)) \cdot I_{\{i \in F_{N}^{c}\}}$$

List decoding of polar codes

SC decoding:

$$\hat{u}_i = (\arg \max_{z \in \{0,1\}} W(y_1^N, \hat{u}_1^{i-1}|z)) \cdot I_{\{i \in F_N^c\}}$$

Keep $L = 2^s$ most probable bit sequences (i_1, \ldots, i_s) , start pruning the list after that.

List decoding of polar codes



List decoding of polar codes



List decoding of polar codes



List decoding of polar codes



List decoding of polar codes

List decoding with CRC achieves state-of-the-art performance

Quantization

Let
$$\rho_i(W) \triangleq L_N^i(y_1^N, \hat{u}_1^{i-1}) = \log \frac{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^{(i)}(y_1^N, \hat{u}_1^{i-1}|1)}$$

Recurstion step:

$$\rho(\boldsymbol{W}^{-}) = \log \frac{\boldsymbol{e}^{\rho' + \rho''} + 1}{\boldsymbol{e}^{\rho'} + \boldsymbol{e}^{\rho''}}, \quad \rho(\boldsymbol{W}^{+}) = \rho' + \boldsymbol{x} \cdot \rho''$$

where *x* is the value of the decoded symbol.

Table-based approximation with only small loss of accuracy

Quantization



Gradient-like decoder



Gradient-like decoder

