

Finite-Level Quantization Procedures for Construction and Decoding of Polar Codes

Yunus Inan and Emre Telatar
EPFL, Lausanne, Switzerland
Email: {yunus.inan,emre.telatar}@epfl.ch

Abstract—We consider finite-level, symmetric quantization procedures for construction and decoding of polar codes. Whether polarization occurs in the presence of quantization is not known in general. In [1], it is shown that a simple three-level quantization procedure polarizes and a calculation method is proposed to obtain a lower bound for achievable rates. We find an improved calculation method for achievable rates and also the exact asymptotic behavior of the block error probability under the aforementioned simple case. We then prove that certain D -level quantization schemes polarize and we give a lower bound on achievable rates. Furthermore, we show that a broad class of quantization procedures result in a weaker form of the polarization phenomenon.

I. INTRODUCTION

Polar codes are the first class of channel codes that achieve capacity for Binary-input Memoryless Symmetric (BMS) channels with low encoding and decoding complexities [2]. As the name suggests, polar codes are based on a polarization phenomenon, which we now describe briefly: Given two identical and independent instances of a BMS channel $W : \mathbb{F}_2 = \mathcal{X} \rightarrow \mathcal{Y}$, create two synthetic channels $W^- : \mathcal{X} \rightarrow \mathcal{Y}^2$ and $W^+ : \mathcal{X} \rightarrow \mathcal{Y}^2 \times \mathcal{X}$ with the polar transform introduced in [2]. Arikan has shown that the mutual information of W^+ is greater than the mutual information of W^- and their average is equal to that of W . This means that from a BMS channel W , its ‘worse’ and ‘better’ versions are synthesized while the average mutual information is preserved. Recursive application of the above construction allows one to synthesize channels W^{s_n} for all $s_n \in \{+, -\}^n$ in n steps. Arikan has also shown that a fraction of synthetic channels eventually become ‘perfect’ whereas the other fraction eventually become ‘useless’. In other words, they eventually polarize. Together with the fact that the average mutual information remains same at each step and the error probability of perfect channels behave as $O(2^{-2^{n/2}})$ (cf. [3]), this shows the capacity achieving property of polar codes.

Arikan has introduced the Successive Cancellation Decoder (SCD) in [2], which estimates the channel input sequence by calculating the individual log-likelihood ratios (LLR) for each bit, exploiting the recursive structure. The basis of code construction is to send the information bits through synthetic channels that are close to perfect. Identifying these almost perfect channels can in principle be done with a density evolution algorithm [4]. We exploit the inherent symmetry of BMS channels and assume all-zero sequence is sent throughout this manuscript. Under this assumption and supposing that the random channel output is Y , the update equations for LLRs are given by

$$L^- = L \boxplus L', \quad L^+ = L + L' \quad (1)$$

where $L \triangleq \ln \left(\frac{W(Y|0)}{W(Y|1)} \right)$, $a \boxplus b \triangleq \ln \left(\frac{e^{a+b} + 1}{e^a + e^b} \right)$ and L' is an identical and independent copy of L . Similar to the creation of synthetic channels, one can calculate the distribution of any L^{s_n} , $s_n \in \{+, -\}^n$. Note that the distribution of L^{s_n} is equivalent to the channel transition probabilities of W^{s_n} given all-zero input.

Now, we state two challenges about code construction and decoder implementation:

- 1) In general, equations (1) suggest that the support size of LLRs grow exponentially in block length. To overcome this problem, special degradation procedures or approximations are proposed (e.g., see [5], [6]).
- 2) LLRs are real numbers, therefore implementation of a real-time SCD has to include an inherent quantization scheme depending on the required precision (c.f. [7]). In [1], robustness of polarization with respect to a specific family of quantization schemes was examined and the authors have shown that even a simple 3-level quantization scheme polarizes.

We refer the reader to the partial list ([8]–[12]) for other studies on these considerations. To the best of our knowledge, little is known about polarization phenomenon for finite-level quantization schemes other than a specific three-level case. We have found that a weaker polarization phenomenon compared to that in [2] exists under some constraints.

The main results of this manuscript are:

- (i) For the three-level quantization scheme in [1], an improved calculation method for the lower bound for achievable rates is obtained.
- (ii) The exact asymptotic behavior of block error probability for the same three-quantized decoder is found to be $O(2^{-\sqrt{N}^{\log \phi}})$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio and $N = 2^n$ is the block length.
- (iii) A broad family of finite-level quantization procedures weakly polarize. The family is to be defined in Section III.

II. NOTATION

The random variables are denoted with uppercase letters whereas their realizations are denoted with lowercase letters (e.g., X_n and x_n). Sets and events are denoted with script-style letters (e.g., \mathcal{A}_n , \mathcal{G}_n). As two special cases, the set $\{1, 2, \dots, n\}$ is denoted $[n]$, $n \in \mathbb{N}$ and $\Pi_{\mathbb{R}}$ denotes the set of all probability distributions on \mathbb{R} . $|\mathcal{A}|$ denotes the cardinality of a set \mathcal{A} . Vectors and sequences are denoted by boldface letters. If their length is known, it is added as a subscript (e.g., s_n). If the length is not known or has no importance, we drop

the subscript (e.g., s). $\mathbb{1}_{\mathcal{A}}$ denotes the indicator function for a set \mathcal{A} .

We abbreviate the following operations: $a \wedge b \triangleq \min\{a, b\}$, $a \vee b \triangleq \max\{a, b\}$, $\text{sign}(x) \triangleq \mathbb{1}_{\{x>0\}} - \mathbb{1}_{\{x<0\}}$. $h(x) \triangleq -x \log x - (1-x) \log(1-x)$ is the binary entropy function defined for $x \in [0, 1]$. All the logarithms are in base 2 unless we use the notation \ln for natural logarithm.

III. STATIC AND DYNAMIC QUANTIZATION PROCEDURES

We define a family of symmetric quantization procedures to unify the approaches in [1], [5] and [6].

Definition 1 (*D*-quantization family and admissible quantization procedures). For a finite $D \in \mathbb{N}$, a *D*-quantization family $\mathcal{Q}^{(D)}$ is a family of odd, increasing step functions which can take at most D values. Moreover, the members are right continuous on \mathbb{R}_+ , and left continuous on \mathbb{R}_- . We also define the family of admissible quantization procedures as $\mathcal{Q} \triangleq \cup_{D \geq 1} \mathcal{Q}^{(D)}$.

Restriction to odd functions provides symmetry. This is necessary to preserve the property that the set of BMS channels are invariant under polar transforms with quantization schemes.

Note that Definition 1 implies that for all $Q \in \mathcal{Q}$, $Q(0) = 0$. Hence, one can always take D as an odd number. Furthermore, for any member of \mathcal{Q} ; the quantization intervals in \mathbb{R}_+ together with their images contain all the information needed for its behavior in \mathbb{R} . Taking into account the above, we have the following definition of static and dynamic quantization procedures.

Definition 2 (*D*-static and *D*-dynamic quantization). A *D*-dynamic quantization $Q_{\beta}^{(D)} : \Pi_{\mathbb{R}} \times \mathbb{R} \rightarrow \mathbb{R}$ is a member of $\mathcal{Q}^{(D)}$, where the right limits of quantization intervals in \mathbb{R}_+ and their images are described in parameter $\beta(\mathbb{P})$, $\mathbb{P} \in \Pi_{\mathbb{R}}$. $\beta(\mathbb{P})$ is a set of 2-tuples with $|\beta| = \frac{D-1}{2}$ and depends on the distribution \mathbb{P} . A *D*-static quantization is a *D*-dynamic quantization with β being same for all $\mathbb{P} \in \Pi_{\mathbb{R}}$.

We give a simple example of a *D*-static quantization procedure.

Example 1. Given $\alpha_1, \alpha_2, \gamma_1, \gamma_2 \in \mathbb{R}$, $0 < \alpha_1 < \alpha_2$ and $0 < \gamma_1 < \gamma_2$, let $\beta = \{(\alpha_1, \gamma_1), (\alpha_2, \gamma_2)\}$. $Q_{\beta}^{(5)}(x)$ is depicted in Figure 1:

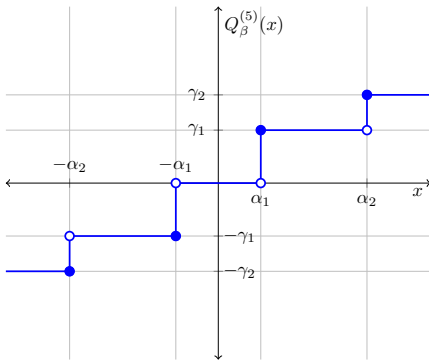


Fig. 1. Graphical representation of $Q_{\beta}^{(5)}(x)$.

A special case is when $\alpha_1 = 0$. Then, $Q_{\beta}(0) = 0$ and $Q_{\beta}(x) = \gamma_1$ for $0 < x < \alpha_2$. Observe that Q_{β} is not continuous at zero for this case.

We sometimes drop the superscript (D) if the number of quantization levels D is known or trivial. For dynamic quantization procedures, the notation $\beta(Y)$ is equivalent to $\beta(\mathbb{P})$ if a random variable Y with distribution \mathbb{P} is to be quantized.

\mathcal{Q} contains a broad class of practical quantization procedures. Observe that any quantization scheme similar to those in [1] belongs to $\mathcal{Q}^{(D)}$. Furthermore, it is immediate from Definition 2 that $Q \circ Q' \in \mathcal{Q}$ for all $Q, Q' \in \mathcal{Q}$. This implies that the greedy quantization procedures in [5] and [6] are dynamic quantization procedures which belong to \mathcal{Q} with the additional condition that zero is an absorbing support, namely, any combination of the zero support with some nonzero support should map to zero. We also emphasize that the widely used approximation (c.f. [13])

$$a \hat{\boxplus} b \triangleq (|a| \wedge |b|) \text{sign}(ab) \approx a \boxplus b$$

results in a dynamic quantization procedure under some conditions.

Lemma 1. Consider a discrete random variable L and its identical and independent copy L' that take values in the finite set $\mathcal{L} = \{d_1, \dots, d_n\}$ for some $n \in \mathbb{N}$. Take the symmetrized set $\tilde{\mathcal{L}} \triangleq \mathcal{L} \cup (-\mathcal{L})$, where $-\mathcal{L} = \{-d_1, \dots, -d_n\}$. Suppose the non-negative elements of $\tilde{\mathcal{L}}$ are ordered as $\alpha_1 \leq \dots \leq \alpha_m$ for some m . If $\alpha_{i+1} > \ln(e^{\alpha_i} + \sqrt{e^{2\alpha_i} - 1})$ for all $1 \leq i \leq m-1$, there exists a dynamic quantization procedure $Q_{\beta(L)}$ such that $L \hat{\boxplus} L' = Q_{\beta(L)}(L \boxplus L')$.

Proof: The random variable $L \boxplus L'$ takes values in the set $\tilde{\mathcal{L}} \boxplus \mathcal{L} = \{-(\alpha_m \boxplus \alpha_m), \dots, \alpha_m \boxplus \alpha_m\}$. Suppose $\alpha_{i+1} > \ln(e^{\alpha_i} + \sqrt{e^{2\alpha_i} - 1})$ for all $1 \leq i \leq m-1$, then one can show $\alpha_{i-1} < \alpha_i \boxplus \alpha_i < \alpha_i \boxplus \alpha_{i+1} < \dots < \alpha_i \boxplus \alpha_m < \alpha_i$ for all $i \in [m]$. Take the dynamic quantization procedure $Q_{\beta(L)}$ with

$$\beta(L) = \cup_{i=1}^m \{(\alpha_i \boxplus \alpha_i, \alpha_i)\}.$$

With the above selection, $Q_{\beta(L)}(\cup_{j \geq i} \{\alpha_i \boxplus \alpha_j\}) = \alpha_i = \cup_{j \geq i} \{\alpha_i \wedge \alpha_j\}$ for all $i \in [m]$. In other words, every $\alpha_i \boxplus \alpha_j$ is mapped to $\alpha_i \wedge \alpha_j$. Since this true for all $i, j \in [m]$, $(L \hat{\boxplus} L') \vee 0 = (Q_{\beta(L)}(L \boxplus L')) \vee 0$. The proof for the negative support follows similarly. ■

Note that the condition in Lemma 1 can be met by simply scaling the random variables L, L' with a large enough constant.

IV. THREE-QUANTIZED CASE

In this section, we study the same three-level quantization procedure from [1]. We briefly explain the findings in [1] with an improvement on calculation of the lower bound for the fraction of perfect channels. We also find the exact asymptotic behavior of the block error probability.

Consider a BMS channel W , whose output Y takes values from the set $\{-\lambda, 0, \lambda\}$. If the initial channel has support size larger than three, it can be quantized with any desired procedure until we obtain a channel with three outputs. The static quantization procedure we consider throughout this section is

$Q_\beta^{(3)}$, $\beta = \{(0, 1)\}$. Verbally, Q_β results in only propagating the signs of the quantized random variables. The quantized channel output, $Y^{s_n} = Q_\beta(Y^{s_{n-1}, s_n})$, $s_n \in \{+, -\}^n$, $n \geq 1$ with Y^{s_{n-1}, s_n} defined according to (1); has therefore three parameters, namely $p^{s_n} \triangleq \Pr(Y^{s_n} = 1)$, $z^{s_n} \triangleq \Pr(Y^{s_n} = 0)$ and $m^{s_n} \triangleq \Pr(Y^{s_n} = -1)$. Without loss of generality, we assume $p \geq m$. Otherwise, one can negate the channel output to fulfil this condition. These parameters completely describe the distribution of Y^{s_n} . Referring to (1), iterations of (p, m, z) under Q_β are given by

$$\begin{aligned} p^+ &= p^2 + 2pz & p^- &= p^2 + m^2 \\ m^+ &= m^2 + 2mz & m^- &= 2mp \\ z^+ &= z^2 + 2mp & z^- &= 2z - z^2. \end{aligned} \quad (2)$$

These iterations are the same as those in [1]. It is possible to calculate (p^s, m^s, z^s) for any $s \in \{+, -\}^*$ with the above transformations. Note that these transformations preserve $p^s \geq m^s$.

A. Feasible Region for Y^s

Our purpose is to track these parameters for the statistic Y^s . At first sight, it may seem that p^s , m^s and z^s can take any value in the set $\mathcal{R}_3 \triangleq \{(p, m, z) : p \geq m, p + m + z = 1, p, m, z \geq 0\}$. However, this is not the case. If it is known that Y^s has gone through $+$ transformation once, there are some restrictions on the feasible region for its parameters.

Lemma 2. Define the limiting curve as the (p, m) pairs with the following parametric equations:

$$\begin{aligned} p^*(t) &= \sqrt{4t^3 - 3t^4} \\ m^*(t) &= 1 - 3t + \frac{3}{2}t^2 + \frac{p^*(t)}{2}, \quad t \in [0, 1]. \end{aligned} \quad (3)$$

Let $\mathcal{R}_3^+ \triangleq \mathcal{R}_3 \cap \{0 \leq m \leq m^*(t), p = p^*(t), \forall t \in [0, 1]\}$. Then, for any $s_n \in \{+, -\}^n$, $n \geq 1$

- (i) It is sufficient that s_n contains at least one $(+)$ to ensure that $(p^{s_n}, m^{s_n}) \in \mathcal{R}_3^+$.
- (ii) If $(p^{s_n}, m^{s_n}) \in \mathcal{R}_3^+$, then $(p^{s_n s}, m^{s_n s}) \in \mathcal{R}_3^+$ for $s \in \{+, -\}$. In words, once (p^{s_n}, m^{s_n}) is driven under the limiting curve, it remains there.

Proof of Lemma 2 is given in Appendix A.

B. Polarization of Quantized Statistics

With a similar approach to those in [1] and [2], parameters of quantized statistics can be examined in a probabilistic setting. The setting is described below:

Fix $\Omega \triangleq \{+, -\}^*$ and let $\mathbf{S}_n = (S_1, S_2, \dots, S_n)$ be a sequence of n random variables where each S_i is independently and uniformly distributed on $\{+, -\}$. Define the natural filtration $\{\mathcal{F}_n\}_{n \geq 1}$ with $\mathcal{F}_n \triangleq \sigma(\mathbf{S}_n)$, $n \geq 1$ and $\mathcal{F}_0 \triangleq \{\Omega, \emptyset\}$. Also define $\mathcal{F} \triangleq \sigma((S_n)_{n \geq 1})$. These ingredients completely define the probability space with filtration $(\Omega, \mathcal{F}, \{\mathcal{F}_n\}, \mathbb{P})$ and for a quantized statistic obtained in n polarization steps, any of its parameter becomes an \mathcal{F}_n -measurable random variable, namely $P_n \triangleq p^{s_n}$, $Z_n \triangleq z^{s_n}$ and $M_n \triangleq m^{s_n}$. Also note that any function of $D_n \triangleq (P_n, Z_n, M_n)$ becomes random.

The quantized statistic Y^{s_n} can also be represented as a 'quantized' or 'degraded' synthetic BMS channel \tilde{W}^{s_n} with

$$\tilde{W}^{s_n}(y|0) = \begin{cases} P_n, & y = 1 \\ Z_n, & y = 0 \\ M_n, & y = -1 \end{cases}.$$

It is known that any bounded submartingale or supermartingale converges almost surely (see, e.g. [14]). Therefore, if a function of D_n is a submartingale or supermartingale, it may give information on whether polarization occurs. From this perspective, we list some consequences of the quantization procedure Q_β in terms of probabilistic arguments. One can verify that P_n , M_n , Z_n themselves exhibit submartingale/supermartingale properties [1]. Moreover, the mutual information of \tilde{W}^{s_n} ,

$$I(\tilde{W}^{s_n}) \triangleq (p^{s_n} + m^{s_n}) \left(1 - h\left(\frac{m^{s_n}}{p^{s_n} + m^{s_n}}\right) \right)$$

is a supermartingale. This property follows simply from data processing inequality as the average mutual information is preserved without quantization.

Lemma 3 ([1], Lemma 4). The random variables P_n , Z_n , M_n converge almost surely. Moreover, $Z_\infty \triangleq \lim_{n \rightarrow \infty} Z_n = 0$ or 1, $P_\infty \triangleq \lim_{n \rightarrow \infty} P_n = 0$ or 1 and $M_\infty \triangleq \lim_{n \rightarrow \infty} M_n = 0$ almost surely. Namely, Y^{s_n} polarizes.

Lemma 3 simply follows from the fact that Z_n is a submartingale and M_n supermartingale.

Knowing that the quantized statistics polarize, we elaborate on the question of what fraction of these statistics carry lossless information. We note that it is very hard to obtain an exact expression for this fraction. Let γ denote the fraction of the lossless statistics. Lower and upper bounds for γ can be obtained from the submartingale and supermartingale properties of some functions $f(D_n)$ with $f(1, 0, 0) = 1$ and $f(0, 1, 0) = 0$. Suppose $f(D_n)$ is a bounded submartingale (supermartingale), i.e., it satisfies $\frac{f(d^+) + f(d^-)}{2} \underset{(\leq)}{\overset{(\geq)}{}} f(d), \forall d \in \mathcal{R}_3$. Then $\gamma = \mathbb{E}[f(P_\infty, Z_\infty, M_\infty)] \underset{(\leq)}{\overset{(\geq)}{}} f(p, z, m)$, which shows that f is useful to obtain an lower (upper) bound on γ . In [1] it is shown that $I(W)^2 \leq \gamma \leq I(\tilde{W})$ as $I(\tilde{W}^{s_n})$ is a supermartingale and $I(\tilde{W}^{s_n})^2$ submartingale. In addition, we have numerically found that $I^{1.24}(\tilde{W}^{s_n})$ is submartingale if the process starts in \mathcal{R}_3^+ . Hence, we have the following improved lower bound for γ .

Lemma 4. If the original (p, m) belongs to \mathcal{R}_3^+ , then $I^{1.24}(W)$ is a lower bound for γ . If not, then $\frac{1}{2}I^{1.24}(\tilde{W}^+) + \frac{1}{2}I^2(\tilde{W}^-)$ is a lower bound for γ . More precisely, define

$$F_0(W) \triangleq \begin{cases} I^{1.24}(W), & (p, m) \in \mathcal{R}_3^+ \\ \frac{1}{2}I^{1.24}(\tilde{W}^+) + \frac{1}{2}I^2(\tilde{W}^-), & \text{else} \end{cases}.$$

Then, $F_0(W) \leq \gamma$.

Corollary 1. F can be improved by increasing the number of

polarization steps. Namely, define

$$F_n(W) \triangleq \begin{cases} \frac{1}{2^n} \sum_{s_n \in \{+, -\}^n} I^{1.24}(\tilde{W}^{s_n}), & (p, m) \in \mathcal{R}_3^+ \\ \frac{1}{2^n} \left(\sum_{s_n \in \{+, -\}^n \setminus (-)^n} I^{1.24}(\tilde{W}^{s_n}) + I^2(\tilde{W}^{(-)^n}) \right), & \text{else} \end{cases}$$

Then, $F_0(W) \leq F_n(W) \leq \gamma$.

The proposed method for calculation of the lower bound in [1] relies on the fact that γ is bounded from above and below as $\mathbb{E}[I^2(\tilde{W}^{s_n})] \leq \gamma \leq \mathbb{E}[I(\tilde{W}^{s_n})]$, and $\mathbb{E}[I(\tilde{W}^{s_n})] - \mathbb{E}[I^2(\tilde{W}^{s_n})] \leq \delta$ for some $\delta > 0$ and large enough n . Therefore, one can obtain a confidence interval of δ for large n . Since $\mathbb{E}[I(\tilde{W}^{s_n})] - F_n(W)$ decreases faster, the same confidence interval δ can be achieved with smaller n compared to the first method. This results in an improved calculation method for the lower bound.

C. Rate of Polarization

From the previous section, we know that the quantized statistics polarize. However, it is required that the error probability $P_e(\tilde{W}^{s_n}) \triangleq M_n + \frac{1}{2}Z_n$ of each perfect statistic decays fast enough, i.e. $o(2^{-n})$, to ensure reliable communication under the aforementioned quantization procedure. For the unquantized case, it is found in [3] that the Bhattacharyya parameter $Z_b(W^{s_n})$, which is an upper bound to the error probability, decays as $O(2^{-2^{n/2}})$ and in [1], it is shown that $Z_b(\tilde{W}^{s_n}) \triangleq 2\sqrt{P_n M_n} + Z_n$ decays as $O(2^{-2^{\alpha n}})$, $\alpha < \frac{\log 1.5}{2}$ under Q_β according to the previously given probabilistic setting. Since $(P_n, M_n) \in \mathcal{R}_3^+$ and thus $M_n \leq Z_n$ eventually, this also implies Z_n and M_n decay at least with the same rate. However, one cannot compare the decay rates of Z_n and M_n only knowing the decay rate of $Z_b(\tilde{W}^{s_n})$. If M_n decays much faster than Z_n , it is possible that the code constructed with Q_β can be concatenated with an erasure-only code as an outer code for large n . Unfortunately, this is not the case. To show this, we present the following lemma and theorem, whose proofs are given in Appendices B and C respectively.

Lemma 5. For all $\epsilon_r > 0$,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\left| \frac{\log M_n}{\log Z_n} - \phi \right| \leq \epsilon_r \right) = \gamma, \quad \phi = \frac{1 + \sqrt{5}}{2}.$$

Lemma 5 suggests that with probability close to γ , M_n and Z_n decay with same rate. With the next theorem, we obtain the exact rate.

Theorem 1. In limit, the random processes Z_n and M_n roughly behave as $O(2^{-2^{\alpha n}})$, $\alpha = \frac{\log \phi}{2}$ with probability close to γ . That is, for any $\delta, \delta' > 0$,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(2^{-2^{n \frac{\log \phi + \delta'}{2}}} \leq Z_n \leq 2^{-2^{n \frac{\log \phi - \delta}{2}}} \right) = \gamma$$

and

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(2^{-2^{n \frac{\log \phi + \delta'}{2}}} \leq M_n \leq 2^{-2^{n \frac{\log \phi - \delta}{2}}} \right) = \gamma.$$

Lemma 5 and Theorem 1 imply that Z_n and M_n decay at the same rate. Consequently, concatenation with an erasure-only code does not improve the error probability. Also note that the rate of polarization for this particular three-quantized case is bounded away from $O(2^{-2^{n/2}})$, which shows that longer codes are required to ensure reliable communication compared to the unquantized case.

V. D-QUANTIZED CASE

In this section, we consider static and dynamic quantization procedures $Q_\beta^{(D)}$, where $D = 2d + 1$ is an odd number by definition. Note that $|\beta| = d$. Similar to the three-level case, we start with a BMS channel W whose output Y takes values in the set $\{0, \pm\lambda_1, \dots, \pm\lambda_d\}$, $\lambda_i > 0$, $i \in [d]$. Define the parameters of the quantized statistic Y^{s_n} as $p_i^{s_n}$, $m_i^{s_n}$ and z^{s_n} in a similar fashion to that in Section IV and assume $p_i \geq m_i$. Also define $p^{s_n} \triangleq \sum_{i=1}^d p_i^{s_n}$ and $m^{s_n} \triangleq \sum_{i=1}^d m_i^{s_n}$.

In general, it appears to be hard to obtain good lower bounds on the achievable rates for quantization procedures with output size greater than three. However, we have found that there are non-trivial D -static and D -dynamic quantization procedures that result in the same dynamics as the simple three-quantized case. We formally define these procedures below.

Definition 3 (Proper quantization procedures). A quantization procedure $Q_{\beta(\mathbb{P})}^{(D)}$ is proper if $\beta(\mathbb{P})_i \neq \beta(\mathbb{P})_j$ for all $i \neq j \in [d]$ and $\mathbb{P} \in \mathcal{P}$. In words, β consists of distinct elements.

Note that if a quantization procedure is not proper, then it is equivalent to another quantization procedure with $|\beta| < d$.

Lemma 6. There exists

- (i) a pair of proper D -static quantization procedures Q_{β^+} , Q_{β^-} with $Y^+ = Q_{\beta^+}(Y + Y')$, $Y^- = Q_{\beta^-}(Y \boxplus Y')$ that results in the same dynamics as the three-quantized case,
- (ii) a single proper D -static quantization procedure Q_β that results in the same dynamics as the three-quantized case.

Proof Sketch:

- (i) Take any

$$\beta^+ = \cup_{i=1}^d \{(\alpha_i, \alpha_i)\}, \quad \beta^- = \cup_{i=1}^d \{(\alpha_i \boxplus \alpha_i, \alpha_i)\}$$

such that $0 < \alpha_1 < \alpha_i < 2\alpha_1$, $i \in [d]$, $i \neq 1$.

- (ii) Take $\beta = \cup_{i=1}^d \{(\alpha_i \boxplus \alpha_i, \alpha_i)\}$ such that $0 < \alpha_1 < \alpha_i < 2(\alpha_1 \boxplus \alpha_1)$, $i \in [d]$, $i \neq 1$.

Under these assumptions, one can verify that the resulting dynamics for both cases become the same as those in the formerly discussed three-quantized case. ■

Lemma 6 shows that with a pair of two proper D -static quantization procedures, or with a single proper D -static quantization procedure, the system performance can be made equivalent to that in the simple three-quantized case. This also implies that there are proper D -dynamic quantization schemes with the same performance. Based on this fact, a lower bound on the achievable rates can be derived for D -quantization families.

Lemma 7. Consider the function F_n defined in Corollary 1 for an $n \geq 0$. Then, the following claims hold:

- (i) With a pair of proper D -static quantization procedures Q_{β^+} and Q_{β^-} , one can achieve rates greater than

$$R_{s,2}^{(D)}(W) \triangleq \max_{\substack{\alpha_1 \leq \alpha_2 \dots \leq \alpha_d \\ \alpha_d \leq 2\alpha_1 \\ \alpha_1 \boxplus \alpha_1 \vee (\alpha_1/2) \leq \lambda_d}} \frac{F_n(\tilde{W}^+) + F_n(\tilde{W}^-)}{2},$$

where $\beta^+ = \cup_{i=1}^d \{(\alpha_i, \alpha_i)\}$ and $\beta^- = \cup_{i=1}^d \{(\alpha_i \boxplus \alpha_i, \alpha_i)\}$.

- (ii) With a single proper D -static quantization procedure Q_β , one can achieve rates greater than

$$R_{s,1}^{(D)}(W) \triangleq \max_{\substack{\alpha_1 \leq \alpha_2 \dots \leq \alpha_d \\ \alpha_d \leq 2(\alpha_1 \boxplus \alpha_1) \\ \alpha_1 \boxplus \alpha_1 \leq \lambda_d}} \frac{F_n(\tilde{W}^+) + F_n(\tilde{W}^-)}{2},$$

where $\beta = \cup_{i=1}^d \{(\alpha_i \boxplus \alpha_i, \alpha_i)\}$.

- (iii) With a proper D -dynamic quantization procedure Q_β , one can achieve rates greater than

$$R_d^{(D)}(W) \triangleq \sup_{\substack{Q_{\beta(Y+Y')} \in \mathcal{Q}^{(D)} \\ Q_{\beta(Y \boxplus Y')} \in \mathcal{Q}^{(D)}}} \frac{F_n(\tilde{W}^+) + F_n(\tilde{W}^-)}{2},$$

where $Y^+ = Q_{\beta(Y+Y')}(Y + Y')$ and $Y^- = Q_{\beta(Y \boxplus Y')}(Y + Y')$. In other words, quantize $Y + Y'$ and $Y \boxplus Y'$ in the best possible way to maximize the objective function.

Proof: For (i) and (ii), take the procedures described in Lemma 6. Since the evolution of the parameters are same as the three-quantized case after one polarization step, we use the same lower bound. The last inequalities are added to make the region compact. For (iii), we see that at any step, a proper dynamic quantization exists to ensure that the parameters evolve similarly to the three-quantized case. Quantization at first step is optimized to get a better lower bound. ■

It is important to note that the special quantization schemes considered in the proof of Lemma 6 ensure that the quantized statistics polarize as the resulting dynamics are equivalent to that in three-level case. At first glance, it is not obvious that the statistics polarize for any admissible quantization procedure. Surprisingly, the quantized statistics polarize in a weaker manner under any admissible static or dynamic quantization procedure.

Theorem 2. Consider the probabilistic setting in Section IV-B and define $P_{i,n} \triangleq p_i^{S_n}$, $M_{i,n} \triangleq m_i^{S_n}$ for all $i \in [d]$. Then, for all static or dynamic quantization procedures in \mathcal{Q} , Z_n converges to 0 or 1 almost surely and for any i , $P_{i,n}M_{i,n}$ converges to 0 in probability.

Proof: We use the abbreviations $X_n \xrightarrow{\text{a.s.}} c$ and $X_n \xrightarrow{P} c$ to denote that X_n converges to $c \in \mathbb{R}$ almost surely or in probability respectively. For every static or dynamic $Q_\beta \in \mathcal{Q}$, it is known that $Q_\beta(0) = 0$. This implies that if $Y = 0$ or $Y' = 0$ then $Y^- = Q_\beta(Y \boxplus Y') = 0$ and if $Y, Y' = 0$ or $Y = -Y'$ then $Y^+ = Q_\beta(Y + Y') = 0$. One thus obtains

$$z^- \geq 2z - z^2, \quad z^+ \geq z^2 + 2 \sum_{i=1}^d p_i m_i.$$

Therefore, Z_n is a bounded submartingale as $\mathbb{E}[Z_{n+1}|\mathcal{F}_n] \geq Z_n + \sum_{i=1}^d P_{i,n}M_{i,n}$. Considering the $-$ transformation and following the same steps in [2], we obtain

$$\mathbb{E}[|Z_{n+1} - Z_n|] \geq \frac{1}{2} \mathbb{E}[Z_n^- - Z_n] \geq \frac{1}{2} \mathbb{E}[Z_n - Z_n^2].$$

Since $\lim_n \mathbb{E}[|Z_{n+1} - Z_n|] = 0$ and Z_n converges almost surely, $Z_n \xrightarrow{\text{a.s.}} 0$ or 1. Studying the $+$ transformation instead, we obtain

$$\mathbb{E}[|Z_n^+ - Z_n|] = \mathbb{E}\left[Z_n^2 - Z_n + 2 \sum_{i=0}^d P_{i,n}M_{i,n} + J_n\right],$$

where J_n is an \mathcal{F}_n -measurable non-negative remainder term. With a similar reasoning, we know that the right hand side goes to zero as n tends to infinity. This implies that $Z_n^2 - Z_n + 2 \sum_{i=0}^d P_{i,n}M_{i,n} + J_n \xrightarrow{P} 0$. $Z_n^2 - Z_n \xrightarrow{\text{a.s.}} 0$ implies $Z_n^2 - Z_n \xrightarrow{P} 0$. It is well-known that if $X_n \xrightarrow{P} x$ and $Y_n \xrightarrow{P} y$ for some constants x and y , then $X_n + Y_n \xrightarrow{P} x + y$. From this fact, we conclude that $2 \sum_{i=0}^d P_{i,n}M_{i,n} + J_n \xrightarrow{P} 0$ as well. Since both $2 \sum_{i=0}^d P_{i,n}M_{i,n}$ and J_n are non-negative random variables, we have $\sum_{i=0}^d P_{i,n}M_{i,n} \xrightarrow{P} 0$ and $P_{i,n}M_{i,n} \xrightarrow{P} 0$ for all $i \in [d]$. ■

Theorem 2 has significance in practice as it implies Tal-Vardy construction in [5] under the assumption that zero is an absorbing support, any quantization scheme as in [1] and many other schemes weakly polarize. The weak polarization implies that for sufficiently large n , some fraction of synthetic channels meet the condition that $\tilde{W}^{s_n}(y|0)$ and $\tilde{W}^{s_n}(y|1)$ have almost non-overlapping supports. If one is allowed to remap the supports and change the quantization procedure once at some n , one can show that the quantized statistics can be forced to polarize strongly.

Lemma 8. Assume $Z_\infty = 0$ with probability $\gamma_Z > 0$, i.e., a non-zero fraction γ_Z of quantized statistics tend to become non-zero with probability 1. Given $\epsilon, \delta > 0$ and $\delta \leq \gamma_Z$, one can ensure that the quantized statistics polarize and at least $(\gamma_Z - \delta)(1 - \epsilon - 2\sqrt{d}\epsilon^{1/4})^2$ fraction of the statistics will eventually become perfect by remapping of supports and changing the procedure to the simple three-quantized case after some $n_0(\delta, \epsilon)$.

Proof: Given ϵ, δ , Theorem 2 implies the existence of an n_0 such that

$$\mathbb{P}(Z_n \leq \epsilon, P_{i,n}M_{i,n} \leq \epsilon, i \in [d]) \geq \gamma_Z - \delta, \quad n \geq n_0.$$

We consider $s_n \in \{+, -\}^n$ such that the condition in the above event holds. For such s_n , $p_i^{s_n} \wedge m_i^{s_n} \leq \sqrt{\epsilon}$ for all $i \in [d]$. At n_0 , we remap the support such that $m_i^{s_n} \leftarrow p_i^{s_n} \wedge m_i^{s_n}$ and we switch to the simple three-level quantization procedure Q_β , $\beta = \{(0, 1)\}$. This will ensure that $m^{s_n} \leq d\sqrt{\epsilon}$. Under these conditions the Bhattacharyya parameters are bounded as $Z_b(\tilde{W}^{s_n}) \triangleq z^{s_n} + 2\sqrt{p^{s_n}m^{s_n}} \leq \epsilon + 2\sqrt{d}\epsilon^{1/4}$. For BMS channels, it is known that $I(W) \geq 1 - Z_b(W)$, thus $I(\tilde{W}^{s_n}) \geq 1 - \epsilon - 2\sqrt{d}\epsilon^{1/4}$. Observe that the specific three-quantized case polarizes strongly. Now we use the simple lower bound $I(W)^2$

to show that at least $(\gamma_Z - \delta)(1 - \epsilon - 2\sqrt{d}\epsilon^{1/4})^2$ fraction of channels will eventually become perfect. ■

Note that the three-quantized case assures that the block error probability behaves roughly as $O(2^{-\sqrt{N}^{\log \phi}})$. Together with Lemma 8, it implies that one achieves reliable communication at rates arbitrarily close to γ_Z by constructing and decoding polar codes with D -level quantization procedures, if it is allowed to change the procedure and remap the supports once at an arbitrary n . As a final note, we remark that if the quantization procedures take some special form, e.g., if they ensure that the quantized statistics are LLRs as in [5], then the remapping of the support is not needed since $M_n \leq P_n$ always.

REFERENCES

- [1] S. H. Hassani and R. Urbanke, "Polar codes: Robustness of the successive cancellation decoder with respect to quantization," in *2012 IEEE International Symposium on Information Theory Proceedings*, July 2012, pp. 1962–1966.
- [2] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.
- [3] E. Arikan and E. Telatar, "On the rate of channel polarization," in *2009 IEEE International Symposium on Information Theory*, June 2009, pp. 1493–1495.
- [4] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *2009 IEEE International Symposium on Information Theory*, June 2009, pp. 1496–1500.
- [5] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6562–6582, Oct 2013.
- [6] R. Pedarsani, S. H. Hassani, I. Tal, and E. Telatar, "On the construction of polar codes," in *2011 IEEE International Symposium on Information Theory Proceedings*, July 2011, pp. 11–15.
- [7] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5165–5179, Oct 2015.
- [8] P. Trifonov, "Efficient design and decoding of polar codes," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3221–3227, November 2012.
- [9] R. Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," *IEEE Communications Letters*, vol. 13, no. 7, pp. 519–521, July 2009.
- [10] Z. Shi and K. Niu, "On uniform quantization for successive cancellation decoder of polar codes," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, Sep. 2014, pp. 545–549.
- [11] J. Neu, "Quantized polar code decoders: Analysis and design," *CoRR*, vol. abs/1902.10395, 2019. [Online]. Available: <http://arxiv.org/abs/1902.10395>
- [12] G. Bocherer, T. Prinz, P. Yuan, and F. Steiner, "Efficient polar code construction for higher-order modulation," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, March 2017, pp. 1–6.
- [13] C. Leroux, I. Tal, A. Vardy, and W. J. Gross, "Hardware architectures for successive cancellation decoding of polar codes," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011, pp. 1665–1668.
- [14] D. Williams, *Probability with Martingales*, ser. Cambridge mathematical textbooks. Cambridge University Press, 1991.

APPENDIX

A. Proof of Lemma 2

- (i) Our purpose here is to show that when s_n contains at least one (+), (p^{s_n}, m^{s_n}) is driven under the limiting curve. In other words, for a fixed p^{s_n+} , we want to prove that m^{s_n+} cannot exceed the limiting curve. To this end, using

(2), we formulate the following optimization problem.

$$\begin{aligned} \max_{p, m} \quad & m^+ = 2m - m^2 - 2mp \\ \text{s.t} \quad & p^+ = 2p - p^2 - 2mp \\ & p, m \geq 0 \\ & p + m \leq 1 \end{aligned}$$

where p^+ is a fixed constant in $[0, 1]$. From the equality constraint, we have $m = (1 - p/2 - p^+/2p)$ and the objective function can be modified as

$$\begin{aligned} 2m - m^2 + p^2 - 2p &= 1 - \left(\frac{p}{2} + \frac{p^+}{2p}\right)^2 + p^2 - 2p \\ &= (p - 1)^2 + \left(\frac{p}{2} + \frac{p^+}{2p}\right)^2. \end{aligned}$$

Taking the derivative and setting to 0, we obtain the only extremal p in an implicit function

$$p^+ = \sqrt{4p^3 - 3p^4}.$$

The same extremal p yields the maximized objective function

$$m^+ = 1 - 3p + \frac{3}{2}p + \frac{1}{2}\sqrt{4p^3 - 3p^4}.$$

Note that the map $p \rightarrow p^+$ is bijective in $[0, 1]$. This gives a parametric description of (p^+, m^+) , where $p^+, m^+ \in [0, 1]$ for $p \in [0, 1]$. However, we note that for $p \leq 1/3$, $m^+ \geq p^+$ which is a contradiction to our assumptions. Incorporating the fact that p^+ is always greater than m^+ , the parametric curve can be described as above for $p \in [1/3, 1]$, and $p^+ = m^+ = p$ for $p \in [0, 1/3]$. Renaming the variable p as t , we obtain the same parametric description given in the statement of Lemma 2.

The optimization problem above was formulated to find the maximum m^+ value corresponding to a p^+ . Hence, given s_n contains at least one (+), we have shown that (p^{s_n}, m^{s_n}) cannot exceed the limiting curve and any such (p^{s_n}, m^{s_n}) is driven into \mathcal{R}_3^+ .

Before proving part (ii), we give the following property.

Property 1. *The limiting curve is non-increasing and convex on $p \in [1/3, 1]$. Moreover, $\frac{\partial m^*}{\partial p^*} \geq -1$ and $\frac{\partial^2 m^*}{\partial (p^*)^2} \big|_{p^* \rightarrow 1} = \infty$.*

$$\text{Proof: } \frac{\partial m^*}{\partial p^*} = \frac{1}{2} \left(1 - \sqrt{\frac{4}{t} - 3} \right).$$

$$\frac{\partial^2 m^*}{\partial (p^*)^2} = \frac{\frac{\partial}{\partial t} \frac{\partial m^*}{\partial p^*}}{\frac{\partial p^*}{\partial t}} = \frac{1}{6(t^2 - t^3)} \geq 0.$$

The inequality and limit argument follows easily. ■

- (ii) For this part, we have to show that once a (p^{s_n}, m^{s_n}) is driven under the limiting curve, it remains there. Similar to part (i), we consider the following optimization problem to find the maximum value of a m^- with respect

to a fixed p^- :

$$\begin{aligned} \max_{p,m} \quad & m^- = 2mp \\ \text{s.t} \quad & p^- = p^2 + m^2 \\ & (p, m) \in \mathcal{R}_3^+ \end{aligned}$$

where p^- is a fixed constant in $[0, 1]$. It is easy to see that the optimal (\hat{p}, \hat{m}) for this problem also maximizes the function $p + m$. Therefore, for $p^- \leq \frac{2}{9}$, $\hat{p} = \hat{m} = \sqrt{\frac{p^-}{2}}$ and $p^- = m^- = 2\hat{m}\hat{p}$. The (p^-, m^-) corresponding to (\hat{p}, \hat{m}) remains in \mathcal{R}_3^+ . If $p^- > \frac{2}{9}$, then the optimal (\hat{p}, \hat{m}) always lies on the limiting curve. Therefore, the parametric description for the solution is given by

$$\begin{aligned} \tilde{p}(t) &= (p^*(t))^2 + (m^*(t))^2 \\ &= (4t^3 - 3t^4) + \left(1 - 3t + \frac{3}{2}t^2 + \frac{\sqrt{4t^3 - 3t^4}}{2}\right)^2 \\ \tilde{m}(t) &= 2p^*(t)m^*(t) \\ &= \sqrt{4t^3 - 3t^4} \left(1 - 3t + \frac{3}{2}t^2\right) + \frac{1}{2}(4t^3 - 3t^4). \end{aligned}$$

for $t \in [1/3, 1]$.

Now, one has to check if $(\tilde{p}(t), \tilde{m}(t)) \in \mathcal{R}_3^+$ for all $t \in [1/3, 1]$. Observe that for any $(p, m) \in \mathcal{R}_3^+$, $p^- = p^2 + m^2 \leq p$, thus $\tilde{p}(t) \leq p^*(t)$. The equality holds if and only if $t = 1$. Moreover, we note that $\tilde{m}(p)$ has to be convex in $p > p_c$ for some critical p_c as its derivative is zero at $p = 1$ and being concave will drive it to the negative side, which is impossible. From these facts, we observe that if $\tilde{m}(p)$ exceeds $m^*(p)$ at some p , it is required that $\frac{\partial \tilde{m}}{\partial p'} \geq \frac{\partial m^*}{\partial p'}$ for some other $p' \geq p$. Hence if we show that this inequality does not hold, then the proof will be complete. Noting that $\tilde{p}(t) \leq p^*(t)$, it is sufficient to prove the stronger statement

$$\frac{\frac{\partial \tilde{m}}{\partial t}}{\frac{\partial \tilde{p}}{\partial t}} \geq \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}, \quad t \in [1/3, 1]. \quad (4)$$

One can derive

$$\begin{aligned} \frac{\partial \tilde{p}}{\partial t} &= 2p^*(t) \frac{\partial p^*}{\partial t} + 2m^*(t) \frac{\partial m^*}{\partial t}, \\ \frac{\partial \tilde{m}}{\partial t} &= 2p^*(t) \frac{\partial m^*}{\partial t} + 2m^*(t) \frac{\partial p^*}{\partial t}. \end{aligned}$$

Hence,

$$\frac{\frac{\partial \tilde{m}}{\partial t}}{\frac{\partial \tilde{p}}{\partial t}} = \frac{2p^*(t) \frac{\partial m^*}{\partial t} + 2m^*(t) \frac{\partial p^*}{\partial t}}{2p^*(t) \frac{\partial p^*}{\partial t} + 2m^*(t) \frac{\partial m^*}{\partial t}} = \frac{\frac{m^*(t)}{p^*(t)} + \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}}{1 + \frac{m^*(t)}{p^*(t)} \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}}.$$

The inequality (4) then becomes

$$\frac{\frac{m^*(t)}{p^*(t)} + \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}}{1 + \frac{m^*(t)}{p^*(t)} \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}} \geq \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}}$$

and if the denominator is positive for all $t \in [1/3, 1]$, we have

$$1 \geq \left(\frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}} \right)^2,$$

which is correct regarding Property 1. As the final step, we show that the denominator is positive. First, note that $\frac{\partial p^*}{\partial t} \geq 0$ and $\frac{\partial m^*}{\partial t} \leq 0$. Then,

$$1 + \frac{m^*(t)}{p^*(t)} \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}} \geq 1 + \frac{\frac{\partial m^*}{\partial t}}{\frac{\partial p^*}{\partial t}} \geq 0,$$

which is again satisfied because of Property 1, and the first inequality follows from the fact that $m^* \leq p^*$.

These together prove that for any $(p, m) \in \mathcal{R}_3^+$, (p^-, m^-) lies under the limiting curve and hence belongs to \mathcal{R}_3^+ . It straightforwardly follows from part (i) that (p^+, m^+) also belongs to \mathcal{R}_3^+ . Therefore once a pair (p, m) is driven into \mathcal{R}_3^+ , it remains there.

B. Proof of Lemma 5

To begin with, the following upper bound for the limiting curve will be useful for the proof.

Lemma 9. *The curve $\bar{m}(p) = C(1-p)^{3/2}$, $C \geq 2$ lies above the limiting curve.*

Proof: According to the parametric description (3), choose any $t \geq 1/3$. At this t , we have

$$\begin{aligned} p^*(t) &= \sqrt{4t^3 - 3t^4} \\ m^*(t) &= 1 - 3t + \frac{3}{2}t^2 + \frac{\sqrt{4t^3 - 3t^4}}{2}. \end{aligned}$$

For the chosen t , $\bar{m}(t) = C(1 - \sqrt{4t^3 - 3t^4})^{3/2}$. Now, one needs to check if

$$C(1 - \sqrt{4t^3 - 3t^4})^{3/2} \geq 1 - 3t + \frac{3}{2}t^2 + \frac{\sqrt{4t^3 - 3t^4}}{2}.$$

We use the upper bound $2t - t^2 \geq \sqrt{4t^3 - 3t^4}$ to obtain the stronger statement

$$\begin{aligned} C(1 - (2t - t^2))^{3/2} &\geq 1 - 3t + \frac{3}{2}t^2 + \frac{\sqrt{4t^3 - 3t^4}}{2} \\ \iff C(1 - t)^3 &\geq 1 - 3t + \frac{3}{2}t^2 + \frac{\sqrt{4t^3 - 3t^4}}{2} \end{aligned} \quad (5)$$

With a change of variable $v \triangleq 1 - t$ and rearranging the terms, we have

$$C \geq \frac{\frac{3}{2}v^2 - \frac{1}{2} + \frac{\sqrt{4(1-v)^3 - 3(1-v)^4}}{2}}{v^3} \triangleq g(v).$$

Observe that

$$\lim_{v \rightarrow 0} g(v) = 2, \quad g(1) = 1,$$

hence g is bounded in $(0, 1]$. Therefore, if one takes $C = \sup_{v \in (0, 1)} g(v)$, the inequality (5) is satisfied. We now show that $g(v)$ is decreasing in $(0, 1)$. Taking the derivative, we have

$$g'(v) = \frac{3\sqrt{1-v} \left((1-v)^2 - 2 + (1+v)\sqrt{(1-v)(1+3v)} \right)}{2v^4 \sqrt{(1+3v)}}.$$

It suffices to check if the nominator is non-positive in $(0, 1)$. To this end, we need to verify the following statement.

$$h(v) \triangleq (1-v)^2 - 2 + (1+v)\sqrt{(1-v)(1+3v)} \leq 0.$$

To find the extrema of $h(v)$ in $(0, 1)$, we take the derivative of $h(v)$ and equate to zero.

$$\begin{aligned} h'(v) &= -2(1-v) + \sqrt{(1-v)(1+3v)} \\ &\quad + \frac{(1+v)(1-3v)}{\sqrt{(1-v)(1+3v)}} = 0 \\ \iff -2(1-v)\sqrt{(1-v)(1+3v)} \\ &\quad + (1-v)(1+3v) + (1+v)(1-3v) = 0 \\ \iff 1-3v^2 - (1-v)\sqrt{(1-v)(1+3v)} &= 0 \\ \iff 1-3v^2 = (1-v)\sqrt{(1-v)(1+3v)} \\ \iff 1-6v^2+9v^4 = (1-v)^3(1+3v), \quad \text{for } v < \frac{1}{\sqrt{3}} \\ \iff 4v^3(3v-2) &= 0 \\ \iff v &= 2/3. \end{aligned}$$

However, $\frac{2}{3} > \frac{1}{\sqrt{3}}$. Therefore, $h(v)$ has no extremal points in $(0, 1)$. Observe that h is continuous and $h(0) = 0$, $h(1) = -1$. These together imply $h(v) < 0$ for $v \in (0, 1)$. Hence we have shown that $g'(v) < 0$ for $v \in (0, 1)$ and $g(v)$ is decreasing on the same interval. Finally, we obtain $\sup_{v \in (0, 1)} g(v) = 2$. ■

We are now in position to prove Lemma 5.

Let $C_n \triangleq \frac{Z_n^2}{P_n M_n}$. Choose a δ such that $\delta < \epsilon_r$ and $\delta(2 + \delta)e^\delta - \frac{4}{\log \delta} \leq 1/2$ (e.g. $\delta < 0.003$). Choose a small $\epsilon > 0$.

Now, define the event $\mathcal{A}_n(\delta) \triangleq \{P_n \geq 1 - \delta\}$. From the almost sure convergence of P_n , we know that

$$\mathbb{P}(\cup_m \cap_{n \geq m} \mathcal{A}_n(\delta)) = \lim_m \mathbb{P}(\cap_{n \geq m} \mathcal{A}_n(\delta)) = \gamma.$$

The sequence above is increasing. Hence, given ϵ , there exists an $n_0(\delta, \epsilon)$ such that

$$\mathbb{P}(\cap_{n \geq n_0} \mathcal{A}_n(\delta)) \geq \gamma - \epsilon/3.$$

This also implies that $\mathbb{P}(\cap_{k=n_0}^n \mathcal{A}_k(\delta)) \geq \gamma - \epsilon/3$ for any $n \geq n_0$. Define $\mathcal{B}_{n,m}(\delta) \triangleq \cap_{k=m}^n \mathcal{A}_k(\delta)$. For any $s_n \in \mathcal{B}_{n,n_0}(\delta)$, $n \geq n_0$, the iterations for C_{n+1} can be upper bounded as below. We drop the subscripts and use lowercase characters for simplicity.

$$\begin{aligned} c^+ &= \frac{(z^2 + 2mp)^2}{mp(m+2z)(p+2z)} = \frac{mp(z^2/mp + 2)^2}{(m+2z)(p+2z)} \\ &\leq \frac{mp(z^2/mp + 2)^2}{mp + 4z^2 + 2z(m+p)} = \frac{(c+2)^2}{3+4c} \\ &\leq \begin{cases} c, & c > \frac{4}{3} \\ \frac{4}{3}, & c \leq \frac{4}{3} \end{cases} \\ c^- &= \frac{(2z - z^2)^2}{2mp(p^2 + m^2)} = \frac{c(1+m+p)^2}{2(p^2 + m^2)} \leq c \left(1 + \frac{1}{m+p}\right)^2 \\ &\leq c \left(\frac{2-\delta}{1-\delta}\right)^2 \leq 9c \end{aligned}$$

since $\delta < 1/2$. We create another process D_n as follows: Let $C^*(\delta, \epsilon) = C_{n_0}^* \triangleq \max_{s_{n_0} \in \{+, -\}^{n_0}} c^{s_{n_0}} \vee \frac{4}{3}$. Then,

$$D_{n+1} = 9D_n, \quad n \geq n_0,$$

$$D_{n_0} = C_{n_0}^*.$$

It is easy to see that for any $s_n \in \mathcal{B}_{n,n_0}(\delta)$, $n \geq n_0$; D_n dominates C_n and therefore,

$$C_n \leq C^*(\delta, \epsilon) 9^{n-n_0}. \quad (6)$$

Let $A_n \triangleq -\log M_n$, $B_n \triangleq -\log Z_n$. For $s_n \in \mathcal{B}_{n,n_0}(\delta)$, $n \geq n_0$, we derive upper and lower bounds for a^+ , a^- and b^+ , b^- :

$$a - 1 \leq a^- \leq a,$$

$$b - 1 \leq b^- \leq b,$$

$$a + b - \log 3 \leq a^+ \leq a + b - 1,$$

$$\left(a - n \log 9 - \log C^* - \left(1 + \frac{2}{C^* 9^n} \right) \right) \vee \log(1/\delta) \leq b^+ \leq a. \quad (7)$$

The last inequality is obtained using (6) and knowing $Z_n \leq \delta$.

The upper bound derived in Lemma 9 yields

$$\begin{aligned} z^+ &= z^2 + 2mp \leq z^2 + 4(z+m)^{3/2} \\ &\leq z^2 + 4(2z)^{3/2} \\ &\leq 13z^{3/2} \end{aligned} \quad (8)$$

and we already have

$$z^- \leq 2z. \quad (9)$$

Now, define $\mathcal{G}_{n,n_0}(\beta)$ as the event $\sum_{k=n_0}^n \mathbb{1}_{\{S_k=+\}} \geq (n-n_0)\beta$, $\beta < 1/2$. For sufficiently large n , we know that $\mathcal{G}_{n,n_0}(\beta)$ occurs with high probability as a result of the law of large numbers. This implies the existence of $n_1 \geq n_0$ satisfying $\mathbb{P}(\mathcal{G}_{n,n_0}(\beta)) \geq 1 - \epsilon/3$, $n \geq n_1$. Note that $\mathbb{P}(\mathcal{G}_{n,n_0}(\beta) \cap \mathcal{B}_{n,n_0}) \geq \gamma - 2\epsilon/3$ for $n \geq n_1$.

Using the same machinery in [3], one can refer to inequalities (8), (9) and show that there exists an $n_2 \geq n_0$ such that for any $s_n \in \mathcal{G}_{n,n_0}(\beta) \cap \mathcal{B}_{n,n_0}$, both $(n \log 9)/B_n + \log C^*(\delta, \epsilon) + (1 + \frac{2}{C^* 9^n})/B_n \leq 2^{-\alpha' n}$ and $\log(1/\delta)/B_n \leq 2^{-\alpha' n}$ for any $\alpha' < \log 1.5/2$ and $n \geq n_2$.

Define $R_n \triangleq A_n/B_n$. Again, from the upper bound in Lemma 9 one observes that $M_n \leq 2(4Z_n)^{3/2}$. Thus $R_n = \frac{\log M_n}{\log Z_n} \geq \frac{3}{2} + \frac{4}{\log Z_n} \geq \frac{3}{2} + \frac{4}{\log \delta} \geq 1 + \delta(2 + \delta)e^\delta$ for all $s_n \in \mathcal{B}_{n,n_0}(\delta)$ and for the previously chosen δ .

Referring to (7), we have the following upper bound for r^+ .

$$r^+ \leq \frac{-1/b + 1 + r}{\left(r - n \log 9/b - \log C^*/b - \left(1 + \frac{2}{C^* 9^n} \right)/b \right) \vee \log(1/\delta)/b}$$

For $n \geq n_3 \triangleq n_1 \vee n_2$ and same kind of s_n , we know $r > 1$, $n \log 9/b + \log C^*/b + (1 + \frac{2}{C^* 9^n})/b \leq 2^{-\alpha' n}$ and $\log(1/\delta)/b \leq 2^{-\alpha' n}$. Hence, the upper bound becomes

$$r^+ \leq \frac{1 + r - 2^{-\alpha' n}}{r - 2^{-\alpha' n}}.$$

In similar manner, iterations for R_n are bounded as

$$\frac{1 + r - 2^{-\alpha' n}}{r} \leq r^+ \leq \frac{1 + r - 2^{-\alpha' n}}{r - 2^{-\alpha' n}}$$

and

$$r - 2^{-\alpha' n} \leq r^- \leq \frac{r}{1 - 2^{-\alpha' n}}.$$

From these, one concludes that

$$\left| R_{n+1}^+ - \left(\frac{R_n + 1}{R_n} \right) \right| \leq 2^{-\alpha' n+1} \quad (10)$$

and

$$R_n - 2^{-\alpha' n+1} \leq R_{n+1}^- \leq R_n(1 + 2^{-\alpha' n+1}). \quad (11)$$

Now, choose an n_4 such that $n_4 \triangleq \left\lceil \frac{1}{\alpha'} \log \left(\frac{2(2+\delta)e^\delta}{\delta(1-2^{-\alpha'})} \right) \right\rceil \vee n_3$. Define $\sigma_n \triangleq 2 \sum_{k=n_4}^n 2^{-\alpha' k}$ and observe $\sigma_n \leq 2 \sum_{k=n_4}^\infty 2^{-\alpha' k} \leq \delta$ for $n \geq n_4$. Since $R_n > 1$, the $+$ iteration ensures that $R_{n+1}^+ \leq 2 + 2^{-\alpha' n+1} \leq 2 + \delta$. Note that after exposed to $+$ transformation once, even infinitely many $-$ transformations cannot force R_n to grow unboundedly as

$$R_\infty^{(-\infty)} \leq (2 + \delta) \prod_{k=n_4}^\infty (1 + 2^{-\alpha' k+1}) \leq (2 + \delta) e^\delta.$$

This shows that R_n is bounded with probability close to γ . Using the upper bound found above, we obtain

$$|R_{n+1}^- - R_n| \leq (2 + \delta) e^\delta 2^{-\alpha' n+1}. \quad (12)$$

Define another process X_n such that $X_{n_4} = R_{n_4}$ and

$$X_{n+1}^+ = \frac{X_n + 1}{X_n}, \quad X_{n+1}^- = X_n, \quad n \geq n_4.$$

Using all these facts, we can also show that

$$|R_n - X_n| \leq (2 + \delta) e^\delta \sigma_{n-1}, \quad n \geq n_4. \quad (13)$$

This follows by induction. The base case is easily proven from inequalities (10) and (12). We now verify the other cases. Assuming the induction hypothesis we have $|R_n - X_n| \leq (2 + \delta) e^\delta \sigma_{n-1}$.

For $-$ iteration, we have

$$|R_{n+1}^- - X_{n+1}^-| \leq |R_n - X_n| + (2 + \delta) e^\delta 2^{-\alpha' n+1} = (2 + \delta) e^\delta \sigma_n.$$

For $+$ iteration, we have

$$\begin{aligned} |R_{n+1}^+ - X_{n+1}^+| &= \left| R_{n+1}^+ - \frac{X_n + 1}{X_n} \right| \\ &\leq \left| \frac{R_n + 1}{R_n} - \frac{X_n + 1}{X_n} \right| + 2^{-\alpha' n+1}. \end{aligned}$$

We have assumed that $|R_n - X_n| \leq (2 + \delta) e^\delta \sigma_{n-1}$. Note that since for all $n \geq n_4$, $\sigma_n \leq \delta$, this also implies $|R_n - X_n| \leq (2 + \delta) e^\delta \delta$. Recall that $R_n \geq 1 + \delta(2 + \delta) e^\delta$ for all $s_n \in \mathcal{B}_{n,n_0}(\delta)$ and therefore $X_n \geq 1$ for such s_n . The magnitude of derivative of $\frac{x+1}{x}$ is bounded by 1 on $[1, \infty)$. Hence,

$$\left| \frac{R_n + 1}{R_n} - \frac{X_n + 1}{X_n} \right| \leq |R_n - X_n| \leq (2 + \delta) e^\delta \sigma_{n-1}$$

and

$$|R_{n+1}^+ - X_{n+1}^+| \leq (2 + \delta) e^\delta \sigma_{n-1} + 2^{-\alpha' n+1} \leq (2 + \delta) e^\delta \sigma_n.$$

Therefore, we have proved the inequality (13) for all $n \geq n_4$. As we also have $(2 + \delta) e^\delta \sigma_n \leq \delta$, we deduce

$$|R_n - X_n| \leq \delta, \quad n \geq n_4. \quad (14)$$

Finally, we know that for any $s_n \in \mathcal{G}_{n,n_4}(\beta)$ and sufficiently large n , there will be arbitrarily large number of $+$ operations with high probability, say $\epsilon/3$. Since $|X_{n+1}^+ - \phi| = \left| \frac{X_n + 1}{X_n} - \frac{\phi + 1}{\phi} \right| = \left| \frac{X_n - \phi}{X_n \phi} \right| < \frac{1}{\phi} |X_n - \phi|$, X_n converges to ϕ . This shows the existence of an $n_5 \geq n_4$ such that

$$|X_n - \phi| < \epsilon_r - \delta \text{ and } \mathbb{P}(\mathcal{G}_{n_5,n_4}(\beta)) \geq 1 - \epsilon/3, \quad n \geq n_5. \quad (15)$$

(14) and (15) imply $|R_n - \phi| \leq \epsilon_r$ for $n \geq n_5$ and $s_n \in \mathcal{G}_{n,n_0}(\beta) \cap \mathcal{B}_{n,n_0} \cap \mathcal{G}_{n,n_4}(\beta) = \mathcal{B}_{n,n_0} \cap \mathcal{G}_{n,n_0}(\beta)$ where

$$\mathbb{P}(\mathcal{B}_{n,n_0} \cap \mathcal{G}_{n,n_0}(\beta)) \geq \gamma - \epsilon/3 - \epsilon/3 - \epsilon/3 = \gamma - \epsilon, \quad n \geq n_5.$$

C. Proof of Theorem 1

We continue from the proof of Lemma 5. For all $s_n \in \mathcal{B}_{n,n_0} \cap \mathcal{G}_{n,n_0}(\beta)$, $n \geq n_5$; we have $Z_n^{\phi+\epsilon_r} \leq M_n \leq Z_n^{\phi-\epsilon_r}$. Therefore, one obtains the following upper and lower bounds for iterations of Z_n .

$$\frac{1}{3} z^{\phi+\epsilon_r} \leq z^+ \leq 3z^{\phi-\epsilon_r}, \quad \frac{1}{2} z \leq z^- \leq 2z. \quad (16)$$

Let $\bar{\beta} \triangleq 1 - \beta$. For a sufficiently large n_6 , $\mathcal{G}_{n_6,n_5}(\beta) \cap \mathcal{G}_{n_6,n_5}(\bar{\beta})^C$ occurs with high probability. For once again, the same machinery in [3] is used to obtain

$$2^{-2^{n\bar{\beta}}(\log \phi + \delta'')} \leq Z_n \leq 2^{-2^{n\bar{\beta}}(\log \phi - \delta')} \quad (17)$$

for $n > n_6$, and any $\delta', \delta'' > 0$ which proves the first part of the theorem.

For the second part, the upper and lower bounds on iterations of M_n are given by

$$\frac{1}{3} m^{1+1/(\phi-\epsilon_r)} \leq m_+ \leq 3m^{1+1/(\phi+\epsilon_r)}, \quad \frac{1}{2} m \leq m_- \leq 2m.$$

Observe that $1 + \frac{1}{\phi+\epsilon_r} \geq \phi - \epsilon_r$ and $1 + \frac{1}{\phi-\epsilon_r} \leq \phi + \epsilon_r$ for small ϵ_r . Now, the same argument that we used to show (17) from (16) allows us to conclude

$$2^{-2^{n\bar{\beta}}(\log \phi + \delta'')} \leq M_n \leq 2^{-2^{n\bar{\beta}}(\log \phi - \delta')}$$

from the bounds on m^+ and m^- .