

β -expansion: A Theoretical Framework for Fast and Recursive Construction of Polar Codes

Gaoning He, Jean-Claude Belfiore, Ingmar Land, Ganghua Yang
Paris Research Center, Huawei Technologies
20 quai du Point du Jour, Boulogne Billancourt, France
Email: {hegaoning, jean.claude.belfiore}@huawei.com

Xiaocheng Liu, Ying Chen, Rong Li, Jun Wang
Hangzhou Research Center, Huawei Technologies
360 Jiangshu Road, Binjiang, Hangzhou, China
Email: {liuxiaocheng, chenying18}@huawei.com

Yiqun Ge, Ran Zhang, Wen Tong
Ottawa Research Center, Huawei Technologies
303 Terry Fox Drive, Ottawa, Canada
Email: {yiqun.ge, ran.zhang1}@huawei.com

Abstract—In this work, we introduce β -expansion, a notion borrowed from number theory, as a theoretical framework to study fast construction of polar codes based on a recursive structure of universal partial order (UPO) and polarization weight (PW) algorithm. We show that polar codes can be recursively constructed from UPO by continuously solving several polynomial equations at each recursive step. From these polynomial equations, we can extract an interval for β , such that ranking the synthetic channels through a closed-form β -expansion preserves the property of nested frozen sets, which is a desired feature for low-complex construction. In an example of AWGN channels, we show that this interval for β converges to a constant close to $1.1892 \approx 2^{1/4}$ when the code block-length trends to infinity. Both asymptotic analysis and simulation results validate our theoretical claims.

I. INTRODUCTION

Polar code, introduced by Arikan [1], is the first code with an explicit construction to achieve the channel capacity for many classes of channels. The key idea of polar codes lies in the famous phenomenon of channel polarization, which transforms physical channels into virtual channels (or called synthetic channels). These virtual channels tend to either extreme good (reliability equals to 1) or extreme bad (reliability equals to 0) when the block-length N goes to infinity. In other words, channels are polarized. In this case, the best strategy is to transmit useful information bits only in the positions of good channels and leave the positions of bad channels "frozen". As a consequence, the question of how to efficiently identify the positions and rank the reliability order of these good and bad channels becomes critical for polar code construction.

Unfortunately, up to now, efficient construction only exists for binary erasure channel (BEC) [1]. However, polar code is supposed to work at least for additive white Gaussian noise (AWGN) channels in the 5th generation wireless systems. In the case of AWGN channels, several techniques are commonly used, for example, density evolution (DE) [2] and Gaussian approximation (GA) of density evolution [3]. However, the main drawback of DE/GA is their high computational complexity, which scales linearly with the code block-length, and therefore

unacceptable for practical systems with varying parameters such as block-length and code rate. They are even infeasible to be used for an on-the-fly implementation of a low-latency encoder/decoder.

While the low-complex construction problem remains unsolved for the AWGN channel, it has been shown recently in [4]–[6] that a certain partial order relation exists between the reliabilities of the synthetic channels of a polar code. This discovery may greatly reduce the complexity of polar code construction to a sublinear level, since these partial orders are deterministic and *universal*, in the sense that it holds for any transmission channel. It is further shown in [7] that if we take the advantage of the partial order, we can construct a polar code of block-length N by only computing the reliability of roughly a fraction $1/\log^{3/2} N$ of the synthetic channels. Separately in [8], a closed-form algorithm called polarization weight is proposed to characterize the reliability order of synthetic channels for AWGN channels with low complexity. These two independent works enlighten us to pursue a theoretical explanation towards a fast construction scheme for practical transmission channels such as AWGN.

In this paper, we analyse the properties of universal partial order (UPO) and discover that UPO has an inherent recursive structure. We explore the theory of polarization weight algorithm by introducing a number theoretical concept called β -expansion. From this theory and the recursive structure of UPO, we find that polar codes can actually be efficiently constructed from UPO by applying β -expansion at each recursive step with a carefully chosen β .

The paper is organized in the following form: We first revisit the concept of channel polarization and UPO of polar codes in section II. In section III, we show the recursive structure of UPO. In section IV, we study β -expansion theory of polarization weight algorithm. We show in section V how β -expansion can help towards a fast construction. Finally, we provide asymptotic analysis and numerical results in section V followed by conclusions in section VII.

II. PRELIMINARIES

A. Channel polarization

Channel polarization is a key phenomenon in polar codes. It consists in "splitting" the channel $W : \mathcal{X} \rightarrow \mathcal{Y}$ into a pair of channels $W^0 : \mathcal{X} \rightarrow \mathcal{Y}^2$ and $W^1 : \mathcal{X} \rightarrow \mathcal{X} \times \mathcal{Y}$, defined as

$$W^0(y_1, y_2|x_1) = \frac{1}{2} \sum_{x_2 \in \mathcal{X}} W(y_1|x_1 \oplus x_2)W(y_2|x_2), \quad (1)$$

$$W^1(y_1, y_2, x_1|x_2) = \frac{1}{2} W(y_1|x_1 \oplus x_2)W(y_2|x_2). \quad (2)$$

After applying n times this "splitting" operation, from the original channel W , we obtain $N = 2^n$ different channels $\{W_N^0, W_N^1, \dots, W_N^{N-1}\}$, which are called "synthetic channels".

Definition 1. (Synthetic channel): Let $(b_{n-1}, \dots, b_1, b_0)$, $b_k \in \{0, 1\}$, be the binary expansion of integer $i \in [0, N-1]$ over n bits with the most significant bit on the left. The synthetic channels are defined as

$$W_N^i = ((W^{b_0})^{b_1} \dots)^{b_{n-1}}, \quad i = 0, \dots, N-1$$

where $(\cdot)^{b_k}$ is obtained from equation (1) and (2).

Definition 2. (Reliability measure): If the mutual information $I(W_N^i) > I(W_N^j)$, or equivalently if the Bhattacharyya parameter [1] $Z(W_N^i) < Z(W_N^j)$, we say the synthetic channel W_N^i is more reliable than W_N^j , denoted as $W_N^i \succ W_N^j$, or simply $i \succ j$. $I(\cdot)$ and $Z(\cdot)$ are defined as

$$I(W) = I(X; Y),$$

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

where $p_{Y|X}(y|x)$ is the transmission probability.

B. Universal partial order (UPO)

In [6] it is proved that a partial order of reliability measure exists for any symmetric channels with binary inputs. They are "partial" because they are insufficient to form a fully ordered sequence covering all N bit positions, each corresponds to an index of the synthetic channel.

Given any pair of synthetic channel indices (x, y) , their reliability relation may be determined by applying the following rules [7]:

- **Addition:** If a binary representation of the index of a synthetic channel is $(a, b, 1, c)$, then it must be less reliable than the synthetic channel whose index has a binary representation $(a, b, 0, c)$. Such "1 \succ 0" pattern can happen on one bit or multiple bits. For example:

$$2 \ (0, 1, \underline{0}) \prec 3 \ (0, 1, \underline{1}),$$

$$9 \ (1, \underline{0}, \underline{0}, 1) \prec 15 \ (1, \underline{1}, \underline{1}, 1).$$

- **Left-swap:** If a binary representation of the index of a synthetic channel is $(a, 0, b, 1, c)$, then it must be less reliable than the synthetic channel whose index has a binary representation $(a, 1, b, 0, c)$. Such "0..1 \prec 1..0" pattern can occur multiple times, and 0, 1 do not need to be adjacent to each other. For example:

$$2 \ (\underline{0}, \underline{1}, 0) \prec 4 \ (\underline{1}, \underline{0}, 0),$$

$$12 \ (\underline{0}, 1, \underline{1}, 0, 0) \prec 24 \ (\underline{1}, 1, \underline{0}, 0, 0).$$

However, for some pairs of synthetic channel indices (x, y) , their orders cannot be determined by the rule of Addition or Left-swap or their combination. For example:

$$3 \ (0, 1, 1) \quad \text{and} \quad 4 \ (1, 0, 0),$$

$$7 \ (0, 1, 1, 1) \quad \text{and} \quad 12 \ (1, 1, 0, 0).$$

We say that these orders are unknown to UPO.

III. PROPERTIES OF UNIVERSAL PARTIAL ORDER

Proposition 1. (Nested and Symmetric) The universal partial order of polar codes has two important properties:

- **Nested:** The orders determined for a code of length N remain unchanged in code length of $2N$.
- **Symmetric:** The order of $x \prec y$ and the order of $(N-1-x) \succ (N-1-y)$ are twin pairs for a polar code of length N .

Proof. The Nested property is easy to be proved, since a binary expansion (a, b, c) in length N can be expressed as $(0, a, b, c)$ in length $2N$, which doesn't affect the rule of Addition and Left-swap.

To prove the Symmetric property, we let the binary expansion of x be $(x_{n-1}, \dots, x_1, x_0)$ and the binary expansion of y be $(y_{n-1}, \dots, y_1, y_0)$. Now assume $x \prec y$, we must have either for some $i \in [0, N-1]$

$$x_i = 0 \text{ and } y_i = 1 \text{ (Addition)} \quad (3)$$

and/or for some $i, j \in [0, n-1], i \neq j$

$$x_i (= 0), \dots, x_j (= 1) \text{ and } y_i (= 1), \dots, y_j (= 0) \text{ (Left-swap)}. \quad (4)$$

Now, let \bar{x} be the one's complement of x . We write the binary expansion of $(N-1-x)$, the symmetric node of x , as $(\bar{x}_{n-1}, \dots, \bar{x}_1, \bar{x}_0)$, and the binary expansion of $(N-1-y)$, the symmetric node of y , as $(\bar{y}_{n-1}, \dots, \bar{y}_1, \bar{y}_0)$. From (3) and (4), we must have $(N-1-x) \succ (N-1-y)$. This is because we have either $\bar{x}_i (= 1) \succ \bar{y}_i (= 0)$ and/or $\bar{x}_i (= 1), \dots, \bar{x}_j (= 0) \succ \bar{y}_i (= 0), \dots, \bar{y}_j (= 1)$. This proves the symmetric property. \square

Now, we are ready to show the recursive structure of the UPO. Let us first define \mathbf{UPO}_n as the minimum set of UPO relation $x \prec y$ (denoted as $\{x, y\}$) of a polar code with length $N = 2^n$, where x, y are integers in $[0, N-1]$. Here, the minimum set means that if we have a relation chain $x \prec y \prec z$,

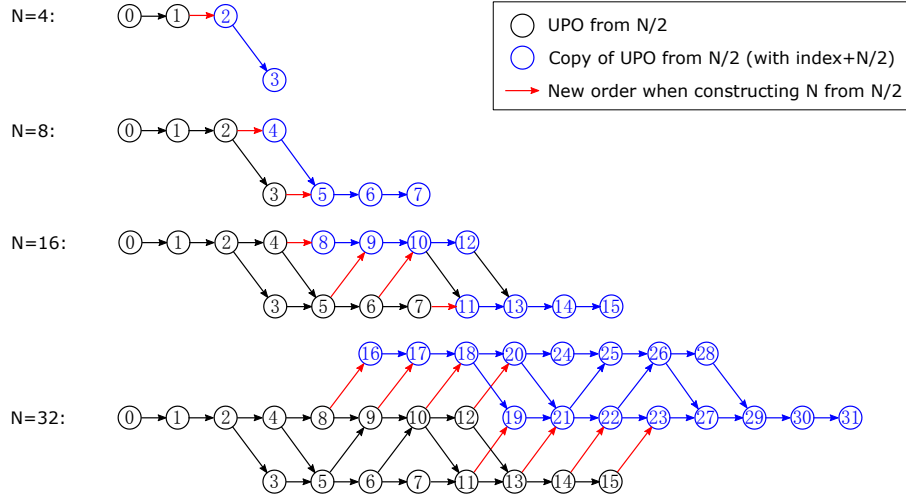


Figure 1. Illustration of recursive construction structure of universal partial orders of polar codes. The directed arrow between two nodes (synthetic channel indices) $x \rightarrow y$ indicate that the source node x has lower reliability than the destination node y .

we will express them as several sub-chains between only the most adjacent nodes, i.e., $x \prec y$ and $y \prec z$. We have:

$$\begin{aligned}
 \text{UPO}_1 &= \{\{0, 1\}\}, \\
 \text{UPO}_2 &= \{\{0, 1\}, \{1, 2\}, \{2, 3\}\}, \\
 \text{UPO}_3 &= \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 5\}, \\
 &\quad \{4, 5\}, \{5, 6\}, \{6, 7\}\}, \\
 \text{UPO}_4 &= \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 5\}, \\
 &\quad \{4, 5\}, \{5, 6\}, \{6, 7\} \\
 &\quad \{4, 8\}, \{5, 9\}, \{6, 10\}, \{7, 11\}, \\
 &\quad \{8, 9\}, \{9, 10\}, \{10, 11\}, \{10, 12\}, \{11, 13\}, \\
 &\quad \{12, 13\}, \{13, 14\}, \{14, 15\}\}
 \end{aligned}$$

where the orders in black color in level n are inherited from UPO in the upper level $n - 1$, i.e., UPO_{n-1} (corresponds to the nested property in Proposition 1). The orders in blue color represent the symmetric part of the orders in black color (corresponds to the symmetric property in Proposition 1), and the orders in red color represents the new orders when constructing UPO_n from UPO_{n-1} .

Generally speaking, any UPO of length 2^n (UPO_n) can be recursively generated from $\text{UPO}_1 = \{\{0, 1\}\}$ by applying the same rule. This phenomenon can be observed from Figure 1.

IV. β -EXPANSION: THEORY OF PW ALGORITHM

The notion of polarization weight (PW) is first introduced in [8], where a closed-form algorithm is used to fully characterize the reliability orders of synthetic channels of a polar code.

Definition 3. (PW algorithm) Consider a synthetic channel index x and its binary expansion $B = (b_{n-1}, \dots, b_1, b_0)$ over n bits with the most significant bit on the left. Its polarization weight is defined as

$$f^{\text{PW}} : x \mapsto \sum_{i=1}^n b_i \beta^i \quad (5)$$

where β is a carefully chosen number. For example, $\beta = 2^{1/4}$ is suggested in [8].

In mathematics, this notion is called β -expansions [9], [10] introduced by Reñyi as a number theoretical concept in 1957. β -expansions are a generalization of decimal expansions and can be seen as a non-integral representation (with base β) of any real number y .

Example 1. Let $\beta = 2^{1/4}$ and block-length $N = 2^n = 16$. The β -expansion of the synthetic channel with index 3, i.e., $B_3 = (0, 0, 1, 1)$, can be computed as

$$w_3 = 0 \cdot 2^{3/4} + 0 \cdot 2^{2/4} + 1 \cdot 2^{1/4} + 1 \cdot 2^{0/4} = 2.189 \dots$$

Similarly, we can write the β -expansions of all the synthetic channels as

$$\begin{aligned}
 \mathbf{w} = \{ &0.000 \ 1.000 \ 1.189 \ 2.189 \ 1.414 \ 2.414 \ 2.603 \ 3.603 \\
 &1.682 \ 2.682 \ 2.871 \ 3.871 \ 3.096 \ 4.096 \ 4.285 \ 5.285 \}
 \end{aligned}$$

where a larger value of w_x indicates a higher reliability of the synthetic channel with index x . By sorting \mathbf{w} , we obtain a total order

$$\text{Order} = \{0 \ 1 \ 2 \ 4 \ 8 \ 3 \ 5 \ 6 \ 9 \ 10 \ 12 \ 7 \ 11 \ 13 \ 14 \ 15\}.$$

The advantage of PW algorithm is that it provides a neat and low-complex method to fully rank the reliability of synthetic channels while keeping the property of nested frozen sets when the code length 2^n grows.

Proposition 2. (Nested structure) The PW algorithm preserves the feature of nested code construction (or nested frozen sets) for polar codes.

Proof. Similar to the proof of Proposition 1, any arbitrary binary expansion (a, b, c, \dots) in length N can be expressed as $(0, a, b, c, \dots)$ in length $2N$. But this does not change the outcome of PW algorithm according to equation (5). \square

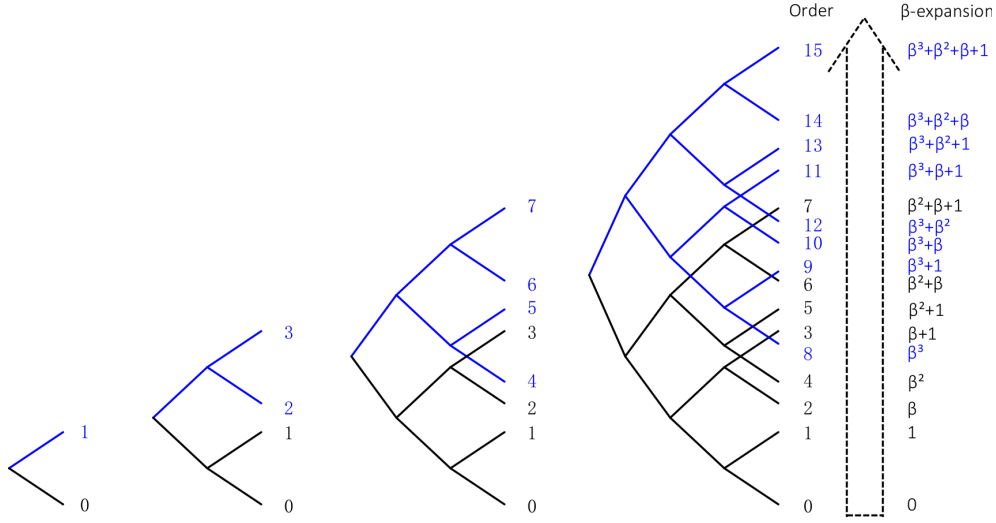


Figure 2. Illustration of nested structure of β -expansions with $\beta = 2^{1/4}$ for block-length $N = 2, 4, 8, 16$.

Nested structure is a highly desired feature when designing code construction with variable block-lengths (which is the case for wireless systems). It helps to greatly reduce the overall construction complexity, in the sense that a construction at block-length N can be kept and reused at longer block-length $2N, 4N, \dots$, etc. Figure 2 shows the nested structure of β -expansions with $\beta = 2^{1/4}$ for block-length $N = 2, 4, 8, 16$.

Proposition 3. When $\beta > 1$, any sequence derived from PW algorithm respects the UPO of polar codes.

Proof. First, the Addition rule is respected by β -expansion, because $0 < \beta^j$ holds for any non-negative integer j . Second, the left-swap rule is also respected, since when $\beta > 1$ the inequality $\beta^j < \beta^{j+k}$ holds for any non-negative integer j and positive integer k . This completes the proof. \square

From this proposition, we know that the sequence derived from the PW algorithm does not violate the orders from UPO as long as $\beta \in (1, +\infty)$. This also implies that if β picks a specific number in $(1, +\infty)$, PW algorithm introduces new orders which do not belong to UPO. Now, the question is which value β should take such that PW algorithm or β -expansions can give a good sequence.

It is known that β -expansions are not necessarily unique. A counter-example is when $\beta = \phi = \frac{1+\sqrt{5}}{2}$, the famous golden ratio, we have $\phi + 1 = \phi^2$. This means that β -expansions may become ill-conditioned (in the sense that it loses the ability to fully rank the sequence) when β equals some algebraic numbers that are real number roots of 0-1 polynomials (whose exponents are either 0 or 1 or -1). For example, ϕ is the root of the polynomial $x^2 - x - 1 = 0$. This is the reason we pointed out in Definition 3 that the value of β shall be carefully chosen. To address this issue, we have the following theorem:

Theorem 1. For a polar code of length 2^n ($n \geq 3$), there exists a set of ascending numbers $\mathcal{A}_n = \{a_0, a_1, a_2, \dots, a_{i_{\max}}, +\infty\}$, where $a_0 = 1$ and $a_1, a_2, \dots, a_{i_{\max}}$ are algebraic numbers,

such that for any β in the interval (a_i, a_{i+1}) , $\forall i \geq 0$, β -expansion is unique and results in a different ordered sequence. Moreover, the set \mathcal{A}_n is nested, i.e., $\mathcal{A}_n \subset \mathcal{A}_{n+1}$.

Proof. From equation (5), we can analyse the β -expansions for $n = 1$ to 4, as follows

- For $n = 1$ and 2, the sequence order is unique. This is because we have $\beta > 1$ by default.
- For $n = 3$, there is only one undecided relation, i.e., $(\beta + 1, \beta^2)$, whose order depends on the value of β . In order to distinguish their order, we need to solve the polynomial equation $x^2 - x - 1 = 0$, and we have

$$\mathcal{A}_3 = \{1, 1.618, +\infty\}.$$

When $\beta \in (1, 1.618)$, we have $\beta + 1 > \beta^2$, the corresponding sequence is

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 7.$$

When $\beta \in (1.618, +\infty)$, we have $\beta + 1 < \beta^2$, the corresponding sequence is

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7.$$

That is, when β falls in any interval of \mathcal{A}_3 , β -expansion is unique and gives a different sequence.

- For $n = 4$, there are 4 undecided relations, including the previous one $(\beta + 1, \beta^2)$ and two of its equivalent forms, i.e.,

$$(\beta + 1, \beta^2), (\beta^2 + \beta, \beta^3), (\beta^2 + \beta, \beta^3) \\ (\beta + 1, \beta^3), (\beta^2 + 1, \beta^3), (\beta^2 + \beta + 1, \beta^3)$$

In order to fully distinguish their orders, we need to solve 4 polynomial equations

$$x^3 - x^2 - x - 1 = 0 \quad (6)$$

$$x^3 - x^2 - 1 = 0 \quad (7)$$

$$x^2 - x - 1 = 0 \quad (8)$$

$$x^3 - x - 1 = 0 \quad (9)$$

and we have

$$\mathcal{A}_4 = \{1, 1.325, 1.466, 1.618, 1.839, +\infty\},$$

where 1.325, 1.466, 1.618, 1.839 are the roots of the four polynomial equations (6)-(9), respectively.

Similarly, we can iteratively run this process for the case of $n > 4$. It is apparent that the set \mathcal{A}_n is nested, because of the nested property of β -expansion. More precisely, if we have a undecided relation (x, y) in the sequence of length N , it must remain in the sequence of length $2N$, which results in a nested set for the corresponding algebraic number. This completes the proof. \square

V. AN EXAMPLE OF FAST CONSTRUCTION FOR AWGN CHANNELS

As discussed previously, UPO is a fundamental basis of polar code construction, which can determine many of the reliability orders of the synthetic channels, however, it cannot fully rank the whole sequence. On the other hand, although techniques such as DE/GA are able to rank the whole sequence, they are not suitable for practical implementation due to their high complexity. To compensate the drawbacks of both approaches, in this section, we present a fast construction method based on UPO and β -expansions.

We first give some intuition through the following Figure 3.

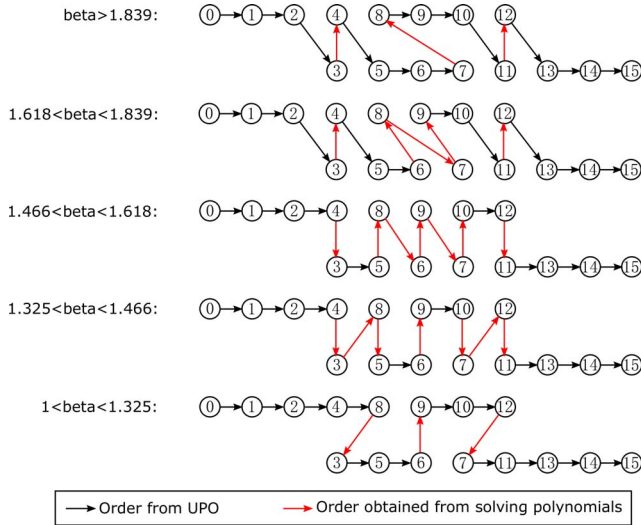


Figure 3. β -expansions for a polar code of block-length $N = 16$

We observe that when β falls in different interval in the set $\mathcal{A}_4 = \{1, 1.325, 1.466, 1.618, 1.839, +\infty\}$, β -expansion gives a different ordered sequence for polar codes of block-length $N = 16$.

From DE/GA, we know that for any SNR the sequence order for AWGN channels is

$$\begin{aligned} 0 &\rightarrow 1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 9 \\ &\rightarrow 10 \rightarrow 12 \rightarrow 7 \rightarrow 11 \rightarrow 13 \rightarrow 14 \rightarrow 15 \end{aligned}$$

which corresponds to the interval of $\beta \in (1, 1.325)$. This means if we carefully choose a interval for β , we can control

the outcome of β -expansion so that it gives the same or approximately the same good sequence compared with DE/GA.

In the following example, we show how this idea works for AWGN channels and how the interval of β behaves when the block-length grows from 8 to 1024.

- **N = 8:** Thanks to the recursive structure of UPO, we can construct an ordered sequence of length $N = 8$ from two sequences of length $N = 4$, as shown in Figure 4. Although the order of (3, 4) is unknown to UPO, from DE-GA we know $4 \prec 3$ for any SNR. This decides the interval (1, 1.618) for β .

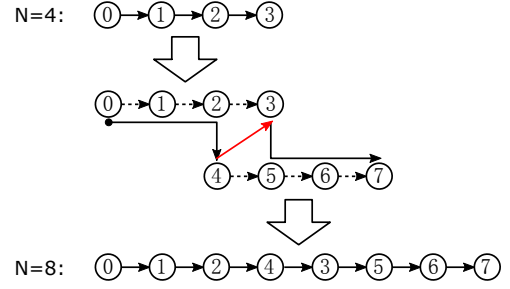


Figure 4. Illustration of sequence construction from $N = 4$ to 8.

- **N = 16:** Similar to $N=8$, we can construct the sequence of length $N = 16$ from two sequences of length $N = 8$, as shown in Figure 5. We have 3 new pairs (6, 9), (3, 8) and (7, 12) that are unknown to UPO. Again, from DE/GA we know $6 \prec 9, 8 \prec 3$ and $12 \prec 7$ for any SNR. Accordingly, the range of β is reduced from (1, 1.618) to (1, 1.325).
- **N = 32:** We have 5 new pairs that are unknown to UPO: (28, 15), (14, 19), (24, 13), (24, 11) and (24, 7). Again, from DE-GA we have

$$\begin{aligned} 28 \prec 15, 24 \prec 11 &\iff \beta < 1.221 \\ 14 \prec 19 &\iff \beta < 1.325 \\ 24 \prec 13 &\iff \beta < 1.272 \end{aligned}$$

The order (24, 7) is in general SNR-dependent for the AWGN channel. However, simulations tell us that the order $7 \prec 24$ has an overall better performance than the order $7 \succ 24$ for nearly all SNR values. Therefore, we choose

$$7 \prec 24 \iff \beta > 1.179$$

Accordingly, the range of β is reduced from to (1, 1.325) to $\in (1.179, 1.221)$.

- **N > 32:** We can repeat this searching process and we obtain Table I.. We see that the interval of β converges to a constant close to $1.1892 \approx 2^{1/4}$, and the number of new pairs is less than approximately 20% of the total number of synthetic channels.

VI. ASYMPTOTIC ANALYSIS AND NUMERICAL RESULTS

In this section, we study the asymptotic behaviour of β -expansion when $n \rightarrow \infty$. In fact, the problem of studying

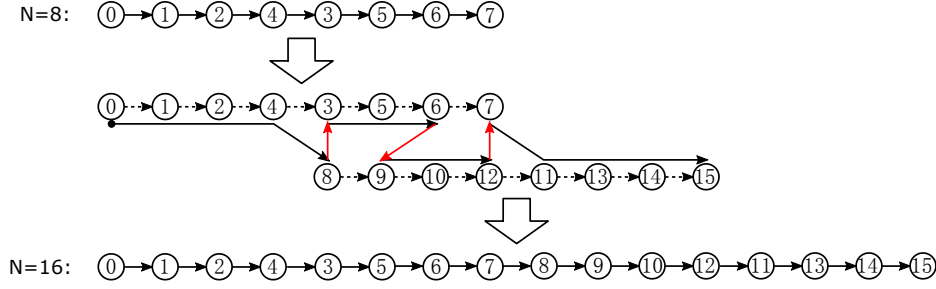


Figure 5. Illustration of sequence construction from $N = 8$ to 16.

Table I
INTERVAL FOR β AND THE NUMBER OF NEW PAIRS WHEN GENERATING
SEQUENCE FROM LENGTH N TO $2N$, FOR AWGN CHANNELS

$N \rightarrow 2N$	Interval of β	Number of new pairs
$16 \rightarrow 32$	(1.179, 1.221)	5
$32 \rightarrow 64$	(1.179, 1.194)	10
$64 \rightarrow 128$	(1.185, 1.190)	~ 30
$128 \rightarrow 256$	(1.1885, 1.190)	~ 50
$256 \rightarrow 512$	(1.18875, 1.18952)	~ 90
$512 \rightarrow 1024$	(1.189, 1.18932)	~ 200

distributions of the β -expansion can be transformed to another concept called Bernoulli convolution [11], [12]. Bernoulli convolution defines a probability measure

$$\nu_\lambda = \sum_{i=1}^{+\infty} b_i \lambda^{-i}, \quad \lambda \in (0, 1)$$

(where λ can be seen as $1/\beta$) assuming $B = (\dots, b_1, b_0)$ is a sequence of independent binary random variables satisfying

$$\Pr\{b_i = 1\} = \Pr\{b_i = 0\} = 0.5, \quad \forall i$$

It has been proved in [11] that the measure ν_λ is either *absolutely continuous* or *singular*. Clearly, we need the property of absolutely continuous for ν_λ to be able to fully rank the reliabilities of an infinite number of synthetic channels. It is further proved in [12] that if λ is of the form of $2^{-1/k}$, where k is any positive integer, then ν_λ is absolutely continuous. Thus, the choice of $\beta = 2^{1/4}$ in [8] satisfies the sufficient condition of absolutely continuous. When $k = 4$, we have $\beta = 1.1892$, which coincides with our observation in Table I.

In Figure 6, we compare the performance of GA and low-complex β -expansion construction with $\beta = 1.1892$ for the AWGN channel with QPSK and target block error rate (BLER) of 0.001. The decoder is successive cancellation list (SCL) decoder with list size 8 and extra 19-bit CRC [13]. As expected, β -expansion performs equally well as GA but with much lower complexity.

REFERENCES

[1] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Trans. Inform. Theory, vol. 55, no. 7, pp. 3051–3073, July 2009.

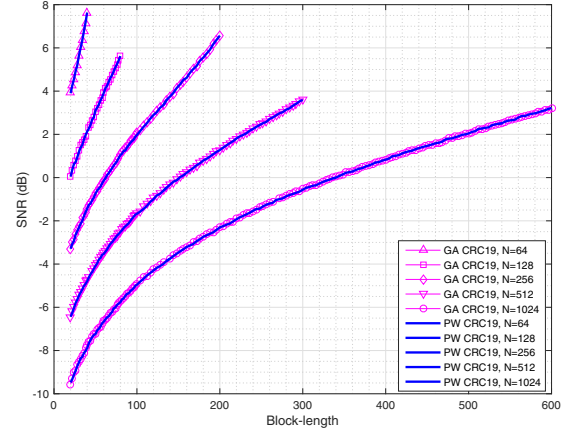


Figure 6. Comparison of PW algorithm with $\beta = 1.1892$ and Gaussian approximation for different block-length N (code length in number of code bits). Simulation assumptions are: BLER = 0.001, QPSK modulation, AWGN channel, successive cancellation list (SCL) decoder with list size 8 and extra 19-bit CRC.

[2] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in Proc. of the IEEE Int. Symposium on Inform. Theory (ISIT), Seoul, South Korea, July 2009, pp. 1496–1500.

[3] I. Tal and A. Vardy, "How to construct polar codes," IEEE Trans. Inf. Theory, vol. 59, no. 10, pp. 6562–6582, 2013.

[4] M. Bardet, J. Chaleut, V. Dragoi, A. Otmani, J. P. Tillich, "Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes", PQCrypto 2016, Feb 2016.

[5] M. Bardet, V. Dragoi, A. Otmani, J. P. Tillich, Algebraic Properties of Polar Codes From a New Polynomial Formalism, <https://arxiv.org/abs/1601.06215>

[6] C. Schurch, "A partial Order for the Synthesized Channels of a Polar Code, ISIT 2016.

[7] M. Mondelli, S. H. Hassani and R. Urbanke, "Construction of Polar Codes with Sublinear Complexity," submitted to ISIT 2017.

[8] 3GPP, R1-167209, Polar code design and rate matching, Huawei, HiSilicon.

[9] Rényi, Alfréd, "Representations for real numbers and their ergodic properties", Acta Mathematica Academiae Scientiarum Hungaricae, 8: 477–493, 1957.

[10] Parry, W., "On the β -expansions of real numbers", Acta Mathematica Academiae Scientiarum Hungaricae, 11: 401–416, 1960.

[11] P. Erdos, On a family of symmetric Bernoulli convolutions, Amer. J. Math, 1939.

[12] A. M. Garsia, Arithmetic properties of Bernoulli convolutions, Trans. Amer. Math. Soc. Vol. 102, 1962.

[13] K. Niu, K. Chen, J. Lin and Q. T. Zhang, Polar Codes: Primary Concepts and Practical Decoding Algorithms, IEEE Comm. Magazine, July 2014.