Electronic Colloquium on Computational Complexity, Report No. 50 (2013)

Polar Codes: Speed of polarization and polynomial gap to capacity

Venkatesan Guruswami* Patrick Xia†

Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

We prove that, for all binary-input symmetric memoryless channels, polar codes enable reliable communication at rates within $\varepsilon > 0$ of the Shannon capacity with a block length, construction complexity, and decoding complexity all bounded by a *polynomial* in $1/\varepsilon$. Polar coding gives the *first known explicit construction* with rigorous proofs of all these properties.

We give an elementary proof of the capacity achieving property of polar codes that does not rely on the martingale convergence theorem. As a result, we are able to explicitly show that polar codes can have block length (and consequently also encoding and decoding complexity) that is bounded by a polynomial in the gap to capacity. The generator matrix of such polar codes can be constructed in polynomial time using merging of channel output symbols to reduce the alphabet size of the channels seen at the decoder.

1 Introduction

In this work, we establish that Arıkan's celebrated polar codes [2] have the desirable property of fast convergence to Shannon capacity. Specifically, we prove that polar codes can operate at rates within $\varepsilon > 0$ of the Shannon capacity of binary-input memoryless output-symmetric (BIS) channels with a block length $N = N(\varepsilon)$ that grows only polynomially in $1/\varepsilon$. Further, a generator matrix of such a code can be deterministically constructed in time polynomial in the block length N. For decoding, Arıkan's successive cancellation decoder has polynomial (in fact $\mathcal{O}(N \log N)$) complexity.

Thus, the delay and construction/decoding complexity of polar codes can *all* be polynomially bounded as a function of the gap to capacity. This provides a complexity-theoretic backing for the statement "polar codes are the first constructive capacity achieving codes," common in the recent coding literature. As explained below, these attributes together distinguish polar codes from the Forney/Justesen style concatenated code constructions for achieving capacity.

Our analysis of polar codes avoids the use of the martingale convergence theorem — this is instrumental in our polynomial convergence bounds and as a side benefit makes the proof elementary and self-contained.

*Research supported in part by a Packard Fellowship, MSR-CMU Center for Computational Thinking, and NSF CCF-0963975. Email: guruswami@cmu.edu

†Research supported in part by an NSF graduate fellowship and NSF CCF-0963975. Email: pjx@cs.cmu.edu

ISSN 1433-8092

1.1 Context

Shannon's noisy channel coding theorem implies that for every memoryless channel W with binary inputs and a finite output alphabet, there is a capacity $I(W) \geqslant 0$ and constants $a_W < \infty$ and $b_W > 0$ such that the following holds: For all $\varepsilon > 0$ and integers $N \geqslant a_W/\varepsilon^2$, there *exists* a binary code $C \subset \{0,1\}^N$ of rate at least $I(W) - \varepsilon$ which enables reliable communication on the channel W with probability of miscommunication at most $2^{-b_W \varepsilon^2 N}$. A proof implying these quantitative bounds is implicit in Wolfowitz's proof of Shannon's theorem [24].

This remarkable theorem showed that a constant factor redundancy was sufficient to achieve arbitrarily small probability of miscommunication, provided we tolerate a "delay" of processing N channel outputs at a time for large enough block length N. Further, together with a converse theorem, it precisely characterized the minimum redundancy factor (namely, $1/I(W)$) needed to achieve such a guarantee. It is also known that a block length of $N \geqslant \Omega(1/\varepsilon^2)$ is required to operate within ε of capacity and even a constant, say 0.1, probability of miscommunication; in fact, a very precise statement that even pinned down the constant in the $\Omega(\cdot)$ notation was obtained by Strassen [21].

As Shannon's theorem is based on random coding and is non-constructive, one of the principal theoretical challenges is to make it constructive. More precisely, the goal is to give an explicit (i.e., constructible in deterministic poly(N) time) description of the encoding function of the code, and a polynomial time error-correction algorithm for decoding the correct transmitted codeword with high probability (over the noise of the channel). Further, it is important to achieve this with small block length N as that corresponds to the delay at the receiver before the message bits can be recovered.

For simplicity let us for now consider the binary symmetric channel (BSC) with crossover probability p, $0 < p < 1/2$, denoted BSC_p (our results hold for any BIS channel). Recall that BSC_p flips each input bit independently with probability p, and leaves it unchanged with probability $1-p$. The Shannon capacity of BSC_p is $1 - h(p)$, where $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. For the BSC, the capacity can be achieved by binary linear codes.

One simple and classic approach to *construct* capacity-achieving codes is via Forney's concatenated codes [9]. We briefly recall this approach (see, for instance, [11, Sec. 3] for more details). Suppose we desire codes of rate $1 - h(p) - \varepsilon$ for communication on BSC_p. The idea is to take as an outer code any binary linear code $C_{\text{out}} \subset \{0,1\}^{n_0}$ of rate $1-\varepsilon/2$ that can correct a fraction $\gamma(\varepsilon) > 0$ of worst-case errors. Then, each block of $b = \Theta(\frac{1}{\varepsilon^2}\log(1/\gamma))$ bits of the outer codeword is further encoded by an inner code of rate within $\varepsilon/2$ of Shannon capacity (i.e., rate at least $1 - h(p) - \varepsilon/2$). This inner code is constructed by brute force in time $\exp(\mathcal{O}(b))$. By decoding the inner blocks by finding the nearest codeword in $\exp(\mathcal{O}(b))$ time, and then correcting up to $\gamma(\varepsilon)n_0$ errors at the outer level, one can achieve exponentially small decoding error probability. However the decoding complexity grows like $n_0 \exp(\mathcal{O}(b))$. Thus both the construction and decoding complexity have an exponential dependence on $1/\varepsilon$. In conclusion, this method allows one to obtain codes within ε of capacity with a block length polynomially large in $1/\varepsilon$. However, the construction and decoding complexity grow exponentially in $1/\varepsilon$, which is undesirable.[1]

[1] One can avoid the brute force search for a good inner code by using a small ensemble of capacity-achieving codes in a Justesen-style construction [15]. But this will require taking the outer code length $n_0 > \exp(1/\varepsilon^2)$, causing a large delay.

1.2 Our result: polynomial convergence to capacity of polar codes

In this work, we prove that Arıkan's remarkable polar codes allow us to approach capacity within a gap $\varepsilon > 0$ with *delay* (block length) and *complexity* both depending polynomially on $1/\varepsilon$. Polar codes are the *first* known construction with this property.[2]

Below is a formal statement of the main result, stated for BIS channels. For general, non-symmetric channels, the same claim holds for achieving the *symmetric capacity*, which is the best rate achievable with the uniform input bit distribution.

Theorem 1. *There is an absolute constant $\mu < \infty$ such that the following holds. Let W be a binary-input memoryless output-symmetric channel with capacity $I(W)$. Then there exists $a_W < \infty$ such that for all $\varepsilon > 0$ and all powers of two $N \geqslant a_W(1/\varepsilon)^\mu$, there is a deterministic* $\text{poly}(N)$ *time construction of a binary linear code of block length N and rate at least $I(W) - \varepsilon$ and a deterministic $N \cdot \text{poly}(\log N)$ time decoding algorithm for the code with block error probability at most $2^{-N^{0.49}}$ for communication over W.*

Remarks:

1. Using our results about polar codes, we can also construct codes of rate $I(W) - \varepsilon$ with $2^{-\Omega_\varepsilon(N)}$ block error probability (similar to Shannon's theorem) with similar claims about the construction and decoding complexity. The idea is to concatenate an outer code that can correct a small fraction of worst-case errors with a capacity-achieving polar code of dimension $\text{poly}(1/\varepsilon)$ as the inner code. A similar idea with outer Reed-Solomon codes yielding $2^{-\Omega(N/\text{poly}(\log N))}$ block error probability is described in [6].

2. The construction time in Theorem 1 can be made $\text{poly}(1/\varepsilon) + \mathcal{O}(N \log N)$. As our main focus is on the finite-length behavior when N is also $\text{poly}(1/\varepsilon)$, we are content with stating the $\text{poly}(N)$ claim above.

Showing that polar codes have a gap to capacity that is polynomially small in $1/N$ is our principal contribution. The decoding algorithm remains the same successive cancellation decoder of Arıkan [2]. The proof of efficient constructibility follows the approach, originally due to Tal and Vardy [22], of approximating the channels corresponding to different input bits seen at the decoder by a degraded version with a smaller output alphabet. The approximation error of this process and some of its variants were analyzed in [19]. We consider and analyze a somewhat simpler degrading process. One slight subtlety here is that we can only estimate the channel's Bhattacharyya parameter within error that is polynomial in $1/N$ in $\text{poly}(N)$ time, which will limit the analysis to an inverse polynomial block error probability. To get a block error probability of $2^{-N^{0.49}}$ we use a two step construction method that follows our analysis of the polarization process. As a bonus, this gives the better construction time alluded to in the second remark above.

Prior to our work, it was known that the block error probability of successive cancellation decoding of polar codes is bounded by $2^{-N^{0.49}}$ for rate approaching $I(W)$ in the limit of $N \to \infty$ [5]. However, the underlying analysis found in [5], which depended on the martingale convergence

[2] Spatially coupled LDPC codes were also recently shown to achieve capacity of general BIS channels [18]. This construction gives a random code ensemble as opposed to a specific code, and as far as we know, rigorous bounds on the code length as a function of gap to capacity are not available.

theorems, did not offer any bounds on the finite-length convergence to capacity, i.e., the block length N required for the rate to be within ε of the capacity $I(W)$. To quote from the introduction of the recent breakthrough on spatially coupled LDPC codes [18]:

> "There are perhaps only two areas in which polar codes could be further improved. First, for polar codes the convergence of their performance to the asymptotic limit is slow. Currently no rigorous statements regarding this convergence for the general case are known. But "calculations" suggest that, for a fixed desired error probability, the required block length scales like $1/\delta^{\mu}$, where δ is the additive gap to capacity and where μ depends on the channel and has a value around 4."[3]

The above-mentioned heuristic calculations are based on "scaling laws" and presented in [17]. We will return to the topic of scaling laws in Section 1.4 on related work.

We note that upper bounds on the block length N as a function of gap ε to capacity are crucial, as without those we cannot estimate the complexity of communicating at rates within ε of capacity. Knowing that the asymptotic complexity is $\mathcal{O}(N \log N)$ for large N by itself is insufficient (for example, to claim that polar codes are better than concatenated codes) as we do not know how large N has to be! While an explicit value of μ in Theorem 1 can be calculated, it will be rather large, and obtaining better bounds on μ, perhaps closer to the empirically suggested bound of ≈ 4, is an interesting open problem[4].

1.3 Techniques

Let us first briefly discuss the concept of polarization in Arıkan's work, and then turn to aspects of our work. More formal background on Arıkan's construction of polar codes appears in Section 3 (with slightly different and notation that is more conventional in the polar coding literature). A good, easy to read, reference on polar codes is the recent survey by Şaşoğlu [7].

Fix W to be an arbitrary symmetric channel. If we have a capacity-achieving binary linear code C of block length N for W, then it is not hard to see that by padding the generator matrix of C one can get an $N \times N$ invertible matrix A_N with the following *polarization property*. Let $\mathbf{u} \in \{0,1\}^N$ be a uniformly random (column) vector. Given the output $\mathbf{y}$ of W when the N bits $\mathbf{x} = A_N \mathbf{u}$ are transmitted on it, for a $1 - o(1)$ fraction of bits u_i, its conditional entropy given $\mathbf{y}$ and the previous bits $u_1, \ldots, u_{i-1}$ is either close to 0 (i.e., that bit can be determined with good probability) or close to 1 (i.e., that bit remains random). Since the conditional entropies of $\mathbf{u}$ given $\mathbf{y}$ and $\mathbf{x}$ given $\mathbf{y}$ are equal to each other, and the latter is $\approx (1 - I(W))N$, the fraction of bits u_i for which the conditional entropy given $\mathbf{y}$ and the previous bits $u_1, \ldots, u_{i-1}$ is ≈ 0 (resp. ≈ 1) is $\approx I(W)$ (resp. $\approx 1 - I(W)$).

Arıkan gave a recursive construction of such a polarizing matrix A_N for $N = 2^n$: $A_N = G_2^{\otimes n} B_n$ where $G_2 = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and B_n is a permutation matrix (for the bit-reversal permutation). In addition, he showed that the recursive structure of the matrix implied the existence of an efficiently decodable capacity-achieving code. The construction of this code amounts to figuring out which input bit

[3] The second aspect concerns *universality*: the design of polar codes depends on the channel being used, and the same code may not achieve capacity over a non-trivial class of channels.

[4] While we were completing the writeup of this paper and circulating a draft, we learned about a recent independently-derived result in [12] stating that $\mu \approx 6$ would suffice for block error probabilities bounded by an inverse polynomial. Our analysis primarily focuses on the $2^{-N^{.49}}$ block error probability result.

positions have conditional entropy ≈ 0, and which don't (the message bits u_i corresponding to the latter positions are "frozen" to 0).

The proof that A_N has the above polarization property proceeds by working with the Bhattacharyya parameters $Z_n(i) \in [0,1]$ associated with decoding u_i from $\mathbf{y}$ and $u_1, \dots, u_{i-1}$. This quantity is the Hellinger affinity between the output distributions when $u_i = 0$ and $u_1 = 1$, and is a better quantity that conditional entropy to work with. The values of the Bhattacharyya parameter of the 2^n bit positions at the n'th level can be viewed as a random variable Z_n (induced by the uniform distribution on the 2^n positions). The simple recursive construction of A_N enabled Arıkan to proved that the sequence of random variables $Z_0, Z_1, Z_2, \dots$ form a supermartingale. In particular, Z_{n+1} equals Z_n^2 with probability 1/2 and is at most $2Z_n - Z_n^2$ with probability 1/2. [5]

One can think the evolution of the Bhattacharyya parameter as a stochastic process on the infinite binary tree, where in each step we branch left or right with probability 1/2. The polarization property is then established by invoking the martingale convergence theorem for supermartingales. The martingale convergence theorem implies that $\lim_{n\to\infty} |Z_{n+1} - Z_n| = 0$, which in this specific case also implies $\lim_{n\to\infty} Z_n(1 - Z_n) = 0$ or in other words polarization of Z_n to 0 or 1 for $n \to \infty$. However, it does *not* yield any effective bounds on the *speed* at which polarization occurs. In particular, it does not say how large n must be as a function of ε before $\mathbb{E}[Z_n(1 - Z_n)] \leqslant \varepsilon$; such a bound is necessary, though not sufficient, to get codes of block length 2^n with rate within ε of capacity.

Starting at the root, the expected number of steps before which $Z_n(1 - Z_n) \leqslant \varepsilon$ for the first time can be as large as $\Omega(1/\varepsilon)$, even for the binary erasure channel. Note that we need a bound of $n \leqslant \mathcal{O}(\log(1/\varepsilon))$ to have any hope of obtaining a polynomial dependence of the block length on the gap to capacity. Thus this situation demands that with high probability $\mathcal{O}(\log(1/\varepsilon))$ steps suffice (for $Z_n(1 - Z_n)$ to fall below ε) even though the expected number of steps for this to happen is $\Omega(1/\varepsilon)$.

Rather than trying to control the ill-behaved random variable that counts the number of steps needed for $Z_n(1-Z_n)$ to drop below ε, we simply prove that $\mathbb{E}[Z_n(1-Z_n)]$ decreases by a constant factor in each step. This immediately implies that $\mathbb{E}[Z_n(1 - Z_n)] \leqslant \rho^n$ for some $\rho < 1$, and thus $n = \mathcal{O}(\log(1/\varepsilon))$ suffices to ensure $\mathbb{E}[Z_n(1 - Z_n)] \leqslant \varepsilon$ (we call this *rough polarization*).

The above expectation bound is itself, however, not enough to prove Theorem 1. What one needs is *fine polarization*, where the smallest $\approx I(W)N$ values among $Z_n(i)$ all *add up* to a quantity that tends to 0 for large N (in fact, this sum should be at most $2^{-N^{0.49}}$ if we want the block error probability claimed in Theorem 1). We establish this by using Chernoff-bound arguments (similar to [5]) to bootstrap the rough polarization to a fine polarization.

Our analysis is elementary and self-contained, and does not use the martingale convergence theorem. The ingredients in our analysis were all present explicitly or implicitly in various previous works. However, it appears that their combination to imply a polynomial convergence to capacity has not been observed before, as evidenced by the explicit mention of this as an open problem in the literature, eg. [16, Section 6.6], [18, Section Ia], [23, Section I], [20, Section 1.3].

[5] For the special case of the binary erasure channel, the Bhattacharyya parameters simply equal the probability that the bit is unknown. In this case, the upper bound of $2Z_n - Z_n^2$ becomes an exact bound, and the Z_i's form a martingale.

1.4 Related work

The simplicity and elegance of the construction of polar codes, and their wide applicability to a range of classic information theory problems, have made them a popular choice in the recent literature. Here we only briefly discuss aspects close to our focus on the speed of polarization.

Starting with Arıkan's original paper, the "rate of polarization" has been studied in several works. However, this refers to something different than our focus; this is why we deliberately use the term "speed of polarization" to refer to the question of how large n needs to be before, say, Z_n is in the range $(\varepsilon, 1-\varepsilon)$ with probability ε. The rate of polarization refers to pinpointing a function Υ with $\Upsilon(n) \to 0$ for large n such that $\lim_{n\to\infty} \Pr[Z_n \leqslant \Upsilon(n)] = I(W)$. Arıkan proved that one can take $\Upsilon(n) = O(2^{-5n/4})$ [2], and later Arıkan and Telatar established that one can take $\Upsilon(n) = 2^{-2^{\beta n}}$ for any $\beta < 1/2$ [5]. Further they proved that for $\gamma > 1/2$, $\lim_{n\to\infty} \Pr[Z_n \leqslant 2^{-2^{\gamma n}}] = 0$. This determined the rate at which the Bhattacharyya parameters of the "noiseless" channels polarize to 0 in the limit of larger n. More fine grained bounds on this asymptotic rate of polarization as a function of the code rate were obtained in [13].

For our purpose, to get a finite-length statement about the performance of polar codes, we need to understand the speed at which $\Pr[Z_n \leqslant \Upsilon(n)]$ approaches the limit $I(W)$ as n grows (any function Υ with $\Upsilon(n) = o(1/2^n)$ will do, though we get the right $2^{-2^{0.49n}}$ type decay).

Restated in our terminology, in [10] the authors prove the following "negative result" concerning gap to capacity: For polar coding with successive cancellation (SC) decoding to have vanishing decoding error probability at rates within ε of capacity, the block length has to be *at least* $(1/\varepsilon)^{3.553}$. (A slight caveat is that this uses the sum of the error probabilities of the well-polarized channels as a proxy for the block error probability, whereas in fact this sum is only an upper bound on the decoding error probability of the SC decoder.)

Also related to the gap to capacity question is the work on "scaling laws," which is inspired by the behavior of systems undergoing a phase transition in statistical physics. In coding theory, scaling laws were suggested and studied in the context of iterative decoding of LDPC codes in [1]. In that context, for a channel with capacity C, the scaling law posits the existence of an exponent μ such that the block error probability $P_e(N, R)$ as a function of block length N and rate R tends in the limit of $N \to \infty$ while fixing $N^{1/\mu}(C - R) = x$, to $f(x)$ where f is some function that decreases smoothly from 1 to 0 as its argument changes from $-\infty$ to $+\infty$. Coming back to polar codes, in [17], the authors make a *Scaling Assumption* that the probability $Q_n(x)$ that Z_n exceeds x is such that $\lim_{n\to\infty} N^{1/\mu} Q_n(x)$ exists and equals a function $Q(x)$. Under this assumption, they use simulations to numerically estimate $\mu \approx 3.627$ for the BEC. Using the small x asymptotics of $Q(x)$ suggested by the numerical data, they predict an $\approx (1/\varepsilon)^{\mu}$ upper bound on the block length as a function of the gap ε to capacity for the BEC. For general channels, under the heuristic assumption that the densities of log-likelihood ratios behave like Gaussians, an exponent of $\mu \approx 4.001$ is suggested for the Scaling Assumption. However, to the best of our knowledge, it does not appear that one can get a rigorous upper bound on block length N as a function of the gap to capacity via these methods.

2 Preliminaries

We will work over a binary input alphabet $\mathcal{B} = \{0, 1\}$. Let $W : \mathcal{B} \to \mathcal{Y}$ be a binary-input memoryless symmetric channel with finite output alphabet $\mathcal{Y}$ and transition probabilities $\{W(y|x) : x \in \mathcal{B}, y \in \mathcal{Y}\}$. A binary-input channel is symmetric when the two rows of the transition probability matrix are permutations of each other; i.e., there exists a bijective mapping $\sigma : \mathcal{Y} \mapsto \mathcal{Y}$ where $\sigma = \sigma^{-1}$ and $W(y|0) = W(\sigma(y)|1)$ for all y. Both the binary erasure and binary symmetric channels are examples of symmetric channels.

Let X represent a uniformly distributed binary random variable, and let Y represent the result of sending X through the channel W.

The entropy of the channel W, denote $H(W)$, is defined as the entropy of X, the input, given the output Y, i.e., $H(W) = H(X|Y)$. It represents how much uncertainty there is in the input of the channel given the output of the channel. The mutual information of W, sometimes known as the capacity, and denoted $I(W)$, is defined as the mutual information between X and Y when the input distribution X is uniform:

$$I(W) = I(X;Y) = H(X) - H(X|Y) = 1 - H(X|Y) = 1 - H(W) \ .$$

We have $0 \leqslant I(W) \leqslant 1$, with a larger value meaning a less noisy channel. As the mutual information expression is difficult to work with directly, we will often refer to the Bhattacharyya parameter of W as a proxy for the quality of the channel:

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

This quantity is a natural one to capture the similarity between the channel outputs when the input is 0 and 1: $Z(W)$ is simply the dot product between the unit vectors obtained by taking the square root of the output distributions under input 0 and 1 (which is also called Hellinger affinity between these distributions).

Intuitively, the Bhattacharyya parameter $Z(W)$ should be near 0 when $H(W)$ is near 0 (meaning that it is easy to ascertain the input of a channel given the output), and conversely, $Z(W)$ is near 1 when $H(W)$ is near 1. This intuition is quantified by the following expression (where the upper bound is from [16, Lemma 1.5] and the lower bound is from [3]):

$$Z(W)^2 \leqslant H(W) \leqslant Z(W) \ . \tag{1}$$

Given a single output $y \in \mathcal{Y}$ from a channel W, we would like to be able to map it back to X, the input to the channel. The most obvious way to do this is by using the maximum-likelihood decoder:

$$\hat{X} = \operatorname*{argmax}_{x \in \mathcal{B}} \Pr(x|y) = \operatorname*{argmax}_{x \in \mathcal{B}} W(y|x)$$

where a decoding error is declared if there is a tie. Thus, the probability of error for a uniform input bit under maximum likelihood decoding is

$$P_e(W) = \Pr(\hat{X} \neq X) = \frac{1}{2} \sum_{x \in \mathcal{B}} \sum_{y \in \mathcal{Y}} W(y|x) \, \mathbf{1}_{W(y|x) \leqslant W(y|x \oplus 1)}$$

where $\mathbf{1}_x$ denotes the indicator function of x. Directly from this expression, we can conclude

$$P_e(W) \leqslant Z(W) \tag{2}$$

since $\mathbf{1}_{W(y|x) \leqslant W(y|x\oplus 1)} \leqslant \sqrt{W(y|x \oplus 1)}/\sqrt{W(y|x)}$, and the channel is symmetric (so the sum over $x \in \mathcal{B}$ and the 1/2 cancel out). Thus, the Bhattacharyya parameter $Z(W)$ also bounds the error probability of maximum likelihood decoding based on a single use of the channel W.

3 Polar codes

3.1 Construction preliminaries

This is a short primer on the motivations and techniques behind polar coding, following [2, 7]. Consider a family of invertible linear transformations $G_n : \mathcal{B}^{2^n} \to \mathcal{B}^{2^n}$ defined recursively as follows: $G_0 = [1]$ and for a $2N$-bit vector $u = (u_0, u_1, \dots, u_{2N-1})$ with $N = 2^n$, we define

$$G_{n+1}u = G_n(u_0 \oplus u_1, u_2 \oplus u_3, \dots, u_{2N-2} \oplus u_{2N-1}) \circ G_n(u_1, u_3, u_5, \dots, u_{2N-1}) \tag{3}$$

where $\circ$ is the vector concatenation operator. More explicitly, this construction can be shown to be equivalent to the explicit form $G_n = K^{\otimes n} B_n$ (see [2, Sec. VII]) where B_n is the $2^n \times 2^n$ bit-reversal permutation matrix for n-bit strings, $K = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\otimes$ denotes the Kronecker product.

Suppose we use the matrix G_n to encode a $N = 2^n$-size vector U, $X = G_n U$, and then transmit X over a binary symmetric channel W. It can be shown with a Martingale Convergence Theorem-based proof [2] that for all $\varepsilon > 0$,

$$\lim_{N\to\infty} \Pr_i \left[H(U_i | U_0^{i-1}, Y_0^{N-1}) < \varepsilon \right] = I(W). \tag{4}$$

where the notation U_i^j denotes the subvector $(U_i, U_{i+1}, \dots, U_j)$.

In words, there exists a *good set* of indices i so that for all elements in this set, given all of the outputs from the channel and (correct) decodings of all of the bits indexed less than i, the value of U_i can be ascertained with low probability of error (as it is a low-entropy random variable).

For every element that is outside of the good set, we do not have this guarantee; this suggests a encoding technique wherein we "freeze" all indices outside of this good set to a certain predefined value (0 will do). We call the indices that are not in the good set as the *frozen* set.

3.2 Successive cancellation decoder

The above distinction between good indices and frozen indices suggests a successive cancellation decoding technique where if the index is in the good set, we output the maximum-likelihood bit (which has low probability of being wrong due to the low entropy) or if the index is in the frozen set, we output the predetermined bit (which has zero probability of being incorrect). A sketch of such a successive cancellation decoder is presented in Algorithm 1.

Definition 1. *A polar code with frozen set $F \subset \{0, 1, \dots, N-1\}$ is defined as*

$$C_F = \{G_n u \mid u \in \{0,1\}^N, u_F = 0\} \ .$$

Algorithm 1: Successive cancellation decoder

```
input  : $y_0^{N-1}$, $F$, $W$
output: $u_0^{K-1}$
1  $\hat{u} \leftarrow$ zero vector of size $N$
2  for $i \in 0..N-1$ do
3      if $i \in F$ then
4          $\hat{u}_i \leftarrow 0$
5      else
6          if $\frac{\Pr(U_i=0|U_0^{i-1}=\hat{u}_0^{i-1},Y_0^{N-1}=y_0^{N-1})}{\Pr(U_i=1|U_0^{i-1}=\hat{u}_0^{i-1},Y_0^{N-1}=y_0^{N-1})} > 1$ then
7              $\hat{u}_i \leftarrow 0$
8          else
9              $\hat{u}_i \leftarrow 1$
10 return $\hat{u}_{\overline{F}}$
```

Remark. The probability ratio on line 6 can be computed with a naïve approach by recursively computing (where $n = \lg N$) $W_n^{(i)}(y_0^{N-1}, \hat{u}_0^{i-1}|x)$ for $x \in \mathcal{B}$ according to the recursive evolution equations (5),(6),(7). The result is true if the expression is larger for $x = 1$ than it is for $x = 0$, as by Bayes's theorem,

$$\Pr(U_i = 0|U_0^{i-1} = \hat{u}_0^{i-1}, Y_0^{N-1} = y_0^{N-1}) = \frac{W_n^{(i)}(y_0^{N-1}, \hat{u}_0^{i-1}|0)\Pr(u_i = 0)}{\Pr(U_0^{i-1} = \hat{u}_0^{i-1}, Y_0^{N-1} = y_0^{N-1})},$$

and the term in the denominator is present in both the $U_i = 0$ and $U_i = 1$ expression and therefore cancels in the division; the $\Pr(u_i = 0)$ term cancels as well for a uniform prior on u_i (which is necessary to achieve capacity for the symmetric channel W).
The runtime of the algorithm can be improved to $\mathcal{O}(N \log N)$ by computing the probabilities on line 6 with a divide-and-conquer approach as in [2]. We note that this runtime bound assumes constant-time arithmetic; consideration of n-bit arithmetic relaxes this bound to $\mathcal{O}(N\text{polylog}(N))$. For a treatment of more aggressive quantizations, see [12, Chapter 6].

By (4), if we take F to be the positions with conditional entropy exceeding ε, the rate of such a code would approach $I(W)$ in the limit $N \to \infty$.

To simplify the probability calculation (as seen on line 6 of Algorithm 1 and explained further in the comments), it is useful to consider the induced channel seen by each bit, $W_n^{(i)} : \mathcal{B} \to \mathcal{Y}^N \times \mathcal{B}^i$, for $0 \leqslant i \leqslant 2^n - 1$. Here, we are trying to ascertain the most probable value of the input bit U_i by considering the output from all channels Y_0^{N-1} and the (decoded) input from all channels before index i. Since the probability of decoding error at every step is bounded above by the corresponding Bhattacharyya parameter Z by (2), we can examine $Z(W_n^{(i)})$ as a proxy for $P_e(W_n^{(i)})$.

It will be useful to redefine $W_n^{(i)}$ recursively both to bound the evolution of $Z(W_n^{(i)})$ and to facilitate the computation. Consider the two transformations $^-$ and $^+$ defined as follows:

$$W^-(y_1, y_2|x_1) = \sum_{x_2 \in \mathcal{B}} \frac{1}{2} W(y_1|x_1 \oplus x_2)W(y_2|x_2) \tag{5}$$

and

$$W^+(y_1, y_2, x_1|x_2) = \frac{1}{2}W(y_1|x_1 \oplus x_2)W(y_2|x_2), \tag{6}$$

where we associate $^-$ with a "downgrading" transformation and $^+$ with a "upgrading" transformation. We notice that $W^- = W_1^{(0)}$ (the transformation $^-$ adds uniformly distributed noise from another input x_2, which is equivalent to the induced channel seen by the 0th bit) and $W^+ = W_1^{(1)}$ (where here we clearly have the other input bit).

More generally, by the recursive construction (3), one can conclude that the $W_n^{(i)}$ process can be redefined in a recursive manner as

$$W_{n+1}^{(i)} = \begin{cases} \left(W_n^{(\lfloor i/2 \rfloor)}\right)^- & \text{if } i \text{ is even} \\ \left(W_n^{(\lfloor i/2 \rfloor)}\right)^+ & \text{if } i \text{ is odd} \end{cases} \tag{7}$$

with the base channel $W_0^{(0)} = W$.

Importantly, we can now state the following lemma, which relates the Bhattacharyya parameters of the subchannels to the block error probability obtained by successive cancellation decoding.

Lemma 2. *The block error probability of Algorithm 1 on a polar code C of length n with frozen set F is bounded above by the sum of the Bhattacharyya parameters $\sum_{i \in \overline{F}} Z(W_n^{(i)})$.*

The proof is a simple application of the union bound. The probability of the i'th bit (that is not frozen) being misdecoded given the channel outputs and the input bits with index $< i$ is bounded above by $Z(W_n^{(i)})$ by Equation (2).

Importantly, the evolution processes (5) and (6) preserve information in the sense that

$$I(W^-) + I(W^+) = 2I(W), \tag{8}$$

which follows by the chain rule of mutual information, as (suppose X_1 is the input seen at W^- and X_2 is the input seen at W^+ and Y_1, Y_2 are the corresponding output variables)

$$I(W^-) + I(W^+) = I(X_1; Y_1, Y_2) + I(X_2; Y_1, Y_2|X_1) = I(X_1, X_2; Y_1, Y_2) = 2I(W).$$

3.3 Bounds on $Z(W^-)$ and $Z(W^+)$

The general technique of the proof of these bounds is borrowed from [2, 16], and the results are rederived in Appendix A for clarity and completeness.

Proposition 3. $Z(W^+) = Z(W)^2$ *for all binary symmetric channels W.*

Proposition 4. $Z(W)\sqrt{2 - Z(W)^2} \leqslant Z(W^-) \leqslant 2Z(W) - Z(W)^2$ *for all binary symmetric channels W, with equality holding in the upper bound on $Z(W^-)$ if the channel W is an erasure channel.*

4 Speed of polarization

Our first goal is to show that for some $m = \mathcal{O}(\log(1/\varepsilon))$, we have that $\Pr_i[Z(W_m^{(i)}) \leqslant 2^{-\mathcal{O}(m)}] \geqslant I(W) - \varepsilon$ (the channel is "roughly" polarized). We will then use this rough polarization result to show that, for some $n = \mathcal{O}(\log(1/\varepsilon))$, "fine" polarization occurs: $\Pr_i[Z(W_n^{(i)}) \leqslant 2^{-2^{\beta n}}] \geqslant I(W) - \varepsilon$. This approach is similar to the bootstrapping method used in [4].

4.1 Rough polarization

We will use what we call the *symmetric* Bhattacharyya parameter as a proxy for how polarized a channel is (in a sense, how close to 0 or 1 it is):

$$Y(W) = Z(W)(1 - Z(W)).$$

To relate $Y(W_n^{(i)})$ back to $Z(W_n^{(i)})$, it is useful to define the sets (where $\rho \in (0,1)$):

$$A_\rho^g = \left\{ i : Z(W_n^{(i)}) \leqslant \frac{1 - \sqrt{1 - 4\rho^n}}{2} \right\}, \; A_\rho^b = \left\{ i : Z(W_n^{(i)}) \geqslant \frac{1 + \sqrt{1 - 4\rho^n}}{2} \right\}, \text{ and} \tag{9}$$

$$A_\rho = A_\rho^g \cup A_\rho^b = \{ i : Y(W_n^{(i)}) \leqslant \rho^n \} .$$

We associate A_ρ^g with the "good" set (the set of i such that the Bhattacharyya parameter, and therefore probability of misdecoding, is small) and A_ρ^b with the "bad" set. We record the following useful approximations, both of which follow from $\sqrt{1 - 4\rho^n} \geqslant 1 - 4\rho^n$.

Fact 5. *For $i \in A_\rho^g$, $Z(W_n^{(i)}) \leqslant 2\rho^n$, and for $i \in A_\rho^b$, $Z(W_n^{(i)}) \geqslant 1 - 2\rho^n$.*

4.1.1 Binary erasure channel

If W is the binary erasure channel, we have $I(W_n) = 1 - Z(W_n)$ and $Z(W_n^-) = 2Z(W_n) - Z(W_n^2)$. In this case, we can show the following.

Proposition 6. *For the binary erasure channel W, for all $\alpha \in (3/4, 1)$, there exists a constant c_α such that for all $\varepsilon > 0$ and $m \geqslant c_\alpha \log(1/\varepsilon)$ we have*

$$\Pr_i \left(Z(W_m^{(i)}) \leqslant 2\alpha^m \right) \geqslant I(W) - \varepsilon.$$

Proof. We can rearrange the evolution Equation (7) and apply Propositions 3 and 4 for the BEC case to obtain the equation

$$Y(W_{n+1}^{(i)}) = Y(W_n^{(\lfloor i/2 \rfloor)}) \cdot \begin{cases} Z(W_n^{(\lfloor i/2 \rfloor)})(1 + Z(W_n^{(\lfloor i/2 \rfloor)})) & i \bmod 2 \equiv 1 \\ (1 - Z(W_n^{(\lfloor i/2 \rfloor)}))(2 - Z(W_n^{(\lfloor i/2 \rfloor)})) & i \bmod 2 \equiv 0 \end{cases} \tag{10}$$

Since $\sqrt{z(1+z)} + \sqrt{(1-z)(2-z)} \leqslant \sqrt{3}$ for all $z \in [0,1]$ (observed originally by [4], and $Y(W) \leqslant 1/4$, we can conclude the geometrically decaying upper bound $\mathbb{E}_i \left[\sqrt{Y(W_n^{(i)})} \right] \leqslant \frac{1}{2} \left(\frac{\sqrt{3}}{2} \right)^n$. Therefore, by Markov's inequality, we have

$$\Pr_i [Y(W_n^{(i)}) \geqslant \alpha^n] \leqslant \frac{1}{2} \left(\frac{3}{4\alpha} \right)^{n/2} . \tag{11}$$

We have $\mathbb{E}_i[Z(W_n^{(i)})] = \mathbb{E}_i[Z(W_{n-1}^{(i)})] = Z(W)$, and so

$$\Pr_i(A_\alpha^b) \min_{i \in A_\alpha^b} Z(W_n^{(i)}) \leqslant \mathop{\mathbb{E}}_i[W_n^{(i)}] = Z(W)\ .$$

Since $A_\alpha^g \subset A_\alpha$ and A_α^g is disjoint from A_α^b, we have $\Pr(A_\alpha^b) = 1 - \Pr(A_\alpha^g) - \Pr(\overline{A_\alpha})$, and we obtain

$$\Pr(A_\alpha^g) \geqslant 1 - \frac{Z(W)}{\min_{i \in A_\alpha^b}(Z(W_n^{(i)}))} - \Pr(\overline{A_\alpha}) \geqslant 1 - \frac{Z(W)}{1 - 2\alpha^n} - \frac{1}{2}\left(\frac{3}{4\alpha}\right)^{n/2} \tag{12}$$

where we have used (11) to bound the probability of $\overline{A_\alpha}$ and Fact 5 to lower bound $\min_{i \in A_\alpha^b} Z(W_n^{(i)})$.

BYy Fact 5, $Z(W_n^{(i)}) \leqslant 2\alpha^n$ for $i \in A_\alpha^g$. Together with (12) we can conclude that for all $\alpha \in (3/4, 1)$, there is some constant c_α such that for all $\varepsilon > 0$ and $m \geqslant c_\alpha \log(1/\varepsilon)$, so that

$$\Pr_i[Z(W_m^{(i)}) \leqslant 2\alpha^m] \geqslant \Pr(A_\alpha^g) \geqslant 1 - Z(W) - \varepsilon = I(W) - \varepsilon. \qquad \square$$

4.1.2 General symmetric channels

For a general symmetric channel, we can no longer rely on the explicit value of $Z((W_n^{(i)})^-)$ and must rely on the upper and lower bounds of Proposition 4. To analyze this situation further, we derive a bound on the symmetric Bhattacharyya parameter. By Propositions 3 and 4, we can write

$$\begin{aligned} Z(W_{n+1}^{(i)}) &= Z(W_n^{(\lfloor i/2 \rfloor)})^2 && \text{for } i \text{ odd} \\ Z(W_n^{(\lfloor i/2 \rfloor)})\sqrt{2 - Z(W_n^{(\lfloor i/2 \rfloor)})^2} \leqslant Z(W_{n+1}^{(i)}) &\leqslant 2Z(W_n^{(\lfloor i/2 \rfloor)}) - Z(W_n^{(\lfloor i/2 \rfloor)})^2 && \text{for } i \text{ even}\ . \end{aligned}$$

This means we can also write the corresponding expression for $Y(W_{n+1}^{(i)})$:

$$\begin{aligned} Y(W_{n+1}^{(i)}) &= Z(W_{n+1}^{(i)})(1 - Z(W_{n+1}^{(i)})) \\ &= Z(W_n^{(\lfloor i/2 \rfloor)})^2(1 - Z(W_n^{(\lfloor i/2 \rfloor)})^2) && \text{for } i \text{ odd} \\ &\leqslant \left(2Z(W_n^{(\lfloor i/2 \rfloor)}) - Z(W_n^{(\lfloor i/2 \rfloor)})^2\right)\left(1 - Z(W_n^{(\lfloor i/2 \rfloor)})\sqrt{2 - Z(W_n^{(\lfloor i/2 \rfloor)})^2}\right) && \text{for } i \text{ even} \end{aligned}$$

where we have used both sides of the bound from Proposition 4 to form the second expression.

After rearrangement of terms, the expression above becomes

$$Y(W_{n+1}^{(i)}) \leqslant Y(W_n^{(\lfloor i/2 \rfloor)}) \cdot \begin{cases} Z(W_n^{(\lfloor i/2 \rfloor)})(1 + Z(W_n^{(\lfloor i/2 \rfloor)})) & \text{for } i \text{ odd} \\ (2 - Z(W_n^{(\lfloor i/2 \rfloor)}))\frac{1 - Z(W_n^{(\lfloor i/2 \rfloor)})\sqrt{2 - Z(W_n^{(\lfloor i/2 \rfloor)})^2}}{1 - Z(W_n^{(\lfloor i/2 \rfloor)})} & \text{for } i \text{ even} \end{cases}. \tag{13}$$

We first state a bound on the evolution of $\sqrt{Y(W_{n+1}^{(i)})}$ in terms of the parameters above.

Proposition 7. *Let* $f(z) = \frac{1}{2}\left(\sqrt{z(1+z)} + \sqrt{(2-z)\frac{1 - z\sqrt{2 - z^2}}{1 - z}}\right)$ *and* $\Lambda = \max_{z \in [0,1]} f(z)$*. Then*

$$\mathop{\mathbb{E}}_{i \bmod 2} \sqrt{Y(W_{n+1}^{(i)})} \leqslant \Lambda \sqrt{Y(W_n^{(\lfloor i/2 \rfloor)})}\ . \tag{14}$$

where the meaning of the expectation is that we fix $\lfloor i/2 \rfloor$ *and allow* $i \bmod 2$ *to vary.*

Proof. Expanding the expectation expression with (13), obtain

$$\mathop{\mathbb{E}}_{i \bmod 2} \sqrt{Y(W_{n+1}^{(i)})} \leqslant f(Z(W_n^{(\lfloor i/2 \rfloor)}))\sqrt{Y(W_n^{(\lfloor i/2 \rfloor)})}.$$

Since $Z(W) \in [0,1]$ for all channels W, the bound with Λ follows. □

We now bound Λ away from 1 which implies a geometric decay of the expected value $\mathbb{E}_i[\sqrt{Y(W_n^{(i)})}]$ taken over a uniformly random i, $0 \leqslant i \leqslant 2^n - 1$.

Proposition 8. *Let Λ be defined as in Proposition 7. Then we have $\Lambda < 1$.*

We relegate the proof of Proposition 8 to the appendix, but we note that $\Lambda < 19/20$, which can be verified numerically by maximizing $f(z)$ as defined over the interval $[0,1]$. While preparing this paper, we found a more precise numerical bound in [13] that (14) holds with $\Lambda = 1.85/2$, which was obtained by using a tighter expression for $f(z)$.

Corollary 9. *Taking Λ as defined in Proposition 7, $\Pr_i[Y(W_n^{(i)})] \geqslant \alpha^n] \leqslant \frac{1}{2}\left(\frac{\Lambda^2}{\alpha}\right)^{n/2}$*

Proof. Clearly we have

$$\mathop{\mathbb{E}}_{i} \sqrt{Y(W_{n+1}^{(i)})} \leqslant \Lambda^n \sqrt{Y(W)} \leqslant \Lambda^n \cdot \frac{1}{2}$$

and we can therefore use Markov's inequality to obtain the desired consequence. □

With the corollary in hand, we are ready to state the result for general symmetric channels:

Proposition 10. *For all binary-input symmetric channels W and $\rho \in (\Lambda^2, 1)$, there exists a constant c_ρ (independent of W) such that for all $\varepsilon > 0$ and $m \geqslant b_\rho \log(1/\varepsilon)$, we have*

$$\Pr_i(Z(W_m^{(i)}) \leqslant 2\rho^m) \geqslant I(W) - \varepsilon.$$

Proof. We have

$$\Pr(\overline{A_\rho}) \max_{i \in \overline{A_\rho}}(I(W_n^{(i)})) + \Pr(A_\rho^b) \max_{i \in A_\rho^b} I(W_n^{(i)}) + \Pr(A_\rho^g) \max_{i \in A_\rho^g} I(W_n^{(i)}) \geqslant \mathop{\mathbb{E}}_i(I(W_n^{(i)})) = I(W) \quad (15)$$

where the last equality follows by the conservation of mutual information in our transformation as stated in equation (8).

From [2, Proposition 1], $I(W)^2 \leqslant 1 - Z(W)^2$ for any binary discrete memoryless channel W. As $\min_{i \in A_\rho^b} Z(W_n^{(i)}) \geqslant 1 - 2\rho^n$ by Fact 5, we have $\max_{i \in A_\rho^b} I(W_n^{(i)}) \leqslant 2\rho^{n/2}$. Using this together with equation (15), obtain

$$\Pr(\overline{A_\rho}) + \Pr(A_\rho^b) \cdot 2\rho^{n/2} + \Pr(A_\rho^g) \geqslant I(W)$$

where we used the trivial inequality (apparent from the definition of I of a binary-input channel) $Z(W_n^{(i)}) \leqslant 1$ for every i. Rearranging terms, using the bounds $\Pr(\overline{A_\rho}) \leqslant \frac{1}{2}(\Lambda^2/\rho)^{n/2}$ from Corollary 9 and $Z(W_n^{(i)}) \leqslant 2\rho^n$ for $i \in A_\rho^g$ from Fact 5, we get

$$\Pr[Z(W_m^{(i)}) \leqslant 2\rho^m] \geqslant \Pr(A_\rho^g) \geqslant I(W) - \frac{1}{2}(\Lambda^2/\rho)^{m/2} - 2\rho^{m/2}\ . \quad (16)$$

Clearly, if $\rho > \Lambda^2$, there is a constant b_ρ such that $m \geqslant b_\rho \log(1/\varepsilon)$ implies that the above lower bound is at least $I(W) - \varepsilon$. □

4.2 Fine polarization

The following lemma simplifies some of the arithmetic in the following proposition and specifies one of the constants.

Lemma 11. *For all $\gamma > 0$, $\beta \in (0, 1/2)$ and $\rho \in (0, 1)$, there exists a constant $\theta(\beta, \gamma, \rho)$ such that for all $\varepsilon \in (0, 1)$, if $m > \theta(\beta, \gamma, \rho) \cdot \log(2/\varepsilon)$, then*

$$\left(\frac{\lg(2/\rho)\gamma}{2} + 1\right) \exp\left(-\frac{(1-2\beta)^2 \lg(2/\rho) m}{2}\right) < \varepsilon/2 \ .$$

Proof. We can rewrite this expression as $c_1 \exp(-c_2 m) < \varepsilon$ for constants c_1, c_2 that are independent of ε and the result is clear. □

Proposition 12. *Given $\varepsilon \in (0, 1/2)$, a binary input memoryless channel W, a parameter $\delta \in (0, 1/2)$, there exists a constant c_δ (independent of W and ε) such that if $n_0 > c_\delta \log(1/\varepsilon)$ then*

$$\Pr_i \left[Z(W_{n_0}^{(i)}) \leqslant 2^{-2^{\delta n_0}}\right] \geqslant I(W) - \varepsilon.$$

Proof. Fix a $\beta \in (\delta, 1/2)$, and let $\gamma = \frac{\delta}{\beta - \delta}$. Let ρ be an appropriate constant for Proposition 10, and b_ρ be the associated constant. We will define

$$c_\delta = (1+\gamma) \max\{2b_\rho, \theta(\beta, \gamma, \rho), 2/\rho, c_\beta\},$$

where c_β is defined as a bound on m such that if $m \geqslant c_\beta$, then

$$\frac{1-\beta}{1 - 2^{-\frac{n}{c_\rho}\beta}} \leqslant 1;$$

$c_\beta = \frac{-\lg(\beta)}{2\lg(2/\rho)\beta}$ suffices.

Fix an $n_0 > c_\delta \log(1/\varepsilon)$, $m = \frac{1}{1+\gamma} n_0$ and $n = n_0 - m = \gamma m$. We first start with a set of roughly polarized channels; by our choice of c_δ, $m > b_\rho \log(2/\varepsilon)$ and we can apply Proposition 10 and conclude

$$\Pr_i \left[Z(W_m^{(i)}) \leqslant 2\rho^m\right] \geqslant I(W) - \varepsilon/2 \ . \tag{17}$$

Denote $\mathcal{W}_g$ to be this roughly polarized set of all $W_m^{(i)}$ such that $Z(W_m^{(i)}) \leqslant 2\rho^m$, and $R(m)$ to be the set of all associated indices i. Fix a $M \in \mathcal{W}_g$ and define a sequence $\{\tilde{Z}_n^{(i)}\}$ where

$$\tilde{Z}_{n+1}^{(i)} = \begin{cases} (\tilde{Z}_n^{(\lfloor i/2 \rfloor)})^2 & i \bmod 2 \equiv 1 \\ 2\tilde{Z}_n^{(\lfloor i/2 \rfloor)} & i \bmod 2 \equiv 0 \end{cases}, \tag{18}$$

with the base case $Z_0^{(0)} = Z(M)$. Clearly $Z(M_n^{(i)}) \leqslant \tilde{Z}_n^{(i)}$. (Recall that $X_n^{(i)}$ is the polarization process done for n steps with i determining which branch to take for arbitrary binary input channel X.)

Let $c_\rho = \lceil \frac{n}{2m \lg(2/\rho)} \rceil$. Fix a $\beta \in (0, 1/2)$. Define a collection of events $\{G_j(n) : 1 \leqslant j \leqslant c_\rho\}$:

$$G_j(n) = \left\{ i : \sum_{\substack{k \in [jn/c_\rho, \\ (j+1)n/c_\rho)}} i_k \geqslant \beta n / c_\rho \right\}; \tag{19}$$

here, i_k indicates the k'th least significant bit in the binary representation of i. Qualitatively speaking, G_j occurs when the number of 1's in the j'th block is not too small.

Since each bit of i is independently distributed, we can apply the Chernoff-Hoeffding bound [14] (with $p = 1/2$ and $\varepsilon = 1/2 - \beta$) to conclude

$$\begin{align*}\Pr_i(i \in G_j(n)) &\leqslant 1 - \exp(-2(1/2-\beta)^2 n/(c_\rho)) \\ &= 1 - \exp((1-2\beta)^2 n/(2c_\rho)) \tag{20}\end{align*}$$

for all $j \in [c_\rho]$.

Define

$$G(n) = \bigcap_j G_j(n). \tag{21}$$

Applying the union bound to $G(n)$ with (20), obtain

$$\Pr_i(i \in G(n)) \geqslant 1 - c_\rho \exp(-(1-2\beta)^2 n/(2c_\rho)). \tag{22}$$

Now we develop an upper bound on the evolution of $\tilde{Z}$ for each interval of n/c_ρ squaring/doubling operations, conditioned on i belonging to the high probability set $G(n)$.

Fix an interval $j \in \{0, 1, \ldots, c_\rho\}$. By the evolution equations (18) and the bound provided by (19), it is easy to see that the greatest possible value for $\tilde{Z}_{(j+1)n/c_\rho}$ is attained by $(1-\beta)n/c_\rho$ doublings followed by $\beta n/c_\rho$ squarings. Therefore,

$$\lg \tilde{Z}_{(j+1)n/c_\rho}^{\lfloor i/2^{jn/c_\rho} \rfloor} \leqslant 2^{\beta n/c_\rho}\left((1-\beta)n/c_\rho + \lg \tilde{Z}_{jn/c_\rho}^{\lfloor i/2^{(j-1)n/c_\rho} \rfloor}\right).$$

Cascading this argument over all intervals j, obtain

$$\begin{align*}\lg Z(M_n^{(i)}) &\leqslant \lg \tilde{Z}_n^{(i)} \\ &\leqslant 2^{n\beta} \lg Z(M) + \frac{n}{c_\rho}(1-\beta)(2^{\beta n/c_\rho} + 2^{2\beta n/c_\rho} + \cdots + 2^{n\beta}) \tag{23} \\ &\leqslant 2^{n\beta} \lg Z(M) + \frac{n}{c_\rho}(1-\beta)\frac{2^{n\beta}}{1 - 2^{-\frac{n}{c_\rho}\beta}} \\ &= 2^{n\beta}\left(\lg Z(M) + \frac{n}{c_\rho}\frac{1-\beta}{1 - 2^{-\frac{n}{c_\rho}\beta}}\right) \\ &\leqslant 2^{n\beta}(\lg Z(M) + n/c_\rho) \quad \text{as } m \geqslant c_\beta\end{align*}$$

As $M \in \mathcal{W}_g$, $Z(M) \leqslant 2\rho^m$, and $n/c_\rho \leqslant 2m\lg(2/\rho)$, we can bound above as

$$\begin{align*}&\leqslant -2^{n\beta}\lg(2/\rho)m \tag{24} \\ &\leqslant -2^{n\beta} \quad \text{as } m \geqslant 2/\rho\end{align*}$$

This shows that

$$Z(W_{n_0}^{(i)}) \leqslant 2^{-2^{\beta n}} = 2^{-2^{\delta n_0}},$$

where the equality is due to the definition of n and m, as long as the first m bits of i are in $R(m)$ and the last n bits of i are in $G(n)$. The former has probability at least $I(W) - \varepsilon/2$ by (17) and the latter has probability at least

$$1 - c_\rho \exp(-(1-2\beta)^2 n/(2c_\rho)) \geqslant 1 - \left(\frac{\lg(2/\rho)\gamma}{2} + 1\right) \exp\left(-\frac{(1-2\beta)^2 \lg(2/\rho) m}{2}\right) \geqslant 1 - \varepsilon/2$$

by our choice of c_δ and Lemma 11.

Putting the two together with the union bound, obtain

$$\Pr_i \left[Z(W_{n_0}^{(i)}) \leqslant 2^{-2^{\delta n_0}}\right] \geqslant I(W) - \varepsilon. \qquad \square$$

The following corollary will be useful in the next section, where we will deal with an approximation to the Bhattacharyya parameter.

Corollary 13. *Proposition 12 still holds with a modified set* $\widetilde{\mathcal{W}_g}$ *where* $\widetilde{\mathcal{W}_g} \supset \mathcal{W}_g$ *and* $Z\left(\widetilde{\mathcal{W}_g}\right) \leqslant \sqrt{3\rho^m}$ *(instead of* $2\rho^m$*) with a modified constant* $\widetilde{c_\delta}$.

Proof. The changes that need to be made follow from Equation (24), where $\lg Z(M)$ is used. With the extra square root, an extra factor of $1/2$ appears outside of the lg, which means c_ρ needs to be adjusted by a constant factor. In addition, $\lg(2/\rho)$ needs to be adjusted to $\lg(3/\rho)$, but this is also just a constant change. □

5 Efficient construction of polar codes

The construction of a polar code reduces to determining the frozen set of indices (the generator matrix then consists of columns of $G_n = K^{\otimes n} B_n$ indexed by the non-frozen positions). The core component of the efficient construction of a frozen set is estimating the Bhattacharyya parameters of the subchannels $W_n^{(i)}$. In the erasure case, this is simple because the evolution equation offered by Proposition 4 is exact. In the general case, the naïve calculation takes too much time: $W_n^{(i)}$ has an exponentially large output alphabet size in terms of $N = 2^n$.

Our goal, therefore, is to limit the alphabet size of $W_n^{(i)}$ while roughly maintaining the same Bhattacharyya parameter. With this sort of approach, we can select channels with relatively good Bhattacharyya parameters. The idea of approximating the channel behavior by degrading it via output symbol merging is due to [22] and variants of it were analyzed in [19]. The approach is also discussed in the survey [7, Section 3.3]. Since we can only achieve an inverse polynomial error in estimating the Bhattacharyya parameters with a polynomial alphabet, we use the estimation only up to the rough polarization step, and then use the explicit description of the subsequent good channels that is implicit in the proof of Proposition 12.

For completeness, we include the full analysis of the code construction and conclude Theorem 1 in this section. We note that revised versions of the Tal-Vardy work [22] also include a polynomial time algorithm for code construction by combining their methods with the analysis of [19]. However, as finite-length bounds on the speed of polarization were not available to them, they could not claim poly(N/ε) construction time, but only $c_\varepsilon N$ time for some unspecified c_ε.

For our binning, we deal with the marginal distributions of the input bit given an output symbol. A BIS channel W defines a marginal probability distribution $W(y|x)$. We invert this conditioning to form the expression

$$p(0|y) = \Pr_x(x = 0|W(x) = y) = \frac{1}{2}\frac{W(y|0)}{\Pr_x(W(x) = y)}$$

for a uniformly distributed input bit x. In addition, we introduce the one-argument form

$$p(y) = \Pr_x(W(x) = y)$$

for the simple probability that the output is y given an uniformly distributed input bit x.

Proposition 14. *For a binary-input symmetric channel $W : \mathcal{B} \to \mathcal{Y}$ and all $k > 0$, there exists a channel $\widetilde{W} : \mathcal{B} \to \widetilde{\mathcal{Y}}$ such that $H(W) \leqslant H(\widetilde{W}) \leqslant H(W) + 2\lg(k)/k$, $|\widetilde{\mathcal{Y}}| \leqslant k + 1$, and the marginal probability distribution $\widetilde{W}(y|x)$ is computable, by Algorithm 2, in time polynomial in $|\mathcal{Y}|$ and k.*

Algorithm 2: Binning algorithm

```
input : $W : \mathcal{B} \to \mathcal{Y}$, $k > 0$
output: $\widetilde{W} : \mathcal{B} \to \widetilde{\mathcal{Y}}$
Initialize new channel $\widetilde{W}$ with symbols $\tilde{y}_0, \tilde{y}_1 \ldots \tilde{y}_k$ with $\widetilde{W}(\tilde{y}|x) = 0$ for all $\tilde{y}$ and $x \in \mathcal{B}$
for $y \in \mathcal{Y}$ do
    $p(0|y) \leftarrow \frac{1}{2}\frac{W(y|0)}{\Pr_x(W(x)=y)}$
    $\widetilde{W}(\tilde{y}_{\lfloor kp(0|y) \rfloor}|0) \leftarrow \widetilde{W}(\tilde{y}_{\lfloor kp(0|y) \rfloor}|0) + W(y|0)$
    $\widetilde{W}(\tilde{y}_{\lfloor kp(0|y) \rfloor}|1) \leftarrow \widetilde{W}(\tilde{y}_{\lfloor kp(0|y) \rfloor}|1) + W(y|1)$
return $\widetilde{W}$
```

Proof. First, it is clear that the algorithm runs in time polynomial in $|\mathcal{Y}|$ and k; k bits of precision is more than sufficient for all of the arithmetic operations, and the operations are done for each symbol in $\mathcal{Y}$.

For $\tilde{y} \in \widetilde{\mathcal{Y}}$, let $I_{\tilde{y}}$ be the set of y associated with the symbol $\tilde{y}$; that is, all y such that $p(0|y)$ falls in the interval of $[0, 1]$ associated with $\tilde{y}$ (which is $[j/k, (j + 1)/k)$ for $\tilde{y} = \tilde{y}_j$).

For the lower bound, it is clear that $H(W) \leqslant H(\widetilde{W})$. Juxtaposing the definitions of $H(W)$ and $H(\widetilde{W})$ together, obtain (defining the binary entropy function $h(x) = -x \lg x - (1 - x)\lg(1 - x)$):

$$H(W) = \sum_{y \in Y} p(y)h(p(0|y)) \leqslant \sum_{\tilde{y} \in \widetilde{\mathcal{Y}}} \left(\sum_{y \in I_{\tilde{y}}} p(y) \right) (h(p(0|\tilde{y})))) = H(\widetilde{W})$$

where the inequality is due to the concavity of $h(x)$.

Using the fact $\min_i a_i/b_i \leqslant \sum_i a_i / \sum_i b_i \leqslant \max_i a_i/b_i$, we can bound

$$p(0|\tilde{y}) = \frac{p(\tilde{y}|0)p(0)}{p(\tilde{y})} = \frac{1}{2}\frac{\sum_{y \in I_{\tilde{y}}} p(y|0)}{\sum_{y \in I_{\tilde{y}}} p(y)}$$

with the expressions

$$\min_{y \in I_{\tilde{y}}} p(0|y) \leqslant p(0|\tilde{y}) \leqslant \max_{y \in I_{\tilde{y}}} p(0|y)$$

which implies, for all $y \in I_{\tilde{y}}$,

$$p(0|\tilde{y}) - \frac{1}{k} \leqslant p(0|y) \leqslant p(0|\tilde{y}) + \frac{1}{k}.$$

We will need to offer a bound on $h(p(0|\tilde{y}))$ as a function of $h(p(0|y))$. $h(x)$ is concave and obeys $|h'(x)| \leqslant \lg k$ if $1/k < x < 1-1/k$. Define the "middle set" $\tilde{y}_m = \{\tilde{y}_i : 0 < i < k-1\}$, corresponding with intervals where $p(0|\tilde{y}_m)$ is in the range $1/k < x < 1-1/k$. Then, by the concavity of $h(x)$, for all $\tilde{y} \in \tilde{y}_m$ and $y \in I_{\tilde{y}}$, we have $h(p(0|\tilde{y})) \leqslant h(p(0|y)) + 2\lg(k)/k$.

We now provide a bound for the remaining symbols $\tilde{y}_0$, $\tilde{y}_{k-1}$ and $\tilde{y}_k$. $\tilde{y}_k$ is trivial because it represents all symbols where $p(0|y) = 1$, and merging those symbols together still results in $p(0|\tilde{y}) = 1$. For $\tilde{y}_0$, we have

$$h(p(0|\tilde{y})) \leqslant h(1/k) \leqslant 2\lg(k)/k \leqslant h(p(0|y)) + 2\lg(k)/k$$

and similarly for $\tilde{y}_{k-1}$.

With these expressions in hand, we can now write

$$\begin{aligned} H(\widetilde{W}) &= \sum_{\tilde{y} \in \mathcal{Y}} \sum_{y \in I_{\tilde{y}}} p(y) h(p(0|\tilde{y}))) \\ &\leqslant \sum_{\tilde{y} \in \mathcal{Y}} \sum_{y \in I_{\tilde{y}}} p(y)(h(p(0|y)) + 2\lg(k)/k) \\ &\leqslant H(W) + 2\lg(k)/k \end{aligned}$$ □

We note that a slightly different binning strategy [22] can achieve an approximation error of $O(1/k)$. We chose to employ a simple variant that still works for our purposes. We will iteratively use the binning algorithm underlying Proposition 14 to select the best channels. The following corollary formalizes this.

Corollary 15. *Let $\widehat{W_n^{(i)}}$ indicate the result of using Algorithm 2 after every application of the evolution Equations* (7)*; that is,*

$$\widehat{W_n^{(i)}} = \widetilde{\widetilde{\widetilde{W^+}^{-}}^{\cdot^{\cdot^{\cdot}}}}$$

where the + or − is chosen depending on the corresponding bit, starting from the least significant one, of the binary representation of $i \in \{0, 1, \ldots, 2^n - 1\}$. Then

$$H(W_n^{(i)}) \leqslant H\left(\widehat{W_n^{(i)}}\right) \leqslant H(W_n^{(i)}) + \frac{2^{n+2}\lg(k)}{k}\ .$$

Proof. The lower bound is obvious as the operation $\widetilde{\cdot}$ never decreases the entropy of the channel, as mentioned in the proof of Proposition 14.

For the upper bound, we'd like to consider the error expression summed over all $W_n^{(i)}$:

$$\sum_{i=0}^{2^n-1} H\left(\widehat{W_n^{(i)}}\right) - \sum_{i=0}^{2^n-1} H(W_n^{(i)}) = \sum_{i=0}^{2^n-1} H\left(\widehat{W_n^{(i)}}\right) - 2^n H(W) \tag{25}$$

as $\mathbb{E}_{b\in\{+,-\}} H(W^b) = H(W)$ by (8). At every approximation stage, we have, from Proposition 14,

$$H\left(\widetilde{\widehat{W_m^{(\lfloor i/2\rfloor)}}^{+}}\right) + H\left(\widetilde{\widehat{W_m^{(\lfloor i/2\rfloor)}}^{-}}\right) \leqslant 2\left(H\left(\widehat{W_m^{(\lfloor i/2\rfloor)}}\right) + \frac{2\lg k}{k}\ .\right)$$

Applying this to every level of the expression (25) (colloquially speaking, we strip off the $\widetilde{\ }$s n times), obtain

$$\sum_{i=0}^{2^n-1} H\left(\widehat{W_n^{(i)}}\right) - 2^n H(W) \leqslant \frac{2\lg k}{k}(2 + 2^2 + \cdots + 2^n) \leqslant \frac{2^{n+2}\lg k}{k}\ .$$

Since the sum of all of the errors $H\left(\widehat{W_n^{(i)}}\right) - H(W_n^{(i)})$ is upper bounded by $\frac{2^{n+2}\lg k}{k}$, each error is also upper bounded by $\frac{2^{n+2}\lg k}{k}$ (since no error is negative due to the lower bound). □

We are now in a position to restate and prove our main theorem (Theorem 1).

Theorem. *There is an absolute constant $\mu < \infty$ such that the following holds. Let W be a binary-input output-symmetric memoryless channel with capacity $I(W)$. Then there exists $a_W < \infty$ such that for all $\varepsilon > 0$ and all powers of two $N \geqslant a_W(1/\varepsilon)^\mu$, there is a deterministic* poly(N) *time construction of a binary linear code of block length N and rate at least $I(W) - \varepsilon$ and a deterministic $\mathcal{O}(N\log N)$ time decoding algorithm with block error probability at most $2^{-N^{0.49}}$.*

Proof. Fix an N that is a power of 2, and let $n_0 = \lg(N)$. Define m, n, ρ as they are in Proposition 12. Utilizing the definition of $\widehat{\cdot}$ from Corollary 15 with $k = \left(\frac{2}{\rho}\right)^{2m}$, let $\widehat{\mathcal{W}_g}$ be the set of all channels $W_m^{(i)}$ such that $H\left(\widehat{W_m^{(i)}}\right) \leqslant 3\rho^m$, and let $\widehat{R}(m)$ be the set of corresponding indices i. Define the complement of the frozen set

$$\overline{\hat{F}_{n_0}} = \{i \ \mid \ 0 \leqslant i \leqslant 2^{n_0} - 1, i_0^{m-1} \in \hat{R}(m), i_m^{n_0-1} \in G(n_0 - m)\}$$

where $G(n)$ is defined in Equation 21 and the notation $i_j^k = i/2^j \bmod 2^{k-j+1}$ means the integer with the binary representation of the jth through kth bits of i, inclusive. We note that this set $\overline{\hat{F}_{n_0}}$ is computable in poly$(1/\varepsilon, N)$ time: $\widehat{R}(m)$ is computable in poly$(1/\varepsilon)$ time because $k \leqslant$ poly$(1/\varepsilon)$ and $G(n_0 - m)$ is computable in $\mathcal{O}(N)$ time as it is just counting the number of 1 bits in various intervals.

By Corollary 15 we can conclude that $i \in R(m)$ implies $i \in \hat{R}(m)$ because $Z(W_m^{(i)}) \leqslant 2\rho^m$ implies $H(W_m^{(i)}) \leqslant Z(W_n^{(i)}) \leqslant 2\rho^m$. This in turn implies $H(\widehat{W_m^{(i)}}) \leqslant 3\rho^m$ by our choice of k and the approximation error guaranteed by Corollary 15. Therefore, we have

$$\Pr_{i<2^m}(i \in \hat{R}(m)) \geqslant \Pr_{i<2^m}(i \in R(m))$$

and also that all $M \in \widehat{\mathcal{W}_g}$ satisfy $Z(M) \leqslant \sqrt{H(M)} \leqslant \sqrt{3\rho^m}$, where the former inequality is from (1).

Applying Corollary 13 with our modified set $\widehat{\mathcal{W}_g}$, we can now conclude $\Pr(i \in \overline{\hat{F}_{n_0}}) \geqslant I(W) - \varepsilon$ and $Z(W_{n_0}^{(i)}) \leqslant 2^{-2^{\delta n_0}}$ for all i in $\overline{\hat{F}_{n_0}}$. This implies that

$$\sum_{i \in \overline{\hat{F}_{n_0}}} Z(W_n^{(i)}) \leqslant N 2^{-N^{\delta}} .$$

Taking $\delta = .499$ and $\mu = \widetilde{c_\delta}$, we can conclude the existence of an a_W such that for $N \geqslant a_W (1/\varepsilon)^{\mu}$,

$$\sum_{i \in \overline{\hat{F}_{n_0}}} Z(W_n^{(i)}) \leqslant 2^{-N^{.49}},$$

as such μ satisfies the conditions of Corollary 13. The proof is now complete since by Lemma 2, the block error probability of polar codes with a frozen set F under successive cancellation decoding is bounded by the sum of the Bhattacharyya parameters of the channels not in F. □

6 Future work

The explicit value of μ found in Theorem 1 is a large constant and far from the empirically suggested bound of approximately 4. Tighter versions of this analysis should be able to minimize the difference between the upper bound suggested by Theorem 1 and the available lower bounds.

We hope to extend these results shortly to channels with non-binary input alphabets, utilizing a decomposition of channels to prime input alphabet sizes [8]. Another direction is to study the effect of recursively using larger $\ell \times \ell$ kernels instead of the 2×2 matrix $K = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Of course in the limit of $\ell \to \infty$, by appealing to the behavior of random linear codes we will achieve $\mu \approx 2$, but the decoding complexity will grow as 2^{ℓ}. The trade-off between μ and ℓ for fixed $\ell > 2$ might be interesting to study.

Acknowledgments

We thank Seyed Hamed Hassani, Eren Şaşoğlu, Ido Tal, Rüdiger Urbanke, and Alexander Vardy for useful discussions and comments about the write-up.

References

[1] Abdelaziz Amraoui, Andrea Montanari, Thomas J. Richardson, and Rüdiger L. Urbanke. Finite-length scaling for iteratively decoded LDPC ensembles. *IEEE Transactions on Information Theory*, 55(2):473–498, 2009. 6

[2] Erdal Arıkan. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, pages 3051–3073, July 2009. 1, 3, 6, 8, 9, 10, 13

[3] Erdal Arıkan. Source polarization. In *Proceedings of 2010 IEEE International Symposium on Information Theory*, pages 899–903, 2010. 7

[4] Erdal Arikan and Emre Telatar. On the rate of channel polarization. *CoRR*, abs/0807.3806, 2008. 11

[5] Erdal Arıkan and Emre Telatar. On the rate of channel polarization. In *Proceedings of 2009 IEEE International Symposium on Information Theory*, pages 1493–1495, 2009. 3, 5, 6

[6] Mayank Bakshi, Sidharth Jaggi, and Michelle Effros. Concatenated polar codes. In *ISIT*, pages 918–922. IEEE, 2010. 3

[7] Eren Şaşoğlu. Polarization and polar codes. *Foundations and Trends in Communications and Information Theory*, 8(4):259–381, 2012. 4, 8, 16

[8] Eren Şaşoğlu, Emre Telatar, and Erdal Arikan. Polarization for arbitrary discrete memoryless channels. *CoRR*, abs/0908.0302, 2009. 20

[9] G. David Forney. *Concatenated codes.* PhD thesis, Massachusetts Institute of Technology, 1967. 2

[10] Ali Goli, Seyed Hamed Hassani, and Rüdiger Urbanke. Universal bounds on the scaling behavior of polar codes. In *Proceedings of 2012 IEEE International Symposium on Information Theory*, pages 1957–1961, 2012. 6

[11] Venkatesan Guruswami. Iterative decoding of low-density parity check codes. *Bulletin of the EATCS*, 90:53–88, 2006. 2

[12] Seyed Hamed Hassani. *Polarization and Spatial Coupling: Two Techniques to Boost Performance.* PhD thesis, École Polytechnique Fédérale De Lusanne, 2013. 4, 9

[13] Seyed Hamed Hassani and Rüdiger L. Urbanke. On the scaling of polar codes: I. the behavior of polarized channels. In *ISIT*, pages 874–878, 2010. 6, 13

[14] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):pp. 13–30, 1963. 15

[15] Jorn Justesen. A class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18(5):652–656, 1972. 2

[16] Satish Babu Korada. *Polar Codes for Channel and Source Coding.* PhD thesis, École Polytechnique Fédérale De Lausanne, 2009. 5, 7, 10, 22

[17] Satish Babu Korada, Andrea Montanari, Emre Telatar, and Rüdiger L. Urbanke. An empirical scaling law for polar codes. In *ISIT*, pages 884–888, 2010. 4, 6

[18] Shrinivas Kudekar, Tom Richardson, and Rüdiger L. Urbanke. Spatially coupled ensembles universally achieve capacity under belief propagation. In *ISIT*, pages 453–457, 2012. 3, 4, 5

[19] Ramtin Pedarsani, Seyed Hamed Hassani, Ido Tal, and Emre Telatar. On the construction of polar codes. In *ISIT*, pages 11–15, 2011. 3, 16

[20] Amir Shpilka. Capacity achieving multiwrite WOM codes. *CoRR*, abs/1209.1128, 2012. 5

[21] Volker Strassen. Asymptotische Abschatzungen in Shannon's Informationstheories. In *Trans. 3rd Prague Conf. Info. Theory*, pages 689–723, 1962. 2

[22] Ido Tal and Alexander Vardy. How to construct polar codes. *CoRR*, abs/1105.6164, 2011. 3, 16, 18, 22

[23] Ido Tal and Alexander Vardy. How to construct polar codes. *Manuscript (Personal Communication)*, 2013. Latest version of [22]. 5

[24] Jacob Wolfowitz. The coding of messages subject to chance errors. *Illinois J. Math.*, 1:591–606, 1957. 2

A Proofs of Z-parameter evolution equations

The Z-parameter evolution equations are a special case of the lemmas in [16], specifically in the appendices to Chapters 2 and 3, and the proof techniques used here are based on the proofs of those lemmas.

Proof of Proposition 3. This can be done directly by definition. Let $\mathcal{Y}$ be the output alphabet of W_n. Then

$$\begin{aligned}
Z(W_n^+) &\triangleq \sum_{y\in\mathcal{B}\times\mathcal{Y}^2} \sqrt{W_n^+(y|0)W_n^+(y|1)} \\
&= \frac{1}{2}\sum_{x\in\mathcal{B},y_1,y_2\in\mathcal{Y}} \sqrt{W_n(y_1|x\oplus 0)W_n(y_2|0)W_n(y_1|x\oplus 1)W_n(y_2|1)} \\
&= \frac{1}{2}\sum_{x\in\mathcal{B},y_1\in\mathcal{Y}} \sqrt{W_n(y_1|x)W_n(y_1|x\oplus 1)} \sum_{y_2\in\mathcal{Y}} \sqrt{W_n(y_2|0)W_n(y_2|1)} \\
&= \sum_{y_1\in\mathcal{Y}} \sqrt{W_n(y_1|0)W_n(y_1|1)} \sum_{y_2\in\mathcal{Y}} \sqrt{W_n(y_2|0)W_n(y_2|1)} \\
&\triangleq Z(W_n)^2
\end{aligned}$$

where the first step is the expansion of the definition of W_n^+ and the rest is arithmetic. □

Proof of Proposition 4. We first show $Z(W_n^-) \leqslant 2Z(W_n) - Z(W_n)^2$. Again, let $\mathcal{Y}$ be the output alphabet of W_n. Then we have

$$\begin{aligned}
Z(W_n^-) &\triangleq \sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W_n^-(y_1,y_2|0)W_n^-(y_1,y_2|1)} \qquad (26) \\
&= \frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{\sum_{x_1\in\mathcal{B}} W_n(y_1|x_1)W_n(y_2|x_1)\sum_{x_2\in\mathcal{B}} W_n(y_1|1\oplus x_2)W_n(y_2|x_2)} \\
&= \frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{(W_n(y_1|0)W_n(y_1|1))}\sqrt{(W_n(y_2|0)W_n(y_2|1))} \\
&\qquad \sqrt{\frac{W_n(y_1|0)}{W_n(y_1|1)}+\frac{W_n(y_2|0)}{W_n(y_2|1)}+\frac{W_n(y_1|1)}{W_n(y_2|0)}+\frac{W_n(y_2|1)}{W_n(y_2|0)}} \qquad (27)
\end{aligned}$$

and we note that we can define a probability mass function $p(y) = \frac{\sqrt{W_n(y|0)W_n(y|1)}}{Z(W_n)}$ over $\mathcal{Y}$, so we write

$$= \frac{Z(W_n)^2}{2} \sum_{y_1,y_2 \in \mathcal{Y}} p(y_1)p(y_2) \sqrt{\frac{W_n(y_1|0)^2 + W_n(y_1|1)^2}{W_n(y_1|0)W_n(y_1|1)} + \frac{W_n(y_2|0)^2 + W_n(y_2|1)^2}{W_n(y_2|0)W_n(y_2|1)}}$$

and introducing $f(y) = \sqrt{W_n(y|0)/W_n(y|1)} + \sqrt{W_n(y|1)/W_n(y|0)}$, we can write

$$\begin{aligned} &= \frac{Z(W_n)^2}{2} \mathop{\mathbb{E}}_{y_1,y_2 \sim p(y)} \sqrt{f(y_1)^2 + f(y_2)^2 - 4} \qquad (28) \\ &\leqslant \frac{Z(W_n)^2}{2} \left(\mathbb{E}(f(y_1)) + \mathbb{E}(f(y_2)) - 2\right) \quad \text{using } \sqrt{a+b-c} \leqslant \sqrt{a} + \sqrt{b} - \sqrt{c} \text{ when } a, b \geqslant c \end{aligned}$$

and since $\mathbb{E}_{y_1 \sim p(y)}[f(y_1)] = 2/Z(W_n)$,

$$= 2Z(W_n) - Z(W_n)^2$$

For the lower bound, we can apply Jensen's inequality twice to the function $\sqrt{x^2 + a}$ which is convex for $a \geqslant 0$, together with $f(y_i)^2 \geqslant 4$, to obtain

$$\begin{aligned} Z(W_n^-) &= \frac{Z(W_n)^2}{2} \mathop{\mathbb{E}}_{y_1,y_2 \sim p(y)} \sqrt{f(y_1)^2 + f(y_2)^2 - 4} \\ &\geqslant \frac{Z(W_n)^2}{2} \sqrt{\Big(\mathop{\mathbb{E}}_{y_1 \sim p(y)} f(y_1)\Big)^2 + \Big(\mathop{\mathbb{E}}_{y_2 \sim p(y)} f(y_2)\Big)^2 - 4} \\ &= Z(W_n)\sqrt{2 - Z(W_n)^2}. \end{aligned}$$

We note that $p(y) = 0$ for all y where either $W_n(y|0)$ or $W_n(y|1)$ is zero, so the expressions involving $f(y)$ are well-defined even if $f(y)$ is not defined for all y.

In the case that W is a binary erasure channel, the expression (28) can be simplified to obtain a tight bound. If y is an erasure symbol, then $f(y) = 2$, and otherwise, $p(y) = 0$. This means that we simply have

$$\mathop{\mathbb{E}}_{y_1,y_2 \sim p(y)} \sqrt{f(y_1)^2 + f(y_2)^2 - 4} = \mathop{\mathbb{E}}_{y \sim p(y)} f(y)$$

and the equality follows. □

B Analytic bound on geometric decay rate of $Y(W_n^{(i)})$

The bounds on f as stated in Proposition 8 can be found by numerically maximizing f in the range $[0, 1]$, but it is difficult to verify that f is indeed concave in the range $[0, 1]$ without resorting to more numerical approaches. In this section, we offer an analytic justification that f is bounded by a constant less than 1 on the interval $[0, 1]$.

First, we state the following lemma to make future analysis easier.

Lemma 16. $(2 - z)\frac{1 - z\sqrt{2 - z^2}}{1 - z} \leqslant 2.1(1 - z)$.

With this in hand, we can easily prove the proposition.

Proof of Proposition 8. Using Lemma 16, we have (where we are newly defining $g(z)$):

$$f(z) \leqslant \frac{1}{2}\left(\sqrt{z(1+z)} + \sqrt{2.1}\sqrt{1-z}\right) \triangleq g(z).$$

Since $g(z)$ is continuous over $[0,1]$ and $g(0) < 2$ and $g(1) < 2$, to prove the existence of some $\Lambda < 1$ such that $f(z) \leqslant \Lambda$ for all $z \in [0,1]$, it is sufficient to show that $g(z) \neq 2$ at any point in $[0,1]$.

Therefore, we only need to consider the roots of the equation

$$\sqrt{z(1+z)} + \sqrt{2.1}\sqrt{1-z} - 2 = 0.$$

Expanding the surds, obtain the polynomial equation (which has roots wherever $g(z)-2$ has roots)

$$h(z) \triangleq 100z^4 + 620z^3 - 259z^2 - 422z + 361 = 0$$

which has two complex roots and two real roots at -6.5 and -1. Since $h(z)$ has roots wherever $g(z) - 2$ has roots and none occur in $[0,1]$, we have proven the proposition. □

We then prove the lemma, which is an observation that the $(2-z)\frac{1-z\sqrt{2-z^2}}{1-z}$ is very "close" to the linear function $2(1-z)$, and is indeed bounded above by $2.1(1-z)$.

Proof of Lemma 16. We use the same technique that we used in the proof of Proposition 8. We define the continuous function

$$\tilde{f}(z) \triangleq (2-z)(1-z\sqrt{2-z^2}) - 2.1(1-z)^2 \ .$$

After squaring and simplifying, the equation $\tilde{f}(z) = 0$ implies

$$\tilde{g}(z) \triangleq 1 - 64z + 266z^2 - 544z^3 + 641z^4 - 400z^5 + 100z^6 = 0$$

We can pull out a factor of $(z-1)^2$ to obtain

$$1 - 62z + 141z^2 - 200z^3 + 100z^4 = 0$$

which is a polynomial that has two complex roots, one root at approximately $z_0 = 0.017$, and one root at approximately 1.269. As $\tilde{g}(z)$ has a zero whenever $\tilde{f}(z)$ does and $\tilde{f}(z)$ is continuous on $[0,1]$, it is sufficient to test $\tilde{f}(0) \geqslant 0$, $\tilde{f}(z_0) > 0$ (to conclude that z_0 is not a root of $\tilde{f}$), and $\tilde{f}(1) \geqslant 0$ to conclude the lemma. □

ECCC ISSN 1433-8092

http://eccc.hpi-web.de