On the Construction of Polar Codes for Channels with Moderate Input Alphabet Sizes

Ido Tal
Department of Electrical Engineering,
Technion, Haifa 32000, Israel.
Email: idotal@ee.technion.ac.il

***Abstract*—Current deterministic algorithms for the construction of polar codes cannot be argued to be practical for channels with input alphabets of moderate size. In this paper, we show that any construction algorithm which follows the paradigm of "degrading after each polarization step" will inherently be impractical with respect to a certain "hard" underlying channel having an input alphabet of moderate size. This result also sheds light on why the construction of LDPC codes using density evolution is impractical for channels with moderate sized input alphabets.**

***Index Terms*—Polar codes, construction, degrading cost.**

I. INTRODUCTION

Polar codes [1] are a novel family of error correcting codes which are capacity achieving and have efficient encoding and decoding algorithms. Originally defined for channels with binary input, they were soon generalized to channels with arbitrary input alphabets [2].

The construction of a polar code is essentially equivalent to the selection of "almost noiseless" channels out of a pool of n synthesized channels, where n is the code length. Since the synthesized channels have an output alphabet size which grows exponentially in the code length n, calculating their symbol error rates is intractable if approached directly. To the author's knowledge, currently, the only tunable and deterministic methods of circumventing this difficulty involve approximating some of the intermediate channels by channels which have a manageable output alphabet size. Simply put: before the first polarization step and after each polarization step (up to a certain point), approximate the relevant channel by another channel having a prescribed output alphabet size.

The above "approximate after each polarization step" idea has its origins in density evolution [3, Page 217]. Density evolution was suggested as a method of constructing polar codes in [4]. In order to bound the symbol error rate of a synthesized channel — as opposed to only approximating it — one can force the approximating channel to be either degraded or upgraded with respect to the synthesized channel we are trying to approximate. An efficient algorithm for such a degrading/upgrading approximation was introduced for the binary-input case in [5] and analyzed in [6]. See also [7] for an optimal degrading algorithm. Algorithms for degrading and upgrading for the case in which the channel does not have a binary input were given in [8] and [9], respectively. See also [10]. In the case of a symmetric underlying channel and a symmetric input distribution, a degraded approximation is enough in order to derive a lower bound on the probability of error. For simplicity of exposition, assume that we are dealing with this case. On a related note, the construction of polar codes was recently proven to be polynomial [11], for an arbitrary but *fixed* input alphabet size.

For a fixed input distribution, a degrading approximation results in a channel with reduced mutual information between input and output. This drop in mutual information should ideally be kept small. That is, consider the synthesized channels that are descendants of the approximating channel. The percentage of these synthesized channels which the construction algorithm will designate as "almost noiseless" is upper bounded by the mutual information of the approximating channel.

Let q denote the input alphabet size. Think of q as being not too small, say $q \geq 11$. In this paper, we specify a channel which is "hard to degrade". Namely, in order to ensure a drop in mutual information of at most ϵ, the size of the output alphabet of the approximating channel must be at least proportional to $(1/\epsilon)^{\frac{q-1}{2}}$, with respect to *any degrading algorithm*. Namely, if we are to ensure a drop of at most ϵ in mutual information, we must approximate by a channel with an output alphabet size at least *exponential in the input alphabet size*, the exponent being $1/\sqrt{\epsilon}$.

On a related note, we mention that if the quantization operation in density evolution (a method of constructing LDPC codes) is a degrading one, then the same problem manifests itself. Namely, there are cases in which the quantization is necessarily a bad approximation of the corresponding channel (much smaller mutual information), when only a manageable number of quantization levels are allowed, and no matter how well the quantizer is constructed.

II. NOTATION AND PROBLEM STATEMENT

We denote a channel by $W\colon \mathcal{X} \to \mathcal{Y}$. The probability of receiving $y \in \mathcal{Y}$ given that $x \in \mathcal{X}$ was transmitted over W is denoted $W(y|x)$. All our channels will be defined over a finite input alphabet $\mathcal{X}$, with size $q = |\mathcal{X}|$. Unless specifically stated otherwise, all channels will have a finite output alphabet, denoted $\mathrm{out}(W) = \mathcal{Y}$. Thus, the channel output alphabet size is denoted $|\mathrm{out}(W)|$.

Each channel will typically have a corresponding input distribution, denoted $P_X = P_X^{(W)}$. Note that P_X *need not* necessarily be the input distribution achieving the capacity of

W. We denote the random variables corresponding to the input and output of W by $X = X^{(W)}$ and $Y = Y^{(W)}$, respectively. The distribution of Y is denoted $P_Y = P_Y^{(W)}$. That is, for $y \in \mathcal{Y}$,

$$P_Y(y) = \sum_{x \in \mathcal{X}} P_X(x) W(y|x) \; .$$

The mutual information between X and Y is denoted as

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

and is henceforth measured in nats. That is, all logarithms henceforth are natural. Note that $I(W)$ typically *does not* equal the capacity of W.

We say that a channel $Q\colon \mathcal{X} \to \mathcal{Z}$ is (stochastically) degraded with respect to $W\colon \mathcal{X} \to \mathcal{Y}$ if there exists a channel $\Phi\colon \mathcal{Y} \to \mathcal{Z}$ such that the concatenation of Φ to W yields Q. Namely, for all $x \in \mathcal{X}$ and $z \in \mathcal{Z}$,

$$Q(z|x) = \sum_{y \in \mathcal{Y}} W(y|x) \Phi(z|y) \; . \tag{1}$$

We denote Q being degraded with respect to W as $Q \prec W$.

For input alphabet size $q = |\mathcal{X}|$ and specified output alphabet size L, define the *degrading cost* as

$$\mathrm{DC}(q, L) \triangleq \sup_{W, P_X} \min_{\substack{Q \,:\, Q \prec W, \\ |\mathrm{out}(Q)| \leq L}} \left(I(W) - I(Q) \right) \; . \tag{2}$$

Namely, both W and Q range over channels with input alphabet $\mathcal{X}$ such that $|\mathcal{X}| = q$; both channels share the same input distribution P_X, which we optimize over; the channel Q is degraded with respect to W; both channels have finite output alphabets and the size of the output alphabet of Q is at most L; we calculate the drop in mutual information incurred by degrading W to Q, for the "hardest" channel W and its best approximation Q.

The use of "min" instead of "inf" is justified in (2) by the following claim, which is taken from [7, Lemma 1].

Claim 1: Let $W\colon \mathcal{X} \to \mathcal{Y}$ and P_X be given. Let $L \geq 1$ be a specified integer for which $|\mathcal{Y}| \geq L$. Then,

$$\inf_{\substack{Q \,:\, Q \prec W, \\ |\mathrm{out}(Q)| \leq L}} \left(I(W) - I(Q) \right)$$

is attained by a channel $Q\colon \mathcal{X} \to \mathcal{Z}$ for which it holds that $|\mathrm{out}(Q)| = L$ and

$$Q(z|x) = \sum_{y \in \mathcal{Y}} W(y|x) \Phi(z|y) \; , \quad \Phi(z|y) \in \{0, 1\} \; ,$$

$$\sum_{z \in \mathcal{Z}} \Phi(z|y) = 1 \; .$$

Namely, Q is gotten from W by defining a partition $(A_i)_{i=1}^L$ of $\mathcal{Y}$ and mapping with probability 1 all symbols in A_i to a single symbol $z_i \in \mathcal{Z}$, where $\mathcal{Z} = \{z_i\}_{i=1}^L$.

In [8], an upper bound on $\mathrm{DC}(q, L)$ is derived. Specifically,

$$\mathrm{DC}(q, L) \leq 2q \cdot \left(\frac{1}{L} \right)^{1/q} \; .$$

This bound is constructive and stems from a specific quantizing algorithm. Note that for a fixed input alphabet size q and a target difference ϵ such that $\mathrm{DC}(q, L) \leq \epsilon$, the above implies that we take $L = \lceil (2q/\epsilon)^q \rceil$. Namely, for say $\epsilon = 10^{-2}$, this algorithm can only be proved to be effective for rather small values of q, since the computational hardware must somehow store the probabilities associated with the L output letters.

Our aim is to derive a lower bound on $\mathrm{DC}(q, L)$. Let σ_{q-1} be the constant for which the volume of a sphere in $\mathbb{R}^{q-1}$ of radius r is $\sigma_{q-1} r^{q-1}$. The following is our main result.

Theorem 2: Let q and L be specified. Then,

$$\mathrm{DC}(q, L) \geq \frac{q-1}{2(q+1)} \cdot \left(\frac{1}{\sigma_{q-1} \cdot (q-1)!} \right)^{\frac{2}{q-1}} \cdot \left(\frac{1}{L} \right)^{\frac{2}{q-1}} \; . \tag{3}$$

Thus, for a prescribed ϵ, the need to take very large L for moderate values of q is not an artifact of the algorithm presented in [8]: an optimal quantizing algorithm will have this problem as well, for certain hard channels W. Namely, L must be at least proportional to $(1/\epsilon)^{\frac{q-1}{2}}$.

III. Preliminary lemmas

As a consequence of the data processing inequality, if Q is degraded with respect to W, then $I(W) - I(Q) \geq 0$. In this section, we derive a tighter lower bound on the difference. To that end, let us first define $\eta(p)$ as

$$\eta(p) = -p \cdot \ln p \; , \quad 0 \leq p \leq 1 \; ,$$

where $\eta(0) = 0$. Next, for a probability vector $\mathbf{p} = (p_x)_{x \in \mathcal{X}}$, define

$$h(\mathbf{p}) = \sum_{x \in \mathcal{X}} -p_x \cdot \ln p_x = \sum_{x \in \mathcal{X}} \eta(p_x) \; .$$

For $A = \{y_1, y_2, \ldots, y_t\} \subseteq \mathcal{Y}$, define the quantity $\Delta(A)$ as the decrease in mutual information resulting from merging all symbols in A into single symbol in Q. Namely, define

$$\Delta(A) \triangleq \pi \left(h\left[\sum_{j=1}^{t} \theta_j \mathbf{p}^{(j)} \right] - \left(\sum_{j=1}^{t} \theta_j h\left[\mathbf{p}^{(j)} \right] \right) \right) \; , \tag{4}$$

where

$$\pi = \sum_{y \in A} P_Y(y) \; , \quad \theta_j = P_Y(y_j)/\pi \; , \tag{5}$$

and

$$\mathbf{p}^{(j)} = \left(P(X = x | Y = y_j) \right)_{x \in \mathcal{X}} \; . \tag{6}$$

The following claim is easily derived.

Claim 3: Let W, Q, P_X, L, and $(A_i)_{i=1}^L$ be as in Claim 1. Then,

$$I(W) - I(Q) = \sum_{i=1}^{L} \Delta(A_i) \; . \tag{7}$$

As mentioned, by the concavity of h and Jensen's inequality, we deduce that $\Delta(A_i) \geq 0$. Namely, data processing reduces mutual information. We will shortly make use of the fact that h is strongly concave in order to derive a sharper lower bound. To that end, we now state Hölder's defect formula [12] (see [13, Page 94] for an accessible reference).

As is customary, we will phrase Hölder's defect formula for $\cup$-convex functions, although we will later apply it to h which is $\cap$-concave. We remind the reader that for twice differentiable $\cup$-convex functions, $f\colon D \to \mathbb{R}$, $D \subseteq \mathbb{R}^n$ the Hessian of f, denoted $\nabla^2 f(\alpha) = \left(\frac{\partial^2 f(\alpha)}{\partial\alpha_i \partial\alpha_j}\right)_{i,j}$, is positive semidefinite on the interior of D [14, page 71]. We denote the smallest eigenvalue of $\nabla^2 f(\alpha)$ by $\lambda_{\min}(\nabla^2 f(\alpha))$.

Lemma 4: Let $f(\alpha)\colon D \to \mathbb{R}$ be a twice differentiable convex function defined over a convex domain $D \subseteq \mathbb{R}^n$. Let $m \geq 0$ be such that for all α in the interior of D,

$$m \leq \lambda_{\min}(\nabla^2 f(\alpha))$$

Fix $(\alpha_j)_{j=1}^t \in D$ and let $(\theta_j)_{j=1}^t$ be non-negative coefficients summing to 1. Denote

$$\overline{\alpha} = \sum_{j=1}^t \theta_j \alpha_j$$

and

$$\delta^2 = \sum_{j=1}^t \theta_j \left\| \alpha_j - \overline{\alpha} \right\|_2^2 = \frac{1}{2} \sum_{j=1}^t \sum_{k=1}^t \theta_j \theta_k \left\| \alpha_j - \alpha_k \right\|_2^2$$

Then,

$$\sum_{j=1}^t \theta_j f[\alpha_j] - f[\sum_j \theta_j \alpha_j] \geq \frac{1}{2} m \delta^2 \ .$$

We now apply Hölder's inequality in order to bound $\Delta(A)$. For $A = \{y_1, y_2, \ldots, y_t\} \subseteq \mathcal{Y}$, define

$$\tilde{\Delta}(A) \triangleq \frac{\pi}{2} \sum_{j=1}^t \theta_j \left\| \mathbf{p}^{(j)} - \bar{\mathbf{p}} \right\|_2^2 = \frac{\pi}{4} \sum_{j=1}^t \sum_{k=1}^t \theta_j \theta_k \left\| \mathbf{p}^{(j)} - \mathbf{p}^{(k)} \right\|_2^2 \ , \quad (8)$$

where π and θ_j are as in (5), $\mathbf{p}^{(j)}$ is as defined in (6), and

$$\bar{\mathbf{p}} = \sum_{j=1}^t \theta_j \mathbf{p}(j) \ .$$

The following is a simple corollary of Lemma 4

Corollary 5: Let W, Q, P_X, L, and $(A_i)_{i=1}^L$ be as in Claim 1. Then, for all $1 \leq i \leq L$,

$$\Delta(A_i) \geq \tilde{\Delta}(A_i) \ . \quad (9)$$

Thus,

$$I(W) - I(Q) \geq \sum_{i=1}^L \tilde{\Delta}(A_i) \ . \quad (10)$$

IV. Bounding the degrading cost

We now turn to bounding the degrading cost. As a first step, we define a channel W for which we will prove a lower bound on the cost of degrading. That is, we show that W is "hard" to degrade.

A. The channel W

For a specified integer $M \geq 1$, we now define the channel $\mathsf{W} = \mathsf{W}_M$, where $\mathsf{W}\colon \mathcal{X} \to \mathcal{Y}$. The input alphabet is $\mathcal{X} = \{1, 2, \ldots, q\}$, of size $|\mathcal{X}| = q$. The output alphabet consists of vectors of length q with integer entries, defined as follows:

$$\mathcal{Y} = \Big\{ \langle j_1, j_2, \ldots, j_q \rangle : j_1, j_2, \ldots, j_q \geq 0 \ , \quad \sum_{x=1}^q j_x = M \Big\} \ . \quad (11)$$

The channel transition probabilities are given by

$$\mathsf{W}(\langle j_1, j_2, \ldots, j_q \rangle | x) = \frac{q \cdot j_x}{M\binom{M+q-1}{q-1}} \ .$$

Lemma 6: The above defined W is a valid channel with output alphabet size

$$|\mathrm{out}(\mathsf{W})| = \binom{M+q-1}{q-1} \ . \quad (12)$$

We take the corresponding input distribution as symmetric. Namely, for all $x \in \mathcal{X}$,

$$P(X = x) = \frac{1}{q} \ .$$

As a result, all output letters are equally likely.

Denote the vector of a posteriori probabilities corresponding to $\langle j_1, j_2, \ldots, j_q \rangle$ as

$$\mathbf{p}(j_1, j_2, \ldots, j_q) = (\ P(X = x | Y = \langle j_1, j_2, \ldots, j_q \rangle)\ )_{x=1}^q \ .$$

A short calculation gives

$$\mathbf{p}(j_1, j_2, \ldots, j_q) = \left(\frac{j_1}{M}, \frac{j_2}{M}, \ldots, \frac{j_q}{M} \right) \ . \quad (13)$$

In light of the above, let us define the shorthand

$$\langle j_1, j_2, \ldots, j_q \rangle \triangleq (j_1/M, j_2/M, \ldots, j_q/M) \ .$$

With this shorthand in place, the label of each output letter $\langle j_1, j_2, \ldots, j_q \rangle \in \mathcal{Y}$ is the corresponding a posteriori probability vector $\mathbf{p}(j_1, j_2, \ldots, j_q)$. Thus, we gain a simple expression for $\tilde{\Delta}(A)$. Namely, for $A \subseteq \mathcal{Y}$,

$$\tilde{\Delta}(A) = \frac{1}{2\binom{M+q-1}{q-1}} \sum_{\mathbf{p} \in A} \left\| \mathbf{p} - \bar{\mathbf{p}} \right\|_2^2 \ , \quad \bar{\mathbf{p}} = \sum_{\mathbf{p} \in A} \frac{1}{|A|} \mathbf{p} \ .$$

We remark in passing that as $M \to \infty$, W "converges" to the channel $\mathcal{W}_q\colon \mathcal{X} \to \mathcal{X} \times [0,1]^q$ which we now define. Given an input x, the channel picks $\varphi_1, \varphi_2, \ldots, \varphi_q$ as follows: $\varphi_1, \varphi_2, \ldots, \varphi_{q-1}$ are picked according to the Dirichlet distribution $D(1, 1, \ldots, 1)$, while φ_q is set to $1 - \sum_{x=1}^{q-1} \varphi_x$. Then, the input x is transformed into $x + i$ (with a modulo operation where appropriate[1]) with probability φ_i. The transformed symbol along with the vector $(\varphi_1, \varphi_2, \ldots, \varphi_q)$ is the output of the channel.

[1]To be precise, x is transformed into $1 + (x - 1 + i \mod q)$.

B. Optimizing A'

Our aim is to find a lower bound on $\tilde{\Delta}(A)$, where $A \subseteq \mathcal{Y}$ is constrained to have a size $|A| = t$. Recalling (13), note that all output letters $\mathbf{p} = (p_x)_{x=1}^{q} \in \mathcal{Y}$ must satisfy the following three properties.

1) All entries p_x are of the form j_x/M, where j_x is an integer.
2) All entries p_x sum to 1.
3) All entries p_x are non-negative.

Since all entries must sum to 1 by property 2, entry p_q is redundant. Thus, for a given $\mathbf{p} \in \mathcal{Y}$, denote by $\mathbf{p}'$ the first $q-1$ coordinates of $\mathbf{p}$. Let A' be the set one gets by applying this puncturing operation to each element of A. Denote

$$\tilde{\Delta}(A') \triangleq \frac{1}{2\binom{M+q-1}{q-1}} \sum_{\mathbf{p}' \in A'} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \ , \tag{14}$$

One easily shows that

$$\tilde{\Delta}(A') \leq \tilde{\Delta}(A) \ , \tag{15}$$

thus a lower bound on $\tilde{\Delta}(A')$ is also a lower bound on $\tilde{\Delta}(A)$.

In order to find a lower bound on $\tilde{\Delta}(A')$ we relax constraint 3 above. Namely, a set A' with elements $\mathbf{p}'$ will henceforth mean a set for which each element $\mathbf{p}' = (p_x)_{x=1}^{q-1}$ has entries of the form $p_x = j/M$, and each such entry is *not* required to be non-negative. Our revised aim is to find a lower bound on $\tilde{\Delta}(A')$ where A' holds elements as just defined and is constrained to have size t. The simplification enables us to give a characterization of the optimal A'. Informally, a sphere, up to irregularities on the boundary.

Lemma 7: Let $t > 0$ be a given integer. Let A' be the set of size $|A'| = t$ for which $\tilde{\Delta}(A')$ is minimized. Denote by $\bar{\mathbf{p}}'$ the mean of all elements of A'. Then, A' has a critical radius r: all $\mathbf{p}'$ for which $\|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 < r^2$ are in A' and all $\mathbf{p}'$ for which $\|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 > r^2$ are not in A'.

Proof: We start by considering a general A'. Suppose $\mathbf{p}'(1) \in A'$ is such that $r^2 = \|\mathbf{p}'(1) - \bar{\mathbf{p}}'\|_2^2$. Next, suppose that there is a $\mathbf{p}'(2) \notin A'$ such that $\|\mathbf{p}'(2) - \bar{\mathbf{p}}'\|_2^2 < r^2$. Then, for

$$B' = A' \cup \{\mathbf{p}'(2)\} \setminus \{\mathbf{p}'(1)\} \ , \quad \tilde{\Delta}(B') < \tilde{\Delta}(A') \ .$$

To see this, first note that

$$\sum_{\mathbf{p}' \in B'} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 < \sum_{\mathbf{p}' \in A'} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \ . \tag{16}$$

Next, note that the RHS of (16) is $\tilde{\Delta}(A')$, but the LHS is *not* $\tilde{\Delta}(B')$. Namely, $\bar{\mathbf{p}}'$ is the mean of the vectors in A' but is not the mean of the vectors in B'. However, $\sum_{\mathbf{p}' \in B'} \|\mathbf{p}' - \mathbf{u}'\|_2^2$ is minimized for $\mathbf{u}'$ equal to the mean of the vectors in B' (to see this, differentiate the sum with respect to every coordinate of $\mathbf{u}'$). Thus, the LHS of (16) is at least $\tilde{\Delta}(B')$ while the RHS equals $\tilde{\Delta}(A')$.

The operation of transforming A' into B' as above can be applied repeatedly, and must terminate after a finite number of steps (proof omitted, but follows from the fact that the distance between any two members of A' can be bounded from above, that $\tilde{\Delta}(A')$ is invariant to vector translation, and that vector entries are quantized to be multiples of $1/M$). The ultimate termination implies a critical r as well as the existence of an optimal A'. ■

Recall that a sphere of radius r in $\mathbb{R}^{q-1}$ has volume $\sigma_{q-1} r^{q-1}$, where σ_{q-1} is a well known constant [15, Page 411]. Given a set A', we define the volume of A' as

$$\mathrm{Vol}(A') \triangleq \frac{|A'|}{M^{q-1}} \ .$$

For optimal A' as above, the following lemma approximates $\mathrm{Vol}(A')$ by the volume of a corresponding sphere.

Lemma 8: Let A' be a set of size t for which $\tilde{\Delta}(A')$ is minimized. Let the critical radius be r and assume that $r \leq 4$. Then,

$$\mathrm{Vol}(A') = \sigma_{q-1} r^{q-1} + \epsilon_{q-1}(t) \ .$$

The error term $\epsilon_{q-1}(t)$ is bounded from both above and below by functions of M alone (*not* of t) that are $o(1)$ (decay to 0 as $M \to \infty$).

Proof: Let $\delta \colon \mathbb{R}^{q-1} \to \{0, 1\}$ be the indicator function of a sphere with radius r centered at $\bar{\mathbf{p}}'$. That is,

$$\delta(\mathbf{p}') = \begin{cases} 1 & \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \leq r^2 \\ 0 & \text{otherwise} \ . \end{cases}$$

Note that 1) δ is a bounded function and 2) the measure of points for which δ is not continuous is zero (the boundary of a sphere has no volume). Thus, δ is Riemann integrable [16, Theorem 14.5].

Consider the set Ψ' which is $[-4r, 4r]^{q-1}$ shifted by $\bar{\mathbf{p}}'$. Since Ψ' contains the above sphere, the integral of δ over Ψ' must equal $\sigma_{q-1} r^{q-1}$. We now show a specific Riemann sum [16, Definition 14.2] which must converge to this integral. Consider a partition of Ψ' into cubes of side length $1/M$, where each cube center is of the form $(j_1/M, j_2/M, \ldots, j_{q-1}/M)$ and the j_x are integers (the fact that cubes at the edge of Ψ' are of volume less than $1/M^{q-1}$ is immaterial). Define $[\mathbf{p}' \in A']$ as 1 if the condition $\mathbf{p}' \in A'$ holds and 0 otherwise. We claim that the following is a Riemann sum of δ over Ψ' with respect to the above partition.

$$\sum_{\mathbf{p}' = (j_1/M, j_2/M, \ldots, j_{q-1}/M) \in \Psi'} \frac{1}{M^{q-1}} [\mathbf{p}' \in A']$$

To see this, recall that A' has critical radius r.

The absolute value of the difference between the above sum and $\sigma_{q-1} r^{q-1}$ can be upper bounded by the number of cubes that straddle the sphere times their volume $1/M^{q-1}$ (any finer partition will only affect these cubes). Since $r \leq 4$, this quantity must go to zero as M grows, no matter how we let r depend on M. ■

Lemma 9: Let A' be a set of size t for which $\tilde{\Delta}(A')$ is minimized. Let the critical radius be r and assume that $r \leq 4$. Then,

$$\tilde{\Delta}(A') = \frac{(q-1) \cdot (q-1)!}{2(q+1)} \sigma_{q-1} r^{q+1} + \epsilon_{q-1}(t) \ .$$

The error term $\epsilon_{q-1}(t)$ is bounded from both above and below by functions of M alone (*not* of t) that are $o(1)$ (decay to 0 as $M \to \infty$).

Proof: Let the sphere indicator function δ and the bounding set Ψ' be as in the proof of Lemma 8. Consider the sum

$$\sum_{\mathbf{p}'=(j_1/M, j_2/M, \ldots, j_{q-1}/M)\in\Psi'} \frac{1}{M^{q-1}} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \cdot [\mathbf{p}' \in A'] \ . \tag{17}$$

On the one hand, by (14), this sum is simply

$$\frac{2\binom{M+q-1}{q-1}}{M^{q-1}} \tilde{\Delta}(A') \ . \tag{18}$$

On the other hand, (17) is the Riemann sum corresponding to the integral

$$\int_{\Psi'} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \, [\mathbf{p}' \in A'] \, d\mathbf{p}' \ ,$$

with respect to the same partition as was used in the proof of Lemma 8. As before, the sum must converge to the integral, and the convergence rate can be shown to be bounded by expressions which are not a function of t.

All that remains is to calculate the integral. Denote by $\mathrm{sphere}_{q-1}(r) \subseteq \mathbb{R}^{q-1}$ the sphere centered at the origin with radius r. After translating $\bar{\mathbf{p}}'$ to the origin, the integral becomes

$$\int_{\mathrm{sphere}_{q-1}(r)} \left(x_1^2 + x_2^2 + \cdots + x_{q-1}^2\right) \, dx_1 dx_2 \cdots dx_{q-1} = \frac{\sigma_{q-1} \cdot (q-1) \cdot r^{q+1}}{q+1} \ , \tag{19}$$

where the RHS is derived as follows. After converting the integral to generalized spherical coordinates we get an integrand that is r^2 times the integrand we would have gotten had the original integrand been 1 (proof omitted). We know that had that been the case, the integral would have equaled $\sigma_{q-1} r^{q-1}$.

Since (19) must equal the limit of (18), and since the fraction in (18) converges to $2/(q-1)!$, the claim follows. ■

As a corollary to the above three lemmas, we have the following result. The important point to note is that the RHS is convex in $\mathrm{Vol}(A')$.

Corollary 10: Let $t > 0$ be a given integer. Let A' be a set of size t and assume that

$$\max_{\mathbf{p}' \in A'} \|\mathbf{p}' - \bar{\mathbf{p}}'\|_2^2 \le 2 \ . \tag{20}$$

Then,

$$\tilde{\Delta}(A') \ge \frac{(q-1)\cdot(q-1)!}{2(q+1)\cdot(\sigma_{q-1})^{\frac{2}{q-1}}} \cdot \mathrm{Vol}(A')^{\frac{q+1}{q-1}} + o(1) \ , \tag{21}$$

where the $o(1)$ is a function of M alone and goes to 0 as $M \to \infty$.

Proof: Let B' be the set of size t for which $\tilde{\Delta}(B')$ is minimized. The proof centers on showing that the critical radius of B' is at most 4. All else follows directly from Lemmas 8 and 9. Assume to the contrary that the critical radius of B' is greater than 4. Thus, up to translation, A' is a subset of B'. But this implies that $\tilde{\Delta}(A') < \tilde{\Delta}(B')$, a contradiction. ■

C. *Bounding* $\mathrm{DC}(q, L)$

We are now in a position to prove Theorem 2. Recall that A_i is the set of output letters in $\mathcal{Y}$ which get mapped to the letter $z_i \in \mathcal{Z}$. Also, recall that A'_i is simply A_i with the last entry dropped from each vector.

Proof of Theorem 2: By combining (2), (10), (15), and (21), we have that as long as condition (20) holds for all A'_i, $1 \le i \le L$, the degrading cost $\mathrm{DC}(q, L)$ is at least

$$\frac{(q-1)\cdot(q-1)!}{2(q+1)\cdot(\sigma_{q-1})^{\frac{2}{q-1}}} \sum_{i=1}^{L} \mathrm{Vol}(A'_i)^{\frac{q+1}{q-1}} + o(1) \ . \tag{22}$$

Recalling that the elements of A are probability vectors, we deduce that condition (20) must indeed hold. Next, recall that $\mathrm{Vol}(A'_i) = \mathrm{Vol}(A_i)$, and thus

$$\sum_{i=1}^{L} \mathrm{Vol}(A'_i) = \frac{|\mathrm{out}(\mathsf{W})|}{M^{q-1}} = \frac{\binom{M+q-1}{q-1}}{M^{q-1}} \ . \tag{23}$$

Note that the RHS converges to $1/(q-1)!$ as $M \to \infty$. By convexity, we have that if we are constrained by (23), then the sum in (22) is lower bounded by setting all $\mathrm{Vol}(A'_i)$ equal to the RHS of (23) divided by L. Thus, after taking $M \to \infty$, we get (3). ■

Acknowledgments: The author thanks Eren Şaşoğlu and Igal Sason for their feedback.

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, pp. 3051–3073, 2009.

[2] E. Şaşoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," `arXiv:0908.0302v1`, 2009.

[3] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, UK: Cambridge University Press, 2008.

[4] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2009)*, Seoul, South Korea, 2009, pp. 1496–1500.

[5] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inform. Theory*, vol. 59, pp. 6562–6582, 2013.

[6] R. Pedarsani, S. H. Hassani, I. Tal, and E. Telatar, "On the construction of polar codes," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2011)*, Saint Petersburg, Russia, 2011, pp. 11–15.

[7] B. M. Kurkoski and H. Yagi, "Quantization of binary-input discrete memoryless channels, with applications to LDPC decoding," `arXiv:11107.5637v1`, 2011.

[8] I. Tal, A. Sharov, and A. Vardy, "Constructing polar codes for non-binary alphabets and MACs," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2012)*, Cambridge, Massachusetts, 2012, pp. 2132–2136.

[9] U. Pereg and I. Tal, "Channel upgradation for non-binary input alphabets and MACs," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2014)*, Honolulu, Hawaii, 2014.

[10] A. Ghayoori and T. A. Gulliver, "Upgraded approximation of non-binary alphabets for polar code construction," `arXiv:1304.1790v3`, 2013.

[11] V. Guruswami and A. Velingker, "An entropy sumset inequality and polynomially fast convergence to shannon capacity over all alphabets," `arXiv:1411.6993`, 2014.

[12] O. Hölder, "Über einen mittelwerthssatz," *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.*, pp. 38–47, 1889.

[13] *The Cauchy–Schwarz Master Class*. Cambridge, UK: Cambridge University Press, 2004.

[14] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[15] T. M. Apostol, *Calculus*, 2nd ed. Wiley, 1967, vol. 2.

[16] ——, *Mathematical Analysis*, 2nd ed. Reading, Massachusetts: Addison-Wesley, 1974.