Polar Shaping Codes for Costly Noiseless and Noisy channels

Karthik Nagarjuna Tunuguntla and Paul H. Siegel
CMRR, University of California, San Diego
Email:{tkarthik,psiegel}@ucsd.edu

***Abstract*—We propose a shaping code based on polar codes. For a costly channel, we show that total cost of the proposed polar shaping code approaches optimal total cost as block length grows. We also consider shaping for the costly noisy discrete memoryless channels (DMCs). We first give an upper bound on rate that can be achieved with certain symbol occurrence probability distribution over DMCs. Then we formulate an optimization problem whose solution gives a lower bound on the optimal total cost for the costly noisy DMCs. We compute the lower bound for the M-ary erasure costly channel. Finally, we propose polar shaping codes for costly noisy channels that achieve the lower bound by using the polar codes that are designed to achieve capacity for asymmetric channels proposed by Honda and Yamamoto.**

I. Introduction

Shaping codes encode information for use on costly channels, i.e., channels with symbol costs subject to an average cost constraint. Their conceptual origins can be traced to Shannon's classic 1948 paper [15]. Prominent applications include data transmission with a power constraint [7] and, more recently, data storage on flash memories [10] and efficient strand synthesis for DNA-based storage [9]. Codes that minimize average cost per symbol for a given rate and codes that minimize average symbol cost per source symbol (or total cost) have been investigated, as has their application to noiseless and noisy costly channels. See [10] for further references.

Arıkan [1] constructed capacity-achieving polar codes for binary input symmetric channels. Arıkan also introduced source polarization, which served as the basis for source coding for non-uniform source alphabets [2]. A capacity-achieving coding scheme based on source and channel polarization for binary input asymmetric channels was proposed by Honda and Yamamoto [8]. In this scheme, complex boolean functions are shared between encoder and decoder for non-information carrying bit-channels. The use of common randomness is proposed to avoid these complex boolean functions [8]. En Gad et al. [6] used randomized rounding for low-entropy and not-completely polarized bit-channels. In addition, a side channel was used to reliably transmit bits corresponding to not completely polarized bit-channels, whose fraction is vanishing with respect to the block length. A proof that argmax can be used to encode low-entropy bit-channels is given by Chou and Bloch [5]. We proposed a staircase scheme [12] that avoids both common randomness and complex boolean functions to encode not-completely polarized bit-channels.

In this paper, we consider polar code design for costly memoryless channels, both noiseless and noisy. Shaping can also be viewed as a dual problem to source coding by converting information into symbols satisfying specified probabilistic properties, and we also adopt this perspective.

We first propose a polar shaping code design for a (costly) noiseless channel and a specified symbol probability distribution. The construction is an adaptation of the Honda and Yamamoto polar coding scheme for asymmetric channels [8]. The total cost of the proposed shaping code approaches the minimum possible value when the code is designed with the optimal rate and symbol distribution [10].

We then study shaping codes for costly noisy discrete memoryless channels (DMCs). This model is relevant to the design of efficient codes that combine shaping and error correction for use in a noisy transmission or storage system. We first give an upper bound on the rate that can be achieved on the DMC with a specified symbol occurrence probability distribution on codewords. Then we formulate an optimization problem whose solution gives a lower bound on the optimal total cost for the channel. (Note that the maximum rate achieved with a constraint on the average cost per code symbol has been investigated by Böcherer [3].) Finally, we show that polar codes for asymmetric channels [8] can be used to design shaping codes for costly noisy DMCs so that the total cost of the proposed code approaches the lower bound as the block length grows. The construction uses common randomness for encoding frozen bit-channels and not-completely polarized bit-channels in the code construction. Common randomness is crucial to get the desired shaping distribution on the codeword symbols.

We also show that the optimal total cost can be achieved by using random code construction methods, randomly choosing frozen bits and randomly choosing boolean functions for not-completely polarized channels [12], [8], and thereby avoiding the need for common randomness. For such a random code construction, we show that, with high probability, there exist codes in the random ensemble whose costs approach the optimal total cost with diminishing probability of error.

We note that a scheme that combines polar-coded modulation and probabilistic amplitude shaping [4] was introduced by Prinz et al. [13], and a novel constellation shaping based on polar-coded modulation was proposed by Matsumine [11].

II. Preliminaries

We denote the alphabet of the costly channel by $\mathcal{X}$. We denote the output alphabet of the costly noisy DMC by $\mathcal{Y}$. We express any set of random variables $X_i, X_{i+1}, \ldots, X_j$ $(i < j)$ by a row vector $(X_i, X_{i+1}, \ldots, X_j)$ which is denoted by $X^{i:j}$. We denote the set $\{1, 2, 3, \ldots, N\}$ by $[N]$. Let $U^{1:N}$ be a row vector and let $\mathcal{A} \subset [N]$. $U^{\mathcal{A}}$ denotes the row vector consisting of elements in $U^{1:N}$ corresponding to the subset of positions $\mathcal{A}$ in the same order. Let P and Q be any two distributions on a discrete arbitrary alphabet $\mathcal{Z}$. We denote the total variation distance between the two distributions P and Q as $||P - Q||$. Therefore $||P - Q|| = \sum_{z \in \mathcal{Z}} \frac{1}{2}|P(z) - Q(z)| = \sum_{z:P(z)>Q(z)} P(z) - Q(z)$. We denote the KL-divergence between two distributions P and Q as $D(P||Q)$.

Let X be the random variable distributed as $p(x)$ over alphabet $\mathcal{X}$. In this paper, we provide polar shaping codes for binary alphabets. So we let $\mathcal{X} = \{0, 1\}$ to introduce polarization results. Let $(X_1, Y_1), (X_2, Y_2), \ldots, (X_N, Y_N)$ be i.i.d. random tuples distributed according to $p(x)p(y|x)$ and $N = 2^n$. Let G_N be the conventional polar transformation [1], represented by a binary matrix of dimension $N \times N$. If $U^{1:N} = X^{1:N} G_N$, then we denote $\mathbb{P}(U^{1:N} = u^{1:N})$ by $P_{U^{1:N}}(u^{1:N})$ and similarly we denote $\mathbb{P}(U_i = u_i | U^{1:i-1} Y^{1:N} = u^{1:i-1} y^{1:N})$ by $P_{U_i|U^{1:i-1}Y^{1:N}}(u_i | u^{1:i-1} y^{1:N})$.

For two random variables (X, Y) distributed as $p(x)p(y|x)$, the Bhattacharya parameter is defined as

$$Z(X|Y) = 2 \sum_{y} P_Y(y) \sqrt{P_{X|Y}(1|y) P_{X|Y}(0|y)}.$$

Let $\beta < 0.5$ and define the following subsets obtained by polarization, with notation adapted from [6].

$$\mathcal{H}_X = \{i \in [N] : Z(U_i | U^{1:(i-1)}) \geq 1 - 2^{-N^{\beta}}\}.$$
$$\mathcal{L}_X = \{i \in [N] : Z(U_i | U^{1:(i-1)}) \leq 2^{-N^{\beta}}\}.$$
$$\mathcal{H}_{X|Y} = \{i \in [N] : Z(U_i | U^{1:(i-1)} Y^{1:N}) \geq 1 - 2^{-N^{\beta}}\}.$$
$$\mathcal{L}_{X|Y} = \{i \in [N] : Z(U_i | U^{1:(i-1)} Y^{1:N}) \leq 2^{-N^{\beta}}\}.$$

Note that $\mathcal{L}_X \subseteq \mathcal{L}_{X|Y}$. From Theorem 1 in [8] we have the following results.

$$\lim_{N\to\infty} \frac{1}{N} |\mathcal{H}_X| = H(X), \lim_{N\to\infty} \frac{1}{N} |\mathcal{L}_X| = 1 - H(X),$$
$$\lim_{N\to\infty} \frac{1}{N} |\mathcal{H}_{X|Y}| = H(X|Y),$$
$$\lim_{N\to\infty} \frac{1}{N} |\mathcal{L}_{X|Y}| = 1 - H(X|Y).$$

We define several other subsets of bit-channels as follows:

$$I = \mathcal{H}_X \cap \mathcal{L}_{X|Y}, F = \mathcal{H}_X \cap \mathcal{L}_{X|Y}^c, R = (\mathcal{H}_X \cup \mathcal{L}_X)^c.$$

We refer to these as good, bad, and not completely polarized bit-channels respectively. We refer to bit-channels in $\mathcal{H}_X$ and bit-channels in $\mathcal{L}_X$ as high-entropy bit-channels and low-entropy bit-channels respectively. The size of set R is a vanishing fraction with respect to the block length as N increases due to polarization. From [8, Theorem 1],

$$\lim_{N\to\infty} \frac{|I|}{N} = I(X; Y). \tag{1}$$

We define the cost function for costly channels as $C : \mathcal{X} \to R^+$, where $C(x)$ is cost for the symbol $x \in \mathcal{X}$. For a codeword of length N, we define the symbol frequency function $f_j : \mathcal{X}^N \to [0, 1]$ for $j \in \mathcal{X}$ as follows:

$$f_j(x^{1:N}) = \frac{1}{N} \sum_{i=1}^{N} \mathbb{1}(x_i = j).$$

III. Polar shaping code

A. Code construction

In this section, we provide shaping code that transforms uniformly distributed message $M^{1:|\mathcal{H}_X|}$ ($|\mathcal{H}_X|$ bits) into $X^{1:N}$, whose distribution is close to the distribution induced when $X^{1:N}$ is i.i.d. according to $p(x)$ in total variation distance. We assume that the alphabet $\mathcal{X}$ is binary in our polar code construction below.

Encoding
Input: uniformly distributed message $M^{1:|\mathcal{H}_X|}$ ($|\mathcal{H}_X|$ bits)
Output: codeword $X^{1:N}$
for $i = 1 : N$, set U_i as follows.
1. For $i \in \mathcal{H}_X$, the value of U_i is given by setting $U^{\mathcal{H}_X} = M^{1:|\mathcal{H}_X|}$.
2. For $i \in \mathcal{L}_X$, we set U_i using the **argmax rule**

$$U_i = \text{argmax}_{x \in \{0,1\}} P_{U_i|U^{1:i-1}}(x | U^{1:i-1}).$$

3. For $i \in R$, we set U_i by randomized rounding with the conditional distribution, $P_{U_i|U^{1:i-1}}(x | U^{1:i-1})$.

end
4. $X^{1:N} = U^{1:N} G_N$ becomes the codeword.

The decoding algorithm is as follows.

Decoding
Input: codeword $X^{1:N}$
Output: message estimate $M^{1:|\mathcal{H}_X|}$
1. We reconstruct $U^{1:N}$ by applying G_N to $X^{1:N}$.
2. Therefore $M^{1:|\mathcal{H}_X|} = U^{\mathcal{H}_X}$.

Let Q be the measure on $X^{1:N}$ induced by the polar shaping code. Note that P is the measure on $X^{1:N}$ induced when $X^{1:N}$ is i.i.d. distributed according to $p(x)$. From the results in [8] [6] [5], it is obvious that $||P_{X^{1:N}} - Q_{X^{1:N}}|| = O(2^{-N^{\beta}})$. Note that expected symbol frequency is as follows:

$$\mathbb{E}[f_j(X^{1:N})] = \frac{1}{N} \sum_{i=1}^{N} P(X_i = j).$$

We refer to the distribution given by expected symbol frequency function as symbol occurrence probability distribution for that block code. Let us call it $q_N(x)$. By using the fact that total variation distance $||P_{X^{1:N}} - Q_{X^{1:N}}|| = O(2^{-N^\beta})$, it can be easily shown that $q_N(x)$ approaches $p(x)$ as follows:

$$\begin{aligned} q_N(x) &= \frac{1}{N}\sum_{i=1}^{N} P(X_i = x) \\ &\leq \frac{1}{N}\sum_{i=1}^{N}(p(x) + ||P_{X^{1:N}} - Q_{X^{1:N}}||) \\ &= p(x) + O(2^{-N^\beta}). \end{aligned}$$

Similarly,

$$\begin{aligned} q_N(x) &= \frac{1}{N}\sum_{i=1}^{N} P(X_i = x) \\ &\geq \frac{1}{N}\sum_{i=1}^{N}(p(x) - ||P_{X^{1:N}} - Q_{X^{1:N}}||) \\ &= p(x) - O(2^{-N^\beta}). \end{aligned}$$

Hence $q_N(x)$ approaches $p(x)$ as N grows. Note that the polar shaping code we proposed is error free. As fraction of high-entropy bit-channels, where we provide message bits, approaches $H(X)$, we say that sequence of polar codes achieve any rate $R < H(X)$ with symbol occurrence distribution $p(x)$. The extension to the non-binary case can be done using ideas from [14].

B. *Application to costly channel*

Note the cost of a codeword $x^{1:N} \in \mathcal{X}^N$ per information bit $\bar{C}_N(x^{1:N}) = \frac{1}{R}\sum_{j\in\mathcal{X}} f_j(x^{1:N})C(j)$.
Therefore, the average cost per information bit of the shaping code will be as follows:

$$\begin{aligned} \mathbb{E}[\bar{C}_N(X^{1:N})] &= \frac{1}{R}\sum_{j\in\mathcal{X}} \mathbb{E}[f_j(X^{1:N})]C(j) \\ &= \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)q_N(x). \end{aligned}$$

Note that average cost per information bit, which we refer to as **total cost**, $\frac{1}{R}\sum_{x\in\mathcal{X}} C(x)q_N(x)$, for the sequence of polar codes, approaches the optimal value [10, Theorem 3], by choosing R close to $H(X)$, by choosing $p(x)$ as the symbol occurrence distribution characterized in [10, Theorem 3], which depends on the cost function. Hence, we say that the sequence of polar codes achieve optimal total cost.

IV. Shaping for DMCs

In this section, we consider shaping codes for DMCs characterized by transition probabilities $p(y|x)$.

A $(2^{NR}, N)$ code for a DMC consists of:

- message set: $\{1, 2, \ldots, 2^{NR}\}$,
- source of common randomness Z_N known to encoder and decoder independent of message,
- an encoder $X^{1:N} : \{1, 2, \ldots, 2^{NR}\} \times Z_N \to \mathcal{X}^N$ and
- a decoder at receiver $h : \mathcal{Y}^N \times Z_N \to \{1, 2, \ldots, 2^{NR}\}$.

R is the rate of the message. Let M be chosen uniformly from the set $\{1, 2, \ldots, 2^{NR}\}$. Let $Y^{1:N}$ be the received sequence. Note that we also employ common randomness in the definition of the code. Now we upper bound the rate that can be achieved on DMC with certain symbol occurrence probability distribution in following subsection.

A. *Upper bound on rate under a constraint on symbol occurrence distribution*

The upper bound we provide in this sub-section also applies to the case when $\mathcal{X}$ is non-binary alphabet. We refer to $q_N(x)$ and $\mathbb{E}[\bar{C}_N(X^{1:N})]$ for symbol occurrence distribution and total cost as defined in Section-III.

Definition: We say that R rate is achieved with symbol occurrence probability $p(x)$ iff there exists a sequence of $(2^{NR}, N)$ codes for discrete memoryless channels such that $P_e^N = \mathbb{P}(h(Y^{1:N}, Z_N) \neq M)$ vanishes and $q_N(x)$ approaches $p(x)$ as N goes to ∞.

Lemma 1. *If rate R is achieved with symbol occurrence probability $p(x)$, then $I(X;Y)$, mutual information evaluated at $p(x)$ for the DMC, will be an upper bound on R.*

Proof: Let us consider a sequence of $(2^{NR}, N)$ codes for which $q_N(x)$ approaches $p(x)$ and probability of error diminishes. By Fano's inequality, we get

$$H(M|Y^{1:N}, Z_N) = N\epsilon_N,$$

where ϵ_N vanishes as N grows. Let $\tilde{X}^N$ be the random variable distributed as $q_N(x)$.

$$\begin{aligned} NR &= H(M) \\ &= H(M) - H(M|Y^{1:N}Z_N) + H(M|Y^N Z_N) \\ &\leq H(M) - H(M|Y^{1:N}Z_N) + N\epsilon_N \\ &\overset{(a)}{=} H(M|Z_N) - H(M|Y^N Z_N) + N\epsilon_N \\ &= I(M;Y^{1:N}|Z_N) + N\epsilon_N \\ &= \sum_{i=1}^{N} I(M;Y_i|Z_N Y^{1:i-1}) + N\epsilon_N \\ &= \sum_{i=1}^{N}(H(Y_i|Y^{1:i-1}Z_N) - H(Y_i|M, Y^{1:i-1}, Z_N)) + N\epsilon_N \\ &\overset{(b)}{\leq} \sum_{i=1}^{N}(H(Y_i) - H(Y_i|M, Y^{1:i-1}, X_i, Z_N)) + N\epsilon_N \\ &\overset{(c)}{=} \sum_{i=1}^{N}(H(Y_i) - H(Y_i|X_i)) + N\epsilon_N \\ &= \sum_{i=1}^{N} I(X_i;Y_i) + N\epsilon_N \\ &\overset{(d)}{=} NI(\tilde{X}^N;Y) + N\epsilon_N \end{aligned}$$

where $I(\tilde{X}^N;Y)$ mutual information evaluated at distribution $q_N(x)$ for the DMC $p(y|x)$. Identity (a) follows as source of common randomness is independent of the message. Identity (b) follows as conditioning reduces entropy. Identity (c) follows as Y_i independent of $Y^{1:i-1}, Z_N$ given X_i. Identity

(d) follows as $q_N(x) = \frac{1}{N}\sum_{i=1}^{N} P(X_i = j)$ and mutual information is concave in input distribution for fixed $p(y|x)$.

As N approaches infinity, $I(\tilde{X}^N, Y)$ approaches $I(X;Y)$ since $q_N(x)$ approaches $p(x)$ and mutual information is continuous function with input distribution for fixed $p(y|x)$. Hence $R \leq I(X,Y)$. □

We use this result in the following subsection to define an optimization problem for the costly noisy DMC that provides a lower bound on the optimal total cost.

B. Lower bound on optimal total cost for costly noisy channel

Definition: We say that rate R is achieved with total cost $\tilde{C}$ iff there exists a sequence of $(2^{NR}, N)$ codes for discrete memoryless channels such that $P_e^N = \mathbb{P}(h(Y^{1:N}, Z_N) \neq M)$ vanishes and $\mathbb{E}[\bar{C}_N(X^{1:N})]$ approaches $\tilde{C}$ as N goes to ∞.

Definition: Optimal total cost C_{opt} is defined as follows:

$$C_{opt} = inf_{(R,\tilde{C})}\tilde{C},$$

where infimum is taken over $(R, \tilde{C})$ pairs such that R is achieved with total cost $\tilde{C}$.

Lemma 2. *The optimal total cost $C_{opt} = inf_{(R,p(x))}\tilde{C}$, where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$ and infimum is taken over $(R, p(x))$ pairs such that R is achieved with symbol occurrence distribution $p(x)$.*

Proof: We first provide the proof when $\mathcal{X}$ is binary alphabet. Without loss of generality assume that $C(0) \neq C(1)$ otherwise total cost is always equal to $\frac{C(0)}{R}$. Notice that there will be one to one correspondence between $q_N(x)$ and $\mathbb{E}[\bar{C}_N(X^{1:N})]$, which are affinely related. Hence $q_N(x)$ converges if and only if $\mathbb{E}[\bar{C}_N(X^{1:N})]$ converges as N goes to ∞. The limits are also affinely related by the same function as both the sequences are. Hence, R is achieved with total cost $\tilde{C}$ iff R is achieved with symbol occurrence distribution $p(x)$, where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$.

Therefore, $C_{opt} = inf_{(R,p(x))}\tilde{C}$, where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$ and infimum is taken over $(R, p(x))$ pairs such that R is achieved with symbol occurrence distribution $p(x)$.

When $\mathcal{X}$ is non-binary alphabet, total cost at rate can be same for two different distributions. So, this argument does not apply to non-binary case. We need to use the fact that every bounded sequence has convergent sub-sequence to prove that if rate R is achieved with total cost $\tilde{C}$ then there exist $p(x)$ such that rate R is achieved with symbol occurrence distribution $p(x)$ where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$.

If rate R is achieved with $\tilde{C}$ then there exists a sequence of $(2^{NR}, N)$ codes such that $P_e^N = \mathbb{P}(h(Y^{1:N}, Z_N) \neq M)$ vanishes and $\mathbb{E}[\bar{C}_N]$ approaches $\tilde{C}$ as N goes to ∞. The symbol occurrence distribution $q_N(x)$ may not converge. But there exists a sub-sequence of the sequence $q_N(x)$ that converges, as $q_N(x)$ is a bounded sequence. Let us index such a sub-sequence with k where block length corresponding to the kth element in the sub-sequence is N_k. Let $q_{N_k}(x)$ converges to the distribution $p(x)$. Clearly for sequence of codes $(2^{N_k R}, N_k)$, $\mathbb{E}[\bar{C}_{N_k}]$ approaches $\tilde{C}$ as k goes to ∞. As $\mathbb{E}[\bar{C}_{N_k}] = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)q_{N_k}(x)$, we will have $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$. Therefore we have sequence of codes for which probability of error diminishes and symbol occurrence probability distribution converges to $p(x)$ such that $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$, which means that if rate R is achieved with total cost $\tilde{C}$ then there exists a distribution $p(x)$ such that R rate is achieved with symbol occurrence distribution $p(x)$ where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$. On the other hand, if rate R is achieved with symbol occurrence probability distribution $p(x)$, then obviously rate R is achieved with total cost $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$.

Therefore, $C_{opt} = inf_{(R,p(x))}\tilde{C}$, where $\tilde{C} = \frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x)$ and infimum is taken over $(R, p(x))$ pairs such that R is achieved with symbol occurrence distribution $p(x)$. This concludes the proof of the lemma. □

As stated in the previous subsection, if rate R is achieved with symbol occurrence distribution $p(x)$, then $R < I(X;Y)$. Note that the solution for the following optimization problem is lower bound to C_{opt}.

$$\begin{gathered}\text{Minimize}_{(R,p(x))}\frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x),\\ \text{subject to } R \leq I(X;Y).\end{gathered} \tag{2}$$

In the next subsection, we show that polar coding technique designed for asymmetric channels can be used to achieve any rate $R < I(X;Y)$ with symbol occurrence probability $p(x)$. Therefore, the sequence of polar codes, which are designed with minimizers of the optimization problem achieve the lower bound provided by the solution of the optimization problem. This means that the solution of the optimization problem characterizes the optimal total cost of costly noisy DMCs.

We will now look at the solution of the optimization problem for M-ary costly erasure channel. M-ary erasure channel is a channel whose input alphabet size $|\mathcal{X}|$ is M where each input symbol is erased with certain probability.

Theorem 1. *The optimal symbol occurrence input distribution of the shaping code that achieves optimal total cost for an M-ary erasure costly channel with erasure probability ρ is given by $p^*(x) = 2^{-\mu C(x)}$ such that $\sum_{x\in\mathcal{X}} 2^{-\mu C(x)} = 1$. We assume that the cost function $C(x)$ is non-trivial for each $x \in \mathcal{X}$. The optimal total cost is given by $C_{opt} = \frac{\sum_{x\in\mathcal{X}} p^*(x)C(x)}{(1-\rho)\sum_{x\in\mathcal{X}} p^*(x)\log_2(1/p^*(x))}$.*

Proof: Mutual information $I(X;Y)$ evaluated at the input distribution $p(x)$ for the erasure channel is given by $(1-\rho)\sum_{i=1}^{N} p(x)\log_2(1/p(x))$. By substituting the mutual information in (2), optimization problem for the erasure costly channel for optimal total cost becomes as follows:

$$\text{Minimize}_{(R,p(x))}\frac{1}{R}\sum_{x\in\mathcal{X}} C(x)p(x),$$

$$\text{subject to } R \leq (1-\rho)\sum_{i=1}^{N} p(x)\log_2(1/p(x)).$$

For fixed rate R, finding out the symbol occurrence probability for minimum total cost will be a convex optimization problem. Using Lagrange duality, we get optimal symbol occurrence distribution at a fixed rate R as below:

$$\tilde{p}(x) = \frac{1}{N} 2^{-\mu C(x)},$$

where μ is a positive constant such that rate $R = (1-\rho)\sum_{i=1}^{N} \tilde{p}(x)\log_2(1/\tilde{p}(x))$ and N is normalization factor

$$N = \sum_{x\in\mathcal{X}} 2^{-\mu C(x)}.$$

Now minimizing total cost is equivalent to minimizing the following function:

$$G(\mu) = \frac{\sum_{x\in\mathcal{X}} C(x)2^{-\mu C(x)}}{(1-\rho)(\sum_{x\in\mathcal{X}} \mu C(x)2^{-\mu C(x)} + N\log_2 N)}$$

when $\mu > 0$. Notice that this function is same as function T defined in the proof of [10, Theorem 3] except for a factor $1-\rho$. The derivative $G'(\mu)$ will have negative of the sign of $\log_2 N$ as shown in the proof of [10, Theorem 3]. As we assume that $C(x) > 0$ for each $x \in \mathcal{X}$ and μ increases from 0 to ∞, N is decreasing from $|\mathcal{X}|$ to 0. So G will be initially decreasing as μ increases until N becomes 1 and then will be increasing. So the minimum value of G occurs when $N = 1$. Hence the optimal symbol occurrence distribution that achieves minimum total cost is $p^*(x) = 2^{-\mu C(x)}$ for each $x \in \mathcal{X}$ where $\sum_{x\in\mathcal{X}} 2^{-\mu C(x)} = 1$. Therefore optimal total cost will be $C_{opt} = \frac{\sum_{x\in\mathcal{X}} p^*(x)C(x)}{(1-\rho)\sum_{x\in\mathcal{X}} p^*(x)\log_2(1/p^*(x))}$. □

Now we provide the shaping polar code to achieve any rate $R < I(X;Y)$ with symbol occurrence probability distribution $p(x)$ over DMCs.

C. Polar shaping codes for DMCs

We assume alphabet $\mathcal{X}$ is binary in the proposed polar code construction. The polar code that we provide here transforms uniformly distributed message $M^{1:|I|}$ ($|I|$ bits) into codeword $X^{1:N}$, whose distribution is close to the distribution induced when $X^{1:N}$ is i.i.d. according to $p(x)$ in total variation distance. The code construction we propose here is actually derived from the capacity achieving polar codes for asymmetric channels [8] by Honda and Yamamoto. We use common randomness in the code construction to get the desired shaping property. Now we provide the encoding algorithm.

Encoding
Input: randomly chosen message $M^{1:|I|}$
Output: codeword $X^{1:N}$
for $i = 1 : N$, encode U_i as follows.
1. For $i \in I$, the value of U_i is given by setting $U^I = M^{1:|I|}$.
2. For $i \in F$, we set U_i as uniform independent random variable through common randomness.
3. For $i \in \mathcal{L}_X$, we encode U_i using the **argmax rule**

$$U_i = \text{argmax}_{x\in\{0,1\}} P_{U_i|U^{1:i-1}}(x|U^{1:i-1}).$$

4. For $i \in R$, we set U_i with conditional distribution $P_{U_i|U^{1:i-1}}(x|U^{1:i-1})$ using common randomness.

end
Transmit $X^{1:N} = U^{1:N}G_N$.

The decoding algorithm is as follows.

Decoding
Input: received vector $Y^{1:N}$
Output: message estimate $\hat{M}^{1:|I|}$
for $i = 1 : N$
1. If $i \in F$, we reconstruct $\hat{U}_i$ using common randomness, which is uniform independent random variable.
2. If $i \in \mathcal{L}_X \cup I$, set

$$\hat{U}_i = \text{argmax}_{x\in\{0,1\}} P_{U_i|U^{1:i-1},Y^{1:N}}(x|\hat{U}^{1:i-1}, Y^{1:N}).$$

3. If $i \in R$, we reconstruct $\hat{U}_i$ using common randomness with conditional distribution $P_{U_i|U^{1:i-1}}(x|\hat{U}^{1:i-1})$.

end
Decode $\hat{M} = \hat{U}^I$.

Let Q be the measure on $X^{1:N}$ induced by the polar shaping code. Note that P is the measure on $X^{1:N}$ induced when it is i.i.d. distributed according to $p(x)$. From the results in [8] [6] [5], it is obvious that $||P_{X^{1:N}} - Q_{X^{1:N}}|| = O(2^{-N^{\beta'}})$ for $\beta' < \beta < 0.5$. As mentioned in Section III, $q_N(x)$ approaches $p(x)$ as N grows large. The probability of decoding error is $O(2^{-N^{\beta'}})$ [8].

As fraction of information bit-channels, where we provide message bits, approaches $I(X;Y)$, the sequence of polar codes achieve rate $R < I(X;Y)$ with symbol occurrence distribution $p(x)$. Common randomness we employed in the code construction is crucial to get the desired distribution on the symbols of the codewords. If R and $p(x)$ in the polar code design are minimizers of the optimization problem proposed in the previous subsection, then sequence of polar codes clearly achieve the optimal total cost.

As proposed in [8] [12], instead of common-randomness, if we randomly produce frozen bits for bit-channels in F and boolean functions for encoding bit-channels in R, which are shared between encoder and decoder, then we will not be able to guarantee desired shaping distribution. The ensemble average symbol occurrence distribution has desired shaping distribution, but we should get code in the random ensemble with desired shaping distribution, which we cannot guarantee existence of. Nevertheless, for this random code construction that avoids common randomness, we still prove that there exists sequence of codes whose total cost approaches optimal total cost with diminishing probability of error if we design the polar code with minimizers of the optimization problem. Code constructions avoiding common randomness are advantageous as the practical implementation of common randomness uses pseudo-random generators which often have many limitations. They can suffer from shorter than the expected period for weak seed states.

Let $p^*(x)$ be optimal symbol occurrence distribution and R^* be the optimal rate for costly noisy DMC. Clearly, R^* is the mutual information evaluated at $p^*(x)$ for the DMC.

Now we design sequence of polar codes with optimal symbol occurrence distribution $p^*(x)$ and optimal rate R^* by random code construction method[2], as mentioned above avoiding common randomness. Let W_N denotes the random vector of frozen bits and boolean functions for bit-channels in F and R respectively. Note that the rate sequence $R_N = \frac{|I|}{N}$ approaches R^*. Clearly, the total cost for a given code will become as follows:

$$\begin{aligned}&\mathbb{E}[C_N(X^{1:N})|W_N]\\ &= \textstyle\sum_{x^{1:N}\in\mathcal{X}^{1:N}} 2^{-|I|}\Pi_{i\in F}\mathbb{1}\{f(i)=u_i\}\\ &\qquad \Pi_{i\in\mathcal{L}_X}\delta_i(u_i|u^{1:i-1})\\ &\qquad \Pi_{i\in R}\mathbb{1}\{\lambda_i(u^{1:i-1})=u_i\}C_N(x^{1:N}),\end{aligned}$$

where $x^{1:N} = u^{1:N}G_N$, $\mathbb{1}\{.\}$ is indicator function, $\delta_i(u|u^{1:i-1})$ denotes the conditional distribution induced by argmax rule for bit-channels in $\mathcal{L}_X$ as defined in [12], $f(.)$ is frozen bit function that is randomly chosen for bit-channels in F as defined in [12] and $\lambda_i(.)$ denotes the boolean functions to encode bit-channels in R as defined in [12].

Applying expectation on both sides and by the independence of frozen bits and boolean functions [8] [12], the ensemble average total cost becomes as follows:

$$\begin{aligned}&\mathbb{E}_{W_N}[\mathbb{E}[C_N(X^{1:N})|W_N]]\\ &= \textstyle\sum_{x^{1:N}\in\mathcal{X}^{1:N}} 2^{-|\mathcal{H}_X|}\Pi_{i\in\mathcal{L}_X}\delta_i(u_i|u^{1:i-1})\\ &\qquad \Pi_{i\in R}P_{U_i|U^{1:i-1}}(u_i|u^{1:i-1})C_N(x^{1:N}).\\ &= \textstyle\sum_{x^{1:N}\in\mathcal{X}^{1:N}} Q(x^{1:N})C_N(x^{1:N}).\end{aligned}$$

This implies that

$$\mathbb{E}_{W_N}[\mathbb{E}[C_N(X^{1:N})|W_N]] = \frac{N}{|I|}\textstyle\sum_{x\in\mathcal{X}} C(x)q_N(x).$$

Therefore, as $q_N(x)$ approaches $p^*(x)$ and $\frac{|I|}{N}$ approaches R^*, ensemble average total cost $\mathbb{E}_{W_N}[\mathbb{E}[C_N(X^{1:N})|W_N]]$ approaches $\frac{1}{R^*}\sum_{x\in\mathcal{X}} C(x)p^*(x)$ which is optimal total cost C_{opt}. On the other hand, the ensemble average probability of error $\mathbb{E}_{W_N}[P_e(W_N)] = O(2^{-N^{\beta'}})$ [8] where $\beta' < \beta < 0.5$ and $P_e(W_N)$ is the probability of error of the given code. A good shaping code has total cost close to the optimal value and negligible probability of error. So we should show there exists a sequence of codes whose total cost approaches optimal total cost and probability of error diminishes. We show the existence of such codes with high probability. We precisely state our result in Theorem 2 followed by a rigorous proof. For the sake of brevity, we denote $\mathbb{E}[C_N(X^{1:N})|W_N]$ as T_N.

Theorem 2. *In the above random code construction, the sequence $\mathbb{P}\big(P_e(W_N) < N2^{-N^{\beta'}}, \tilde{b}_N\mathbb{E}_{W_N}[T_N] \leq T_N \leq \tilde{a}_N\mathbb{E}_{W_N}[T_N]\big)$ approaches 1 for some $\tilde{a}_N > 1$ and $\tilde{b}_N < 1$ that converge to 1. This means that, with high probability, there exist codes in the random ensemble with total cost approaching the optimal total cost and diminishing probability of error.*

Proof: We first prove that $\mathbb{P}(b_N\mathbb{E}_{W_N}[T_N] \leq T_N \leq a_N\mathbb{E}_{W_N}[T_N])$ goes to 1 for any b_N that converges to $b < 1$ from below and a_N that converges to $a > 1$ from above. This is equivalent to proving $\mathbb{P}(T_N > a_N\mathbb{E}_{W_N}[T_N])$ converges to zero and $\mathbb{P}(T_N < b_N\mathbb{E}_{W_N}[T_N])$ converges to zero. For the sake of brevity, we denote $\mathbb{E}_{W_N}[T_N]$ as $\tilde{\mathbb{E}}[T_N]$ in the proof.

Now we prove $\mathbb{P}(T_N > a_N\tilde{\mathbb{E}}[T_N])$ converges to zero by contradiction. So we assume there is subsequence indexed by r, $\mathbb{P}(T_{N_r} > a_{N_r}\tilde{\mathbb{E}}[T_{N_r}])$, whose liminf is non-zero. Let us denote the sequence $\mathbb{P}(T_{N_r} > a_{N_r}\tilde{\mathbb{E}}[T_{N_r}])$ as p_{N_r}. Note that limsup of sequence p_{N_r} is less than 1, as p_{N_r} is upper-bounded by $1/a_{N_r}$, by the Markov inequality. As $a_{N_r} > 1$, we will be able to choose $0 \leq l_{N_r} < 1$ such that $\tilde{\mathbb{E}}[T_{N_r}] = p_{N_r}a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]+(1-p_{N_r})l_{N_r}\tilde{\mathbb{E}}[T_{N_r}]$ with limsup of l_{N_r} less than 1. Set $l'_{N_r} = \frac{1+l_{N_r}}{2}$. Therefore, $\tilde{\mathbb{E}}[T_{N_r}] < p_{N_r}a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]+(1-p_{N_r})l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}]$ and limsup of l'_{N_r} is less than 1. Note that

$$\tilde{\mathbb{E}}[T_{N_r}]=p_{N_r}a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]+(1-p_{N_r}-q_{N_r})l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}] \qquad (3)$$

where $q_{N_r} = (1-p_{N_r})\frac{1-l_{N_r}}{1+l_{N_r}}$, and liminf of q_{N_r} does not vanish as the limsups of l_{N_r} and p_{N_r} are less than 1.

Note also that

$$\begin{aligned}\tilde{\mathbb{E}}[T_{N_r}] &\geq p_{N_r}a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]\\ &\quad +\mathbb{P}(l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}]\leq T_{N_r}\leq a_{N_r}\tilde{\mathbb{E}}[T_{N_r}])l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}].\end{aligned}$$

By plugging in for $\tilde{\mathbb{E}}[T_{N_r}]$ using equation (3), we get

$$\mathbb{P}(l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}]\leq T_{N_r}\leq a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]) \leq (1-p_{N_r}-q_{N_r}).$$

This yields

$$\begin{aligned}&\mathbb{P}(T_{N_r} < l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}]) = 1-\mathbb{P}(l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}]\leq T_{N_r}\leq a_{N_r}\tilde{\mathbb{E}}[T_{N_r}])\\ &-\mathbb{P}(T_{N_r}>a_{N_r}\tilde{\mathbb{E}}[T_{N_r}]) \geq 1-(1-p_{N_r}-q_{N_r})-p_{N_r} = q_{N_r}.\end{aligned}$$

Hence q_{N_r} is a lower-bound to $\mathbb{P}(T_{N_r}<l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}])$. Hence $\mathbb{P}(T_{N_r}<l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}])$ does not converge to zero. As $\mathbb{P}(P_e < N_r2^{-N_r^{\beta'}})$ converges to 1, it follows that the sequence $\mathbb{P}(P_e < N_r2^{-N_r^{\beta'}}, T_{N_r} < l'_{N_r}\tilde{\mathbb{E}}[T_{N_r}])$ does not converge to zero. As limsup of l'_{N_r} is less than 1, we can get a sequence of codes whose total costs converge to less than optimal total cost C_{opt} with diminishing probability of error. This is a contradiction. Hence $\mathbb{P}(T_N > a_N\tilde{\mathbb{E}}[T_N])$ converges to zero.

Now we prove that $\mathbb{P}(T_N < b_N\tilde{\mathbb{E}}[T_N])$ converges to zero. We again prove this by contradiction. So assume $\mathbb{P}(T_N < b_N\tilde{\mathbb{E}}[T_N])$ does not converge to zero. As $\mathbb{P}(P_e < N2^{-N^{\beta'}})$ converges to 1, the sequence $\mathbb{P}(P_e < N2^{-N^{\beta'}}, T_N < b_N\tilde{\mathbb{E}}[T_N])$ does not converge to zero. This is a contradiction as we can get a sequence of codes whose total costs converge to less than optimal total cost C_{opt} with diminishing probability of error. Hence $\mathbb{P}(T_N < b_N\tilde{\mathbb{E}}[T_N])$ converges to zero.

We conclude $\mathbb{P}(b_N\tilde{\mathbb{E}}[T_N] \leq T_N \leq a_N\tilde{\mathbb{E}}[T_N])$ goes to 1. As $\mathbb{P}(P_e < N2^{-N^{\beta'}})$ converges to 1, we will have $\mathbb{P}(P_e < N2^{-N^{\beta'}}, b_N\tilde{\mathbb{E}}[T_N] \leq T_N \leq a_N\tilde{\mathbb{E}}[T_N])$ goes to 1.

Let $\hat{a}_m > 1$ be a sequence indexed by m that converges to 1 from above. Let $\hat{b}_m < 1$ be a sequence indexed by m that converges to 1 from below. For each m, let us define a sequence $\hat{a}_{mN}$ that converges to $\hat{a}_m$ from above and also define another sequence $\hat{b}_{mN}$ that converges to $\hat{b}_m$ from below. So for each m, we have

[2]J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Trans. Inf. Theory,* vol. 59, no. 12, pp. 7829–7838, Dec. 2013.

$\mathbb{P}(P_e < N2^{-N^{\beta'}}, \hat{b}_{mN}\tilde{\mathbb{E}}[T_N] \leq T_N \leq \hat{a}_{mN}\tilde{\mathbb{E}}[T_N])$ goes to 1. Notice that $\mathbb{P}(P_e < N2^{-N^{\beta'}}, \hat{b}_{NN}\tilde{\mathbb{E}}[T_N] \leq T_N \leq \hat{b}_{NN}\tilde{\mathbb{E}}[T_N])$ goes to 1 where both $\hat{b}_{NN} < 1$ and $\hat{a}_{NN} > 1$ converge to 1. By setting $\tilde{a}_N = \hat{a}_{NN}$ and $\tilde{b}_N = \hat{b}_{NN}$, we complete the proof of the theorem. □

The extension to non-binary case can be done using ideas in [14].

V. Conclusion

We presented a polar shaping code. For a costly channel, we have shown that total cost of the proposed polar shaping code approaches optimal total cost as block length grows. We looked at costly noisy discrete memoryless channels. We first give an upper bound on the rate that can be achieved with certain symbol occurrence probability distribution over a discrete memoryless channel. We formulated an optimization problem whose solution gives optimal total cost for the costly noisy discrete memoryless channel. We showed that polar codes for asymmetric channels by Honda and Yamamoto with the aid of common randomness can be used to get the desired shaping distribution on symbols of the codewords. To achieve the optimal total cost, we show that we can also use random construction method by randomly choosing frozen bits and randomly choosing boolean functions for not completely polarized channels [12] [8] avoiding common randomness.

VI. Acknowledgement

We would like to thank Samsung for supporting this work.

References

[1] E. Arıkan, “Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory,* vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[2] E. Arıkan, “Source polarization,” *Proc. IEEE Int. Symp. Inf. Theory (ISIT),* Austin, TX, Jun. 13-18, 2010, pp. 899–903.

[3] G. Böcherer, “Capacity-achieving probabilistic shaping for noisy and noiseless channels,” *Ph.D. dissertation, RWTH Aachen University, 2012* [Online]. Available: http://www.georg-boecherer.de/capacityAchievingShaping.pdf

[4] G. Böcherer, F. Steiner and P. Schulte, “Bandwidth efficient and rate-matched low-density parity-check coded modulation,” *IEEE Trans. Commmun.*, vol. 63, no. 12, pp. 4651–4665, Dec. 2015.

[5] R. A. Chou and M. R. Bloch “Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes,” *Proc. 53rd Annu. Allerton Conf. on Commun., Control, and Computing,* Monticello, IL, Sep. 2015, pp. 1380–1385.

[6] E. En Gad, Y. Li, J. Kliewer, M. Langberg, A. A. Jiang and J. Bruck, “Asymmetric error correction and flash-memory rewriting using polar codes,” *IEEE Trans. Inf. Theory,* vol. 62, no. 7, pp. 4024–4038, Jul. 2016.

[7] R. F. H. Fischer, *Precoding and Signal Shaping for Digital Transmission*. Hoboken, NJ, USA: Wiley, 2002.

[8] J. Honda and H. Yamamoto, “Polar coding without alphabet extension for asymmetric models,” *IEEE Trans. Inf. Theory,* vol. 59, no. 12, pp. 7829–7838, Dec. 2013.

[9] A. Lenz, Y. Liu, C. Rashtchian, P. H. Siegel, A. Wachter-Zeh and E. Yaakobi, “Coding for efficient DNA synthesis,” *IEEE Int. Symp. Inf. Theory (ISIT),* Los Angeles, CA, Jun. 21-26, 2020, pp. 2885–2890.

[10] Y. Liu, P. Huang, A. W. Bergman and P. H. Siegel, “Rate-constrained shaping codes for structured sources,” *IEEE Trans. Inf. Theory,* vol. 66, no. 8, pp. 5261-5281, Aug. 2020.

[11] T. Matsumine, T. Koike-Akino, D. S. Millar, K. Kojima and K. Parsons, “Polar coded modulation for joint channel coding and probabilistic shaping,” *Proc. Optical Fiber Commun. Conf. (OFC)*, San Diego, CA, Mar. 3-7, 2019, pp. 1–3.

[12] K. Nagarjuna and P. H. Siegel, “Universal polar coding for asymmetric channels,” *Proc. IEEE Inf. Theory Workshop (ITW)*, Guangzhou, China, Nov. 25-29, 2018, pp. 1–5.

[13] T. Prinz et al., “Polar coded probabilistic amplitude shaping for short packets,” *Proc. IEEE 18^{th} Int. Workshop on Sign. Proc. Advances in Wireless Commun. (SPAWC)*, Sapporo, Japan, Jul. 3-6, 2017, pp 1–5.

[14] E. Şaşoğlu, E. Telatar and E. Arıkan, “Polarization for arbitrary discrete memoryless channels,” *Proc. IEEE Inf. Theory Workshop (ITW),* Taormina, Italy, Oct. 11-16, 2009, pp. 144–148.

[15] C. E. Shannon, “A mathematical theory of communication, Part I, Part II," *Bell Syst. Tech. J.,* vol. 27, pp. 379–423, 1948.