Non-Binary Polar Codes using Reed-Solomon Codes and Algebraic Geometry Codes

Ryuhei Mori Toshiyuki Tanaka

Graduate School of Informatics, Kyoto University

Information Theory Workshop 2010

Contents

- Exponent of matrix
- Reed-Solomon matrix - Our previous work
- Simulation results - This work
- Reed-Solomon matrix and Reed-Muller codes - This work
- Hermitian codes - This work

Exponent of matrix

- G: $\ell \times \ell$ matrix on $\mathbb{F}_q$.
- $P_e(G, n)$: error probability of polar codes of length $\ell^n =: N$ (generator matrix is submatrix of $G^{\otimes n}$).

When rate of polar codes is smaller than capacity, for any $\epsilon > 0$

$$N^{E(G)-\epsilon} \leq -\log P_e(G, n) \leq N^{E(G)+\epsilon}$$

where $E(G) \in [0, 1)$ is

$$E(G) := \frac{1}{\ell} \sum_{i=0}^{\ell-1} \log_\ell D_i$$

D_i: partial distance

[Korada, Şaşoğlu, and Urbanke 2009]
[Arıkan and Telatar 2008]

Partial distance

$$E(G) := \frac{1}{\ell} \sum_{i=0}^{\ell-1} \log_\ell D_i$$

D_i: partial distance

$$\begin{aligned} D_i &:= d(g_i, \langle g_{i+1}, \dots, g_{\ell-1} \rangle) \qquad \text{for } 0 \le i \le \ell - 2 \\ D_{\ell-1} &:= d(g_{\ell-1}, 0) \end{aligned}$$

- g_i: ith row of G
- $\langle g_{i+1}, \dots, g_{\ell-1} \rangle$: a linear space spanned by $g_{i+1}, \dots, g_{\ell-1}$
- $d(\cdot, \cdot)$: Hamming distance

$$\begin{matrix} D_0 = 1 \\ D_1 = 1 \\ D_2 = 3 \end{matrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad \begin{matrix} D_0 = 1 \\ D_1 = 2 \\ D_2 = 2 \end{matrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$D_0 D_1 D_2 = 3, \qquad D_0 D_1 D_2 = 4$$

Intuitive explanation

$D(G, n)$: a minimum distance of polar codes constructed from $G^{\otimes n}$

$P_e(G, n) \geq 2^{-aD(G,n)}$ for some constant $a > 0$

$$N^{E(G)-\epsilon} \leq -\log P_e(G, n) \leq N^{E(G)+\epsilon}$$

$$N^{E(G)-\epsilon} \leq D(G, n) \leq N^{E(G)+\epsilon}$$

where $E(G) \in [0, 1)$ is

$$E(G) := \frac{1}{\ell} \sum_{i=0}^{\ell-1} \log_\ell D_i$$

Matrix transform

$$G = \begin{bmatrix} g_0 \\ \vdots \\ g_{\ell-1} \end{bmatrix} \implies G' = \begin{bmatrix} g_0 \\ \vdots \\ g_{i-1} \\ g_i + g_j \\ g_{i+1} \\ \vdots \\ g_j \\ \vdots \\ g_{\ell-1} \end{bmatrix}, \qquad \text{for } j > i$$

The performance of SC decoder for polar codes is invariant under this transform

Without loss of generality, we can assume $D_i =$ weight of ith row of G

Minimum distance of polar codes

- G: $\ell \times \ell$ matrix on $\mathbb{F}_q$
- D_i: weight of ith row of G
- $D_{i_1,i_2,\ldots,i_n}$: weight of ith row of $G^{\otimes n}$ where ℓ-ary expansion of i is $i_1 \ldots i_n$

$$D_{i_1,i_2,\ldots,i_n} = D_{i_1} D_{i_2} \cdots D_{i_n}$$

From the law of large numbers, one has to choose an index i where number of $a \in \{0, \ldots, \ell - 1\}$ in $i_1 \ldots i_n$ is about n/ℓ

Hence, one has to choose an index i such that

$$\begin{aligned} D_{i_1,i_2,\ldots,i_n} &\approx \left(\prod_{i=0}^{\ell-1} D_i \right)^{\frac{n}{\ell}} \\ &= \exp\left\{ n \frac{1}{\ell} \sum_{i=0}^{\ell-1} \log D_i \right\} = N^{E(G)} \end{aligned}$$

Contents

- Exponent of matrix
- Reed-Solomon matrix - Our previous work
- Simulation results - This work
- Reed-Solomon matrix and Reed-Muller codes - This work
- Hermitian codes - This work

Matrix with large exponent

If G doesn't satisfy

$$D_0 \leq D_2 \leq \cdots \leq D_{\ell-1} \tag{1}$$

there is a matrix G' which is obtained by permutation of rows of G such that $E(G') \geq E(G)$ and G' satisfies (1)
[Korada, Şaşoğlu, and Urbanke 2009]

If (1) is satisfied, $D_i =$ minimum distance of $\langle g_i, \dots, g_{\ell-1} \rangle$.

Hence, obtaining large $E(G)$ is equivalent to obtaining a sequence of linear codes $\mathcal{C}_1, \dots, \mathcal{C}_\ell$ which satisfies

- $\mathcal{C}_i$: a linear code of dimension i and length ℓ
- minimum distance of $\mathcal{C}_i$ is large for $i \in \{1, \dots, \ell\}$
- $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_\ell$

Reed-Solomon codes have these properties.

Reed-Solomon matrix

Let α be a primitive element of $\mathbb{F}_q$.
A Reed-Solomon matrix $G_{\mathrm{RS}}(q)$ is defined as

$$
\begin{array}{c c}
 & \begin{array}{cccccc} \alpha^{q-2} & \alpha^{q-3} & \cdots & \alpha & 1 & 0 \end{array} \\
\begin{array}{c} X^{q-1} \\ X^{q-2} \\ X^{q-3} \\ \vdots \\ X \\ 1 \end{array} &
\begin{bmatrix}
1 & 1 & \cdots & 1 & 1 & 0 \\
\alpha^{(q-2)(q-2)} & \alpha^{(q-3)(q-2)} & \cdots & \alpha^{q-2} & 1 & 0 \\
\alpha^{(q-2)(q-3)} & \alpha^{(q-3)(q-3)} & \cdots & \alpha^{q-3} & 1 & 0 \\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
\alpha^{q-2} & \alpha^{q-3} & \cdots & \alpha & 1 & 0 \\
1 & 1 & \cdots & 1 & 1 & 1
\end{bmatrix}
\end{array}.
$$

Submatrix which consists of ith row to the last row is a generator matrix of extended Reed-Solomon code.
The size ℓ of RS matrix is q.
Since $G_{\mathrm{RS}}(2) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, RS matrix can be regarded as a generalization of Arıkan's binary matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Since $D_i = i + 1$, $E(G_{\mathrm{RS}}(q)) = \frac{\log(q!)}{q \log q}$

Exponent of Reed-Solomon matrix

$$E(G_{\mathrm{RS}}(q)) = \frac{\log(q!)}{q \log q}$$

q	2	4	16	64	256
$E(G_{\mathrm{RS}}(q))$	0.5	0.573120	0.691408	0.770821	0.822264

$$\lim_{q \to \infty} E(G_{\mathrm{RS}}(q)) = 1$$

The exponent of binary matrix of size smaller than 32 is smaller than 0.55 [Korada, Şaşoğlu, and Urbanke 2009]

Reed-Solomon matrix is useful for obtaining large exponent !

How about the performance for finite blocklength ?

Contents

- Exponent of matrix
- Reed-Solomon matrix - Our previous work
- Simulation results - This work
- Reed-Solomon matrix and Reed-Muller codes - This work
- Hermitian codes - This work

Simulation

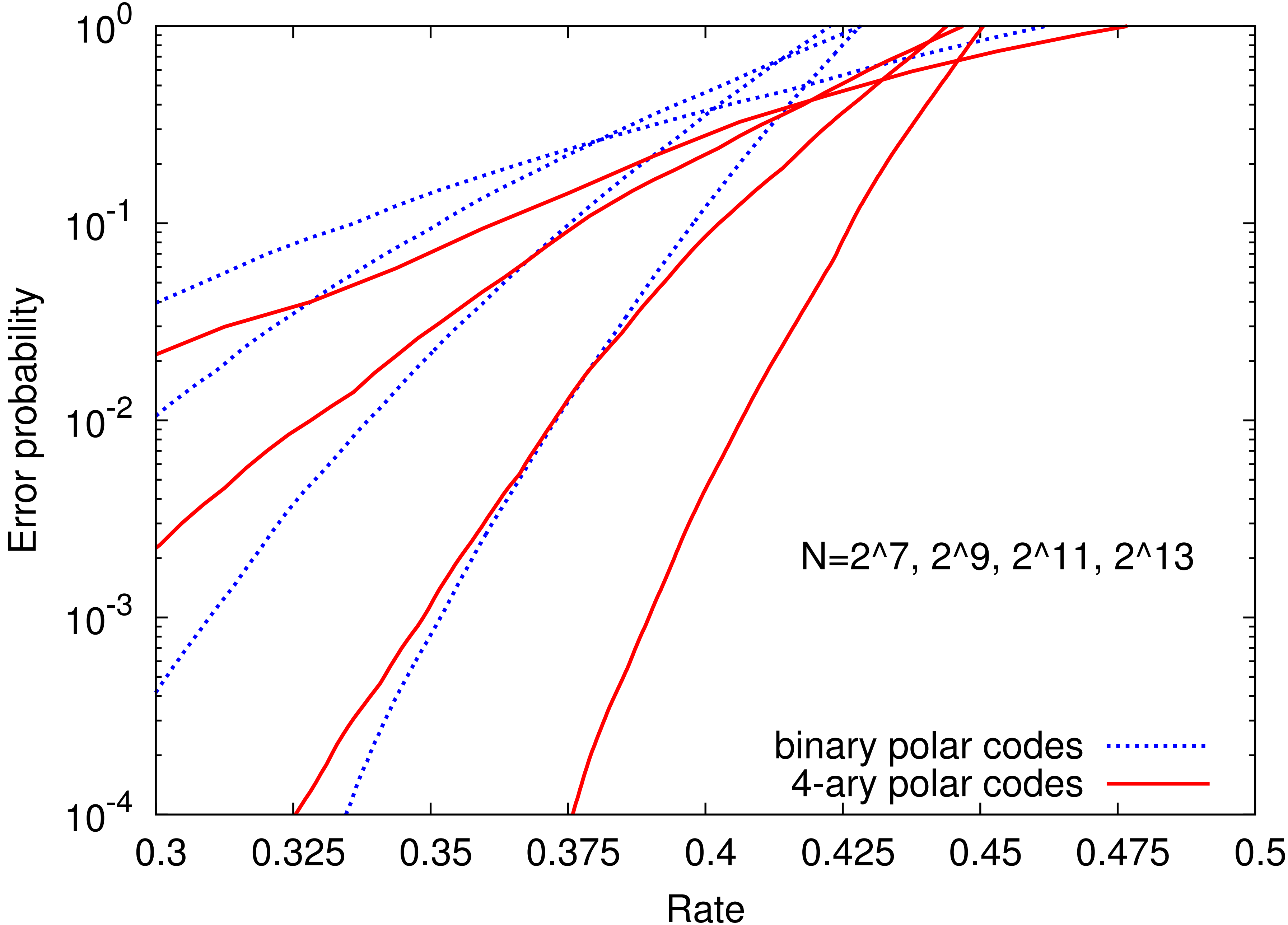
$$\text{Error probability of polar codes} \leq \sum_{i \in \mathcal{F}^c} P_e(W_N^{(i)})$$

Binary polar codes using $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ vs 4-ary polar codes using $G_{\mathrm{RS}}(4)$

Same blocklength as binary codes 2^7, 2^9, 2^{11}, and 2^{13}

AWGN($\sigma = 0.97865$)
Capacity is about 0.5

Simulation result



Contents

Polar codes and Reed-Muller codes: binary case

[Arıkan 2009]

$$X : \; 1 \quad 0 \qquad\qquad (X_2, X_1) : (1,1)(1,0)(0,1)(0,0)$$

$$\begin{array}{cc} X & \\ 1 & \end{array} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \begin{array}{r} X_2X_1 \\ X_2 \\ X_1 \\ 1 \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array}$$

Polar rule: $\{i \in \{0, \ldots, 2^n - 1\} \mid P_e(W^{(i_1)\cdots(i_n)}) < \epsilon\}$
Reed-Muller rule: $\{i \in \{0, \ldots, 2^n - 1\} \mid i_1 + \cdots + i_n > k\}$

Binary polar codes using $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and binary Reed-Muller codes are similar.

Reed-Muller rule maximizes the minimum distance.

Polar codes using RS matrix and Reed-Muller codes: q-ary case

$$
\begin{array}{c|c|c}
(X_2, X_1): & \begin{array}{ccccccccc} (2,2) & (2,1) & (2,0) & (1,2) & (1,1) & (1,0) & (0,2) & (0,1) & (0,0) \end{array} & \\
\begin{array}{c} X_2^2X_1^2 \\ X_2^2X_1 \\ X_2^2 \\ X_2X_1^2 \\ X_2X_1 \\ X_2 \\ X_1^2 \\ X_1 \\ 1 \end{array} &
\begin{bmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
2 & 1 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
2 & 2 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix} &
\begin{array}{c} 00 \\ 01 \\ 02 \\ 10 \\ 11 \\ 12 \\ 20 \\ 21 \\ 22 \end{array}
\end{array}
$$

Polar rule: $\{i \in \{0, \dots, q^n - 1\} \mid P_e(W^{(i_1)\cdots(i_n)}) < \epsilon\}$

Reed-Muller rule: $\{i \in \{0, \dots, q^n - 1\} \mid i_1 + \cdots + i_n > k\}$

Q-ary polar codes using $G_{\mathrm{RS}}(q)$ and q-ary Reed-Muller codes are also similar.

Hyperbolic rule: $\{i \in \{0, \dots, q^n - 1\} \mid (i_1 + 1) \cdots (i_n + 1) > k\}$

Hyperbolic rule maximizes the minimum distance

(Massey-Costello-Justesen codes, hyperbolic cascaded RS codes).

Contents

- Exponent of matrix
- Reed-Solomon matrix - Our previous work
- Simulation results - This work
- Reed-Solomon matrix and Reed-Muller codes - This work
- Hermitian codes - This work

Hermitian codes

$\mathcal{C}_i$: a linear code of dimension i and length ℓ

- minimum distance of $\mathcal{C}_i$ is large for $i \in \{1, \dots, \ell\}$
- $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_\ell$

Some class of algebraic geometry codes have the nested structure.

$G_{\mathrm{H}}(q)$: matrix using q-ary Hermitian codes

q (even power of a prime)	4	16	64	256
$E(G_{\mathrm{RS}}(q))$	0.573120	0.691408	0.770821	0.822264
$E(G_{\mathrm{H}}(q))$	0.562161	0.707337	0.802760	0.859299
$q^{3/2}$ = size of $G_{\mathrm{H}}(q)$	8	64	512	4096

In order to obtain large exponent on fixed q, algebraic geometry codes are useful.

Conclusion

Conclusion

- Reed-Solomon matrix has large exponent (previous work)
- 4-ary polar codes using Reed-Solomon matrix has better performance than binary polar codes using $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ for finite blocklength
- Polar codes using Reed-Solomon matrix, Reed-Muller codes, and Massey-Costello-Justesen/hyperbolic cascaded RS codes are similar (generator matrices are constructed from $G_{\mathrm{RS}}(q)^{\otimes n}$)
- Matrices using Hermitian codes have larger exponent than RS matrix (unless $q = 4$). But size of the matrices are large.

Future works

- Other heuristic decoding for q-ary polar codes using Reed-Solomon matrix e.g., symbolwise/bitwise belief propagation.