On Fast Threefold Polarizations of Binary Discrete Memoryless Channels

Chengrong Huang, Ying Guo and Clement T. Gyamfi
School of Information Science & Engineering
Central South University
Changsha 410083, China
yingguo@csu.edu.cn

Tae Chul Shin and Moon Ho Lee
Institute of Information and Communication
Chonbuk National University
Chonju 561-756, Korea
moonho@chonbuk.ac.kr

***Abstract*—Motivated by a polarization approach to construct code sequences related to Reed-Muller (RM) codes with generator matrix G_{2^n} of size $2^n \times 2^n$ to increase the cutoff rate, we consider a problem of systematic constructions of polar codes as splitting threefold input binary discrete memoryless channels (B-DMC) for generator matrix G_{3^n}. The polarized channel achieves the symmetric capacity of arbitrary binary-input discrete memoryless channels under a low computation complexity of successive cancellation decoding strategy for any core matrix $\mathcal{O}_3$, which is a submatrix of generator matrix $G_4 = \mathcal{O}_2 \otimes \mathcal{O}_2$. In principle larger matrices G_{3^n} with fast construction algorithms can be used for constructions of polar code sequences that tend to polarize with respect to the rate and reliability under certain fast combining and splitting operations. The proposed polarization code scheme has a salient recursiveness feature and hence can be decoded with a belief propagation (BP) decoder, which renders the scheme analytically tractable and provides a powerful low-complexity coding algorithm.**

Keywords-polar codes; binary discrete memoryless channels; channel coding; fast algorithm.

I. Introduction

The channel polarization may be consisted of code sequences using a belief propagation (BP) decoder with symmetric high rate capacity in given binary-input discrete memoryless channels (B-DMC) [1]. It is a commonplace phenomenon that is almost impossible to avoid as long as several similar channels are combined in a sufficient density with certain elegant connections. The investigation of channel polarization not only has become an interesting theoretical problem, but also have lots of practical applications in signal sequence transforms, data processing, signal processing, and code coding theory [2], [3].

Motivated by a fascinating aspect of Shannon's channel coding theorem that shows the existence of capacity-achieving code sequences [4], we show a novel construction of provably capacity-achieving sequences with low coding complexities with BP decoders. This paper is an attempt to meet this elusive goal for B-DMC, which is an extension of work where channel combining and splitting were used to to improve the sum cutoff rate [1]–[3]. In a recent investigation, the above-mentioned rate has been generalized for different forms of polar-code constructions [5]. However, there is few recursive method suggested there to reach the ultimate limit of such improvements. As the present work progressed, it is shown that polar-code sequences have much in common with Reed-Muller codes [6]. Indeed, recursive code construction and successive cancellation decoding, which are two essential characters of polar coding, appear to be introduced into coding theory. It has a relationship to existing work by noting that polar-code sequences can be made to be multilevel in terms of generator matrices G_{p^n} originating from Plotkin's constructions [7]. Therefore, Polar coding has a strong resemblance to Reed-Muller coding, and hence may be regarded as a generalization of Reed-Muller codes since both coding constructions start with a generator matrix for a rate one code and obtain generator matrices of lower rate codes by expurgating rows of the initial generator matrices. While in this paper, we would like to point out that polar-code sequences that have the same structure as Reed-Muller codes have a sparse factor graph representation and can be fast decoded with BP decoder for superior performance [3], [8].

Since polar-coding, which may be considered as a generalization of Reed-Muller coding, is an approach employed to construct capacity-achieving codes with certain symmetries, we demonstrate the performance advantages of several polar-code sequences under BP decoder with respect to symmetric capacity and Bhattacharyya parameter. The symmetric capacity is the highest rate achievable subject to using the input alphabets of B-DMC with equal probability. Polar-code is the first provably capacity achieving code with low coding complexity [9].

According to construction of polar-code sequences, we consider a generic B-DMC denoted by $W : \mathcal{X} \mapsto \mathcal{Y}$ with input alphabets $\mathcal{X} = \{0, 1\}$, output alphabets $\mathcal{Y}$, and transition probabilities $W(y|x)$ for $x \in \mathcal{X}, y \in \mathcal{Y}$. There are two channel parameters [1], i.e., the symmetric capacity

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

and the Bhattacharyya parameter

$$Z(W) = \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}. \quad (2)$$

 ISBN: 978-1-61208-199-1

The two parameters are much useful as measures of rate and reliability of the B-DMC, i.e., the Shannon capacity $I(W)$ is the highest rate at which reliable communication is possible using the inputs with equal frequency, and $Z(W)$ is an upper bound on the probability of maximum-likelihood (ML) decision error.

Throughout this paper, we use the notation $\mathbf{a}_1^N$ to denote a row vector $(a_1, \cdots, a_N)$. Given such a vector $\mathbf{a}_1^N$, we write $\mathbf{a}_i^j$ to denote the subvector $(a_i, \cdots, a_j)$. Moreover, we write $\mathbf{a}_{\mathcal{A}}$ to denote the subvector $(a_i : i \in \mathcal{A} \subseteq \{1, 2, \cdots, N\})$. We write $\mathbf{a}_{1,o}^j$ to denote the subvector with odd indices $(a_i : 1 \leq i \leq j,\ i \text{ odd })$, and $\mathbf{a}_{1,e}^j$ to denote the subvector with even indices $(a_i : 1 \leq i \leq j,\ i \text{ even })$. Similarly, we write $\mathbf{a}_{1,l}^j$ to denote the subvector with the indices $(a_i : 1 \leq i \leq j,\ i = pk + l)$. We write W^N to denote the channel corresponding to N uses of B-DMC W, and hence, $W^N : \mathcal{X}^N \mapsto \mathcal{Y}^N$ with $W^N(\mathbf{y}_1^N|\mathbf{x}_1^N) = \prod_{i=1}^N W(y_i|x_i)$.

This paper is organized as follows. In Sec.II, generation matrices of polar codes are presented via the channel combining and splitting. In Sec.III, according to the properties of polarization constructions, a decoding algorithm is suggested for the G_N-coset codes. Finally, conclusions are drawn in Sec.III.

II. Polarization Construction

In this section, we derive fast constructions of polar-codes based on Arikan's construction [1]. We begin by giving an explicit algebraic expression of generator matrix G_N of polar-code, which has been defined in a schematic form. The algebraic form of G_N point at an efficient implementation of coding operation $\mathbf{u}_1^N G_N$. In analyzing the coding operation, we exploit its relation to fast transforms in signal processing [9].

We carry out the construction of G_N-coset codes before specializing polar-codes. Recall that individual G_N-coset codes are identified by a parameter vector $(N, K, \mathcal{A}, \mu_{\mathcal{A}^c})$ [1]. In the following analysis, we fix the shorted parameter vector $(N, K, \mathcal{A})$ while keeping free $\mu_{\mathcal{A}^c}$ to take any value over $\mathcal{X}^{N-K}$ as frozen bits. In other words, the analysis of polar-code sequences will be over the ensemble of G_N-coset codes with a fixed parameter vector $(N, K, \mathcal{A})$ based on several families of generator matrices $G_N = \mathcal{O}_3^{\otimes n}$, where $\otimes$ denotes keronecker product, n is a positive integer.

Constructions of polar-code sequences based on generator matrices G_{3^n} are derived from the radix $N = 3^n$ channel polarization, which is an operation by which one manufacture out of N independent copies of a given B-DMC W yields a second set of N channels $\{W_N^i : 1 \leq i \leq N\}$ that show a polarization effect in a sense that, as N becomes large, the symmetric capacity terms $\{I(W_N^i) : 1 \leq i \leq N\}$ tend towards 0 or 1 for all but a vanishing fraction of indices i. This operation consists of a channel combining phase and a channel splitting phase.

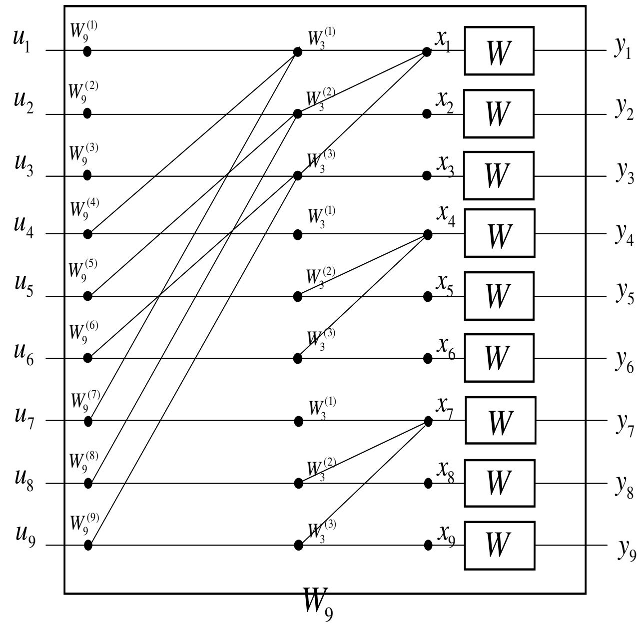

Figure 1. Transformation of $\mathcal{O}_9 = (\mathcal{O}_3 \otimes I_3)(I_3 \otimes \mathcal{O}_3)$.

Taking block length $N = 3^n$, the channel combining based on core matrix $\mathcal{O}_3$ of order 3 includes 3^n copies of a given B-DMC W in a recursive manner to produce a vector channel $W_{3^n}^{(i)}$ for any $1 \leq i \leq 3^n$. In a similar way , the first level of the recursion combines three independent copies of W as shown in Fig. 1 and achieves the combined channel W_3 with the transition probabilities described as

$$W_3(\mathbf{y}_1^3|\mathbf{u}_1^3) = W(y_1|\oplus_{i=1}^3 u_i)W(y_2|u_2)W(y_3|u_3), \qquad (3)$$

where the mapping W_3 is defined as $W_3(\mathbf{y}_1^3|\mathbf{x}_1^3) = W^3(\mathbf{y}_1^3|\mathbf{u}_1^3\mathcal{O}_3)$, where the core matrix

$$\mathcal{O}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

is sub-matrix of $\mathcal{O}_4 = \mathcal{O}_2^{\otimes 2}$, i.e.,

$$\mathcal{O}_4 = \begin{pmatrix} \mathcal{O}_3 & \mathbf{0}_{3\times 1} \\ \mathbf{1}_{1\times 3} & 1 \end{pmatrix},$$

where $\mathbf{1}_{1\times 3} = (1, 1, 1)$ and $\mathbf{0}_{3\times 1} = (0, 0, 0)^T$.

For the second level of the recursion, we combine three independent copies of W_3, as shown in Fig. 2, to generate the channel W_{3^2} with transition probabilities

$$\begin{aligned} W_{3^2}(\mathbf{y}_1^9|\mathbf{u}_1^9) = {} & W_3(y_1^3|\oplus_{i=1}^3 u_i, \oplus_{i=4}^6 u_i, \oplus_{i=7}^9 u_i) \\ & \cdot W_3(y_4^6|u_2, u_5, u_8)W_3(y_7^9|u_3, u_6, u_9). \end{aligned} \qquad (4)$$

Define the permutation operation $B_9 = R_9$, i.e.,

$$B_9(\mathbf{u}_1^9) = (u_1, u_4, u_7, u_2, u_5, u_8, u_3, u_6, u_9). \qquad (5)$$

Therefore, we obtains the mapping $\mathbf{u}_1^9 \to \mathbf{x}_1^9$ from the input of W_9 to the input of W^9 such that $\mathbf{x}_1^9 = \mathbf{u}_1^9 G_9$, where $G_9 = B_9\mathcal{G}_9 = B_9\mathcal{O}_9 = B_9\mathcal{O}_3^{\otimes 2}$.

Generally, we get the extensive form of the recursion while three independent copies of $W_{3^{n-1}}$ are combined to produce the channel W_{3^n}. The input vector $\mathbf{u}_1^{3^n}$ is transformed to $\mathbf{s}_1^{3^n}$ such that

$$s_{3i-2} = \oplus_{j=0}^{2} u_{3i-j}, \quad s_{3i-1} = u_{3i-1}, \quad s_{3i} = u_{3i}$$

for $1 \le i \le 3^{n-1}$. The operator R_{3^n} is a permutation operation defined as

$$\begin{aligned} R_{3^n}(\mathbf{u}_1^{3^n}) &= (\mathbf{u}_{1,1}^{3^n}, \mathbf{u}_{1,2}^{3^n}, \mathbf{u}_{1,3}^{3^n}) \\ &= (u_1, \cdots, u_{3^n-2}, u_2, \cdots, u_{3^n-1}, u_3, \cdots, u_{3^n}). \end{aligned}$$

It is obvious that the mapping $\mathbf{u}_1^{3^n} \to \mathbf{x}_1^{3^n}$ from the input of the synthesized channel W_{3^n} to the input of the underlying raw channels W^{3^n} is linear and hence can be represented with a generator matrix G_{3^n} so that $\mathbf{x}_1^{3^n} = \mathbf{u}_1^{3^n} G_{3^n}$. Thus the relation of transition probabilities of W_{3^n} and W^{3^n} are described as $W_{3^n}(\mathbf{y}_1^{3^n}|\mathbf{u}_1^{3^n}) = W^{3^n}(\mathbf{y}_1^{3^n}|\mathbf{u}_1^{3^n} G_{3^n})$, where $\mathbf{y}_1^{3^n} \in \mathcal{Y}^{3^n}$, $\mathbf{u}_1^{3^n} \in \mathcal{X}^{3^n}$, $G_{3^n} = B_{3^n} G_3^{\otimes n}$ and B_{3^n} is a 3^n-order permutation matrix defined by $B_{3^n} = R_{3^n}(I_3 \otimes B_{3^{n-1}})$.

According to the previously defined processing for channel combining and splitting which transforms 3 independent copies of W into $W_3^{(i)}$ for $1 \le i \le 3$, we get the following one-to-one mapping to describe the relation of W and $W_3^{(i)}$ $\Xi_3 : (W, W, W) \mapsto (W_3^{(1)}, W_3^{(2)}, W_3^{(3)})$, where

$$W_3^{(1)}(\mathbf{y}_1^3|u_1) = \sum_{u_2,u_3} \frac{1}{3} W(y_1| \oplus_{i=1}^3 u_i) W(y_2|u_2) W(y_3|u_3)$$

$$W_3^{(2)}(\mathbf{y}_1^3, u_1|u_2) = \sum_{u_3} \frac{1}{3} W(y_1| \oplus_{i=1}^3 u_i) W(y_2|u_2) W(y_3|u_3)$$

$$W_3^{(2)}(\mathbf{y}_1^3, \mathbf{u}_1^2|u_3) = \frac{1}{3} W(y_1| \oplus_{i=1}^3 u_i) W(y_2|u_2) W(y_3|u_3).$$

In a similar way, for $N = 3^n$ we achieve the generalized mapping to establish the relation of $W_N^{(i)}$ and $W_{3N}^{(k)}$ as follows

$$\Xi_{3^i} : (W_N^{(i)}, W_N^{(i)}, W_N^{(i)}) \mapsto (W_{3N}^{(3i-2)}, W_{3N}^{(3i-1)}, W_{3N}^{(3i)}),$$

where

$$\begin{aligned} &W_{3N}^{(3i-2)}(\mathbf{y}_1^{3N}, \mathbf{u}_1^{3i-3}|u_{3i-2}) \\ &\quad = \sum_{u_{3i-1},u_{3i}} \frac{1}{3} W_N^{(i)}(\mathbf{y}_1^N, \oplus_{j=1}^3 \mathbf{u}_{1,j}^{3i-3}| \oplus_{j=0}^2 u_{3i-j}) \\ &\quad \cdot W_N^{(i)}(\mathbf{y}_{N+1}^{2N}, \mathbf{u}_{1,2}^{3i-3}|u_{3i-1}) W_N^{(i)}(\mathbf{y}_{2N+1}^{3N}, \mathbf{u}_{1,3}^{3i-3}|u_{3i}) \end{aligned}$$

$$\begin{aligned} &W_{3N}^{(3i-1)}(\mathbf{y}_1^{3N}, \mathbf{u}_1^{3i-2}|u_{3i-1}) \\ &\quad = \sum_{u_{3i}} \frac{1}{3} W_N^{(i)}(\mathbf{y}_1^N, \oplus_{j=1}^3 \mathbf{u}_{1,j}^{3i-3}| \oplus_{j=0}^2 u_{3i-j}) \\ &\quad \cdot W_N^{(i)}(\mathbf{y}_{N+1}^{2N}, \mathbf{u}_{1,2}^{3i-3}|u_{3i-1}) W_N^{(i)}(\mathbf{y}_{2N+1}^{3N}, \mathbf{u}_{1,3}^{3i-3}|u_{3i}) \end{aligned}$$

$$\begin{aligned} &W_{3N}^{(3i)}(\mathbf{y}_1^{3N}, \mathbf{u}_1^{3i-1}|u_{3i}) \\ &\quad = \frac{1}{3} W_N^{(i)}(\mathbf{y}_1^N, \oplus_{j=1}^3 \mathbf{u}_{1,j}^{3i-3}| \oplus_{j=0}^2 u_{3i-j}) \\ &\quad \cdot W_N^{(i)}(\mathbf{y}_{N+1}^{2N}, \mathbf{u}_{1,2}^{3i-3}|u_{3i-1}) W_N^{(i)}(\mathbf{y}_{2N+1}^{3N}, \mathbf{u}_{1,3}^{3i-3}|u_{3i}). \end{aligned}$$

The transformation Ξ_{3^n} is not only rate-preserving but also reliability-improving, i.e.,

$$\sum_{j=0}^{2} I(W_{3N}^{(3i-j)}) = 3I(W_N^{(i)})$$

$$\sum_{j=0}^{2} Z(W_{3N}^{(3i-j)}) \le 3Z(W_N^{(i)}).$$

In addition, the channel splitting moves the rate and reliability away from the center. Namely, we obtain the following results

$$I(W_{3N}^{(3i-2)}) \le I(W_{2N}^{(3i-1)}) \le I(W_N^{(i)}) \le I(W_{3N}^{(3i)})$$
$$Z(W_{3N}^{(3i-2)}) \ge Z(W_{3N}^{(3i-1)}) \ge Z(W_N^{(i)}) \ge Z(W_{3N}^{(3i)}).$$

The afore-mentioned reliability terms further satisfy the following constrained conditions

$$\begin{aligned} Z(W_{3N}^{(3i-2)}) &\le 3Z(W_N^{(i)}) - 2Z^3(W_N^{(i)}) \\ Z(W_{3N}^{(3i-1)}) &= Z(W_{3N}^{(3i)}) = Z(W_N^{(i)})^3. \end{aligned} \tag{6}$$

To illustrate the process of polarization on the basis of core matrix $\mathcal{O}_3$ for a given $N = 3^n$, each input sequence $\mathbf{u}_1^N$ can be encoded through using an encoder

$$\mathbf{x}_1^N = \mathbf{u}_1^N G_N, \tag{7}$$

where $G_N = B_N \mathcal{O}_3^{\otimes n}$ is the generator matrix of order N and B_N is a permutation matrix (operation) defined in the recursion way as

$$B_N = R_N(I_3 \otimes R_{N/3}) \cdots (I_{N/3} \otimes R_3). \tag{8}$$

We note that $\mathcal{O}_3 \cdot \mathcal{O}_3 = I_3$ and $B_N = R_N(I_3 \otimes B_{N/3})$.

Actually, it is easy to prove that $R_N(G_3 \otimes I_{N/3}) = (I_{N/3} \otimes \mathcal{O}_3) R_N$. Therefore, one has

$$G_N = (I_{N/3} \otimes G_3) R_N (I_3 \otimes R_{N/3}),$$

which can be rewritten as

$$\begin{aligned} G_N &= R_N(\mathcal{O}_3 \otimes G_{N/3}) \\ &= R_N(I_3 \otimes R_{N/3})(\mathcal{O}_3^{\otimes 2} \otimes G_{N/3^2}). \end{aligned} \tag{9}$$

 ISBN: 978-1-61208-199-1

Denote $\mathcal{G}_N = \mathcal{O}_3^{\otimes n}$. Then one achieves

$$\begin{aligned}\mathcal{G}_N &= \mathcal{G}_{N/3} \otimes \mathcal{G}_3 \\ &= \prod_{i=1}^{n} (I_{3^{n-i}} \otimes \mathcal{O}_3 \otimes I_{3^{i-1}}) = \prod_{i=1}^{n} \mathcal{G}_N^i, \end{aligned} \quad (10)$$

where $\mathcal{G}_N^i = I_{3^{n-i}} \otimes \mathcal{G}_3 \otimes I_{3^{i-1}}$ and $G_3 = \mathcal{O}_3$. Consequently there are N row's permutation matrices $P_N^r(i)$ and N column's permutation matrices $P_N^c(i)$ of $\mathcal{G}_N^i$ such that $P_N^r(i) \cdot P_N^c(i) = P_N^c(i) \cdot P_N^r(i)$. Then we show that the factorizations have equal factors as follows

$$P_N^r G_N P_N^c = \prod_{i=1}^{n} \hat{\mathcal{G}}_N^i = (I_{3^{n-1}} \otimes \mathcal{O}_3)^n, \quad (11)$$

where $\hat{\mathcal{G}}_N^i = P_N^r(i) \cdot \mathcal{G}_N^i \cdot P_N^r(i)$.

Moreover, we consider another channel combining scheme based on core matrix

$$\hat{\mathcal{O}}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

to generate a vector channel $W_{3^n}^{(i)}$, where the core matrix $\hat{\mathcal{O}}_3$ is sub-matrix of $\mathcal{O}_4 = \mathcal{O}_2^{\otimes 2}$, i.e.,

$$\mathcal{O}_4 = \begin{pmatrix} 1 & \mathbf{0}_{3\times 1} \\ \mathbf{1}_{1\times 3} & \hat{\mathcal{O}}_3 \end{pmatrix},$$

where $\mathbf{1}_{1\times 3} = (1,1,1)$, $\mathbf{0}_{3\times 1} = (0,0,0)^T$, and $\hat{\mathcal{O}}_3 \cdot \hat{\mathcal{O}}_3 = I_3$. In this case the first level of the recursion combines three independent copies of W that achieves the combined channel W_3 with the following transition probabilities

$$W_3(\mathbf{y}_1^3|\mathbf{u}_1^3) = W(y_1|u_1 \oplus u_3)W(y_2|u_2 \oplus u_3)W(y_3|u_3), \quad (12)$$

where W_3 is defined as $W_3(\mathbf{y}_1^3|\mathbf{x}_1^3) = W^3(\mathbf{y}_1^3|\mathbf{u}_1^3\hat{\mathcal{O}}_3)$. To design the second level of the recursion we obtain the combined channel W_{3^2} in Fig. 2 with transition probabilities

$$\begin{aligned} W_{3^2}(\mathbf{y}_1^9|\mathbf{u}_1^9) &= W_3(y_1^3|u_1 \oplus u_3, u_4 \oplus u_6, u_7 \oplus u_9) \\ &\cdot W_3(y_4^6| \oplus_{i=2}^3 u_i, \oplus_{i=5}^6 u_i, \oplus_{i=8}^9 u_i) W_3(y_7^9|u_3, u_6, u_9). \end{aligned}$$

To construct polar-code sequences of block length 3^n based on the polarization of channel with generator matrices G_{3^n} for core matrix $\mathcal{O}_3$ of order 3, we should compute the reliability channel polarization in terms of the vector

$$Z(3^n) = (Z_{3^n,1}, Z_{3^n,2}, \cdots, Z_{3^n,3^n})$$

through using the recursion

$$Z_{3k,j} = \begin{cases} 3Z_{k,j} - 2Z_{k,j}^3, & \text{for } 1 \le j \le k; \\ Z_{k,j-k}^3, & \text{for } k+1 \le j \le 2k, \\ Z_{k,j-2k}^3, & \text{for } 2k+1 \le j \le 3k, \end{cases} \quad (13)$$

for any $k = 1, 3, 3^2, \cdots, 3^{n-1}$ starting with $Z_{1,1} = 1/2$. After that we generate a permutation operation $\pi_{3^n} = (i_1, \cdots, i_{3^n})$ with respect to the set $(1, \cdots, 3^n)$ so that $Z_{3^n,i_j} < Z_{3^n,i_k}$ for any $1 \le j < k \le 3^n$. The generator matrix $\mathcal{G}_P(3^n, K)$ of a $(3^n, K)$ polar-code can be constructed from the sub-matrix of G_{3^n} with indices $\{i_1, \cdots, i_K\} \subseteq \{1, \cdots, N\}$. According to the polarization of channel with generator matrices G_{3^n}, it is obvious that the computational complexity of this processing is $2n3^{\frac{n}{2}}$. However, the computational complexity of the direct approach is $n3^n$, which shows an advantage of the proposed construction.

Example 1: Taking the matrix $\mathcal{G}_9 = \mathcal{O}_3^{\otimes 2}$ for recursion in Eq.(13), we have

$$\begin{aligned} Z_9 = (&0.857, 0.034, 0.034, 0.034, 0.001, 0.001, \\ &0.034, 0.001, 0.001), \end{aligned} \quad (14)$$

which gives the permutation $\pi_8 = (9,8,6,5,7,4,3,2,1)$ for rows of the generator matrix $\mathcal{G}_9$. Exploiting the polarization of channel with generator matrices G_9, the code $(9, 5, \{9,8,6,5,7\}, (0,0,0,0)$ can be constructed with the encoder mapping as follows

$$\begin{aligned} \mathbf{x}_1^9 &= \mathbf{u}_1^9 G_9 \\ &= (u_{98657}) \begin{pmatrix} 110110000 \\ 101101000 \\ 100100100 \\ 110110110 \\ 101010101 \end{pmatrix} + (0000) \begin{pmatrix} 100000000 \\ 110000000 \\ 101000000 \\ 000100000 \end{pmatrix}. \end{aligned}$$

For a source block $(1,1,1,1)$, the coded block is $\mathbf{x}_1^9 = (1,1,1,1,1,0,0,0,0)$. It is necessary to note that this code is an $(N,K) = (9,5)$ Reed-Muller code with the generator matrix

$$G_R = \begin{pmatrix} 110110000 \\ 101101000 \\ 100100100 \\ 110110110 \\ 101010101 \end{pmatrix}.$$

III. DECODING ALGORITHM

In this section, we consider the decoding algorithm of the proposed polar codes. As in the previous section, our computational model will be a single processor machine with a random-access memory. We consider the decoding of G_N-coset codes with parameters $(N, K, \mathcal{A}, \mu_{\mathcal{A}^c})$ for a given block length $N = 3^n$.

Recall that the source vector $\mathbf{u}_1^N$ consists of a random part $\mu_{\mathcal{A}}$ and a frozen part $\mu_{\mathcal{A}^c}$ such that $\mathbf{u}_1^N = \{\mu_{\mathcal{A}} \cup \mu_{\mathcal{A}^c}\}$. This vector $\mathbf{u}_1^N$ is transmitted across W_N and a channel output $\mathbf{y}_1^N$ is obtained with probability $W_N(\mathbf{y}_1^N|\mathbf{u}_1^N)$. The decoder observes $(\mathbf{y}_1^N, \mu_{\mathcal{A}^c})$ and generates an estimate $\hat{\mathbf{u}}_1^N$ of $\mathbf{u}_1^N$.

If $i \in \mathcal{A}^c$, the element u_i is known, and thus the i-th decision element is $\hat{u}_i = u_i$. However, if $i \in \mathcal{A}$, then the i-th decision element waits until it has received the previous decisions $\hat{\mathbf{u}}_1^{i-1}$. Upon receiving them, the decoder computes

 ISBN: 978-1-61208-199-1

$$
\begin{aligned}
&L_N^{(3i-2)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-3})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-3}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-3}|1)}\\
&=\frac{L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})[L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})+1]}{L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})+1}\\
&\quad+\frac{L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})[L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})]}{L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})+1}\\
&L_N^{(3i-1)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-2})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-2}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-2}|1)}\\
&=\frac{L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})[L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})^{1-2\hat{u}_{3i-2}}L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})+1]}{L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3})+L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})^{1-2\hat{u}_{3i-2}}}\\
&L_N^{(3i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-1})=\frac{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-1}|0)}{W_N(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{3i-1}|1)}\\
&=L_{N/3}^{(i)}(\mathbf{y}_1^{N/3},\oplus_{j=1}^3\hat{\mathbf{u}}_{1,j}^{3i-3})^{1-2(\hat{u}_{3i-2}\oplus\hat{u}_{3i-1})}L_{N/3}^{(i)}(\mathbf{y}_{N/3+1}^{2N/3},\hat{\mathbf{u}}_{1,2}^{3i-3})^{1-2\hat{u}_{3i-1}}L_{N/3}^{(i)}(\mathbf{y}_{2N/3+1}^{N},\hat{\mathbf{u}}_{1,3}^{3i-3}) \qquad (15)
\end{aligned}
$$

the likelihood ratio (LR) as follows

$$L_N^{(i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1})=\frac{W(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1}|0)}{W(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1}|1)}, \qquad (16)$$

and generates its decision through using

$$\hat{u}_i=\begin{cases}0, & \text{if } L_N^{(i)}(\mathbf{y}_1^N,\hat{\mathbf{u}}_1^{i-1})\geq 1;\\ 1, & \text{otherwise,}\end{cases} \qquad (17)$$

which is then sent to all succeeding decision elements. This processing is a single-pass algorithm, with no revision of estimates. The complexity of this algorithm is determined essentially by the complexity of computing the LRs.

As for polarization of channel based on generator matrix G_{3^n} of order 3^n, we calculate with the recursive formulas (6)-(6) on the top of the next page based on core matrix $\mathcal{O}_3$ and obtain the formula in Eq.(15).

IV. Conclusion

In this paper, we considered the overall encoding/decoding structures and systems of the polar-code sequence to show the expression of encoding/decoding of the polar-code with fast algorithms based on its generator matrix $\mathcal{G}_{3^n}$. The complexity of the proposed encoding scheme is much lower than the previous which is proposed by Arikan. By transmitting the information bits over the almost noiseless B-DMC W, polar-codes of block-length 3^n can be fast constructed starting with any polarizing matrix G_{3^n}. The encoding and successive cancellation decoding complexities of such codes are lower than Arikan's code.

Acknowledgment

This work was supported by World Class University R32-2010-000-20014-0 NRF, FR2010-0020942 NRF, Post BK21, Korea, 2011 Korea-China international Cooperative Research Project(Grant Nos, Dooo66,100026), and partly by NSFC 60902044, the New Century Excellent Talents in University (NCET-11-0510), China.

References

[1] E. Arikan, Channel Polarization: A Method for Constructing Capacity-Achieving codes for Symmetric Binary-Input Memoryless Channel, *IEEE Trans. Inform. Theory*, Vol. 55, No. 7, July 2009.

[2] E. Arikan, Channel Combining and Splitting for Cutoff Rate Improvement, *IEEE Trans. Inform. Theory*, Vol. 52, No. 2, FEB 2006.

[3] E. Arikan, performance comparison of polar-codes and Reed-Muller codes, *IEEE. Comm. Lett.*, Vol. 12, pp. 447-449, June 2008.

[4] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.*, Vol. 27, pp. 379-423, 623-656, Jul.-Oct. 1948.

[5] E. Arikan and E. Telatar, the rate of channel polarization, July 2008. [Online]. Available: arXiv:0807.3806v2.

[6] I. Reed, A class of multiple-error-correcting codes and the decoding scheme, *IRE Trans. Inf. Theory*, Vol. 4, No. 3, pp. 39-44, Sep. 1954.

[7] M. Plotkin, Binary codes with specified minimum distance, *IRE Trans. Inf. Theory*, Vol. 6, No. 3, pp. 445-450, Sep. 1960.

[8] G. D. Forney Jr., Codes on graphs: Normal realizations, *IEEE Trans. Inform. Theory*, Vol. 47, No. 2, pp. 520-548, Feb. 2001.

[9] G. Zeng and M. H. Lee, A Generalized Reverse Block Jacket Transform, *IEEE Trans. Circuits Syst. I*, Vol. 55, No. 6, pp. 651-669, 2008.