Polar Codes for the Deletion Channel: Weak and Strong Polarization

Ido Tal, Henry D. Pfister, Arman Fazeli, and Alexander Vardy

***Abstract*—This paper presents the first proof of polarization for the deletion channel with a constant deletion rate and a regular hidden-Markov input distribution. A key part of this work involves representing the deletion channel using a trellis and describing the plus and minus polar-decoding operations on that trellis. In particular, the plus and minus operations can be seen as combining adjacent trellis stages to yield a new trellis with half as many stages. Using this viewpoint, we prove a weak polarization theorem for standard polar codes on the deletion channel. To achieve strong polarization, we modify this scheme by adding guard bands of repeated zeros between various parts of the codeword. This gives a scheme whose rate approaches the mutual information and whose probability of error decays exponentially in the cube-root of the block length. We conclude by showing that this scheme can achieve capacity on the deletion channel by proving that the capacity of the deletion channel can be achieved by a sequence of regular hidden-Markov input distributions.**

I. Introduction

In many communications systems, symbol-timing errors may result in insertion and deletion errors. For example, a *deletion channel* with constant deletion rate maps a length-N input string to a substring using an i.i.d. process that deletes each input symbol with probability δ. These types of channels were first studied in the 1960s [1], [2] and modern coding techniques were first applied to them in [3]. Over the past 15 years, numerical bounds on the capacity of the deletion channel have been significantly improved but a closed-form expression for the capacity remains elusive [4]–[11]. Recently, polar codes were applied to the deletion channel in a series of papers, but the question of polarization for non-vanishing deletion rates remained open [12]–[15]. In this work, we show that polar codes can be used to efficiently approach the mutual information rate between a regular (i.e., finite-state, irreducible, and aperiodic) hidden-Markov input process and the output of the deletion channel with constant deletion rate.

This paper was presented in part in the at the International Symposium on Information Theory (ISIT'2019).

The work of A. Fazeli and A. Vardy was supported in part by the National Science Foundation (NSF) under Grants CCF-1405119 and CCF-1719139.

The work of I. Tal and A. Vardy was supported in part by the United-States Israel Binational Science Foundation (BSF) under Grant No. 2018218.

The work of H. D. Pfister was supported in part by the National Science Foundation (NSF) under Grant No. 1718494.

I. Tal is with the Department of Electrical Engineering, Technion, Haifa 32000, Israel (email: idotal@ee.technion.ac.il).

H. Pfister is with Duke University in Durham, NC, USA (email: henry.pfister@duke.edu).

A. Fazeli is with the University of California in San Diego, CA, USA (email: afazelic@ucsd.edu).

A. Vardy is with the University of California in San Diego, CA, USA (email: vardy@ece.ucsd.edu).

In [12], a polar code is designed for the binary erasure channel (BEC) and evaluated on a BEC that also introduces a single deletion. An inner cyclic-redundancy check (CRC) code is used and decoding is performed by running the successive cancellation list (SCL) decoder [16] exhaustively over all compatible erasure locations. The results show one can recover a single deletion in this setting. Extensions to a finite number of deletions are also discussed but the decoding complexity grows faster than N^{d+1}, where N is the code length and d is the number of deletions.

In [13], a low-complexity decoder is proposed for the same setup. Its complexity, for a length-N polar code, is roughly $d^3 N \log N$ when d deletions occur[1]. The paper also presents simulation results for polar codes with lengths ranging from 256 to 2048 on two deletion channels. The first channel has a fixed deletion rate of 0.002 and the second introduces exactly 4 deletions. Based on their results, the authors of [13] conjecture that polarization occurs when $N \to \infty$ while the total number of deletions, d, is fixed.

The final papers [14], [15] in this series extend the previous results by proving that weak polarization occurs when $N \to \infty$ and $d = o(N)$. While this result is quite interesting, its proof does not extend to the case of constant deletion rate. For the case where $N \to \infty$ with d fixed, these papers also show strong polarization for the deletion channel and weak polarization for the cascade of the deletion channel and a discrete memoryless channel (DMC).

In this paper, we combine the well-known trellis representation for channels with synchronization errors [3] with low-complexity successive-cancellation (SC) trellis decoding for channels with memory [17], [18]. In particular, [3] describes how the joint input-output probability of the deletion channel (and other synchronization-error channels) can be represented using a trellis. This is closely related to fast algorithms for the edit distance between strings based on dynamic programming [19]. The main advantage of the trellis perspective is that it naturally generalizes to other channels with synchronization errors (e.g., with insertions, deletions, and errors). The papers [17], [18] describe how the plus and minus polar-decoding operations can be efficiently applied to a channel whose input-output mapping is represented by a trellis. Putting these ideas together defines a low-complexity SC decoder for polar codes on the deletion channel that is essentially equivalent to the decoder defined in [13].

Building on previous proofs of polarization for channels with memory [20], [21], this paper proves weak and strong

[1] In [13], this complexity is misstated as $O(d^2 N \log N)$.

polarization for the deletion channel. In order to prove strong polarization, guard bands of '0' symbols are embedded in the codewords of Arıkan's standard polar codes. Effectively, these guard bands allow the decoder to work on independent blocks and enable our proof of strong polarization.

The primary results of this research are summarized in Theorem 1. Conceptually, it provides a polynomial-time method to achieve the mutual information rate between a fixed regular hidden-Markov input process and the binary deletion channel.

Theorem 1. *Fix a regular hidden-Markov input process and a parameter $\nu \in (0, 1/3]$. The rate of our coding scheme approaches the mutual information rate between the input process and the binary deletion channel output. The encoding and decoding complexities of our scheme are $O(\Lambda \log \Lambda)$ and $O(\Lambda^{1+3\nu})$, respectively, where Λ is the blocklength. For any $0 < \nu' < \nu$ and sufficiently large blocklength Λ, the probability of decoding error is at most $2^{-\Lambda^{\nu'}}$.*

The family of allowed input distributions is defined in Subsection II-D and the structure of the codeword is defined in Section VII-A. Its proof can be found in Section VII. While the theorem is stated for a fixed input process, we note that the encoding and decoding complexities scale cubically with the number of states in the input process.

Theorem 2 establishes a sequence of regular hidden-Markov input processes whose mutual information rates approach the deletion channel capacity.

Theorem 2. *Let C be the capacity of the binary deletion channel with deletion probability δ. For any $\epsilon > 0$, there is a regular hidden-Markov input process whose mutual information rate on the binary deletion channel output is at least $C - \epsilon$.*

Together, the two theorems imply that the first scheme can be used to achieve capacity on the binary deletion channel. We should note, however, that we do not provide an efficient method to optimize the input distribution or to bound its complexity in terms of the gap to capacity. Also, Theorem 2 is weaker than a recent result by Li and Tan which proves the capacity can be approached by a sequence of finite-order Markov input distributions that are both irreducible and aperiodic [22]. Both results are both predated by an earlier proof of Dobrushin that shows a sequence of periodic finite-state Markov input distributions can approach capacity on the deletion channel [2].

Here is an outline of the structure of this paper. Section II sets up the basic notation and definitions used in this paper. Section III defines the concept of a trellis and shows how it can be used to compactly represent various deletion patterns and their corresponding probabilities. In Section IV, we describe how plus and minus polarization operations are applied to trellises to yield new trellises. This provides a more detailed description of the SC trellis decoding method introduced in [17]. It is our hope that all sections up to and including Section IV will be accessible to practitioners who are primarily interested in the implementation details. Section V discusses information rates and Section VI proves that, in our setting, weak polarization occurs. Section VII focuses on strong polarization. The practitioner is advised to read Section VII-A which defines the structure and operation of an encoder with guard bands. The proof of the main theorem is presented in Section VII.

II. Background

A. Notation

The natural numbers are denoted by $\mathbb{N} \triangleq \{1, 2, \ldots\}$. We also define $[m] \triangleq \{1, 2, \ldots, m\}$ for $m \in \mathbb{N}$. Let $\mathcal{X}$ denote a finite set (e.g., the input alphabet of a channel). In this paper, we fix $\mathcal{X} = \{0, 1\}$ as the binary alphabet. Extensions to non-binary alphabets are straightforward, see for example [23, Chapter 3] and [21, Appendix A]. Let $\mathbf{x} = (x_1, \ldots, x_N) \in \mathcal{X}^N$ be a vector of length $N = 2^n$. We use $[\mathit{statement}]$ to denote the Iverson bracket which evaluates to 1 if $\mathit{statement}$ is true and 0 otherwise. The concatenation of vectors $\mathbf{y} \in \mathcal{X}^{N_1}$ and $\mathbf{y}' \in \mathcal{X}^{N_2}$ lives in $\mathcal{X}^{N_1+N_2}$ and is denoted by $\mathbf{y} \odot \mathbf{y}'$. The length of a vector $\mathbf{y}$ is denoted by $|\mathbf{y}|$. Random variables will typically be denoted by uppercase letters.

In this paper, we use the standard Arıkan transform presented in the seminal paper [24]. The Arıkan transform of $\mathbf{x} \in \mathcal{X}^N$, $N = 2^n$, is defined recursively using length-$N/2$ binary vectors, $\mathbf{x}^{[0]}$ and $\mathbf{x}^{[1]}$:

$$\mathbf{x}^{[0]} \triangleq (x_1 \oplus x_2, x_3 \oplus x_4, \ldots, x_{N-1} \oplus x_N) \,, \tag{1}$$

$$\mathbf{x}^{[1]} \triangleq (\quad x_2, \quad x_4, \ldots, \quad x_N) \,, \tag{2}$$

where $\oplus$ denotes modulo-2 addition. Then, for any sequence $b_1, b_2, \ldots, b_\lambda \in \{0, 1\}$ with $\lambda \leq n$, we extend this notation to define the vector $\mathbf{x}^{[b_1, b_2, \ldots, b_\lambda]} \in \mathcal{X}^{2^{n-\lambda}}$ recursively via

$$\mathbf{x}^{[b_1, b_2, \ldots, b_\lambda]} = \left(\mathbf{x}^{[b_1, b_2, \ldots, b_{\lambda-1}]}\right)^{[b_\lambda]} . \tag{3}$$

Specifically, if $\lambda = n$, then the vector $\mathbf{x}^{[b_1, b_2, \ldots, b_\lambda]}$ is a scalar. This scalar is denoted by $u_{i(\mathbf{b})}$, where $\mathbf{b}$ defines the index

$$i(\mathbf{b}) \triangleq 1 + \sum_{j=1}^{n} b_j 2^{n-j} \,. \tag{4}$$

The transformed length-N vector is given by

$$\mathbf{u} = (u_1, \ldots, u_N) = \mathcal{A}_n(\mathbf{x}) \,, \tag{5}$$

where $\mathcal{A}_n \colon \mathcal{X}^{2^n} \to \mathcal{X}^{2^n}$ is called the Arıkan transform of order n. Its inverse is denoted $\mathcal{A}_n^{-1}$ and satisfies $\mathcal{A}_n^{-1} = \mathcal{A}_n$.

Let $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ and $\mathbf{x} \in \mathcal{X}^N$ be given, where $N = 2^n$ and $i = i(\mathbf{b})$. As before, let $\mathbf{u} = \mathcal{A}(\mathbf{x})$. Since the vector $u^{i-1} = (u_1, u_2, \ldots, u_{i-1})$ will play an important role later on, we introduce additional notation. First, note that the vectors $\mathbf{b}' \in \{0, 1\}^n$ can be totally ordered according to $i(\mathbf{b}')$ which is equivalent to standard lexicographic ordering. Recalling the notation $\mathbf{x}^{[\mathbf{b}]}$, we now define the related notation $\mathbf{x}^{(\mathbf{b})} = \mathbf{x}^{(b_1, b_2, \ldots, b_n)}$. Namely, $\mathbf{x}^{(\mathbf{b})}$ is the concatenation of $\mathbf{x}^{[\mathbf{b}']}$, over all vectors $\mathbf{b}' \in \{0, 1\}^n$ satisfying $i(\mathbf{b}') < i(\mathbf{b})$. For $i(\mathbf{b}') = i(\mathbf{b}) - 1$, this gives

$$\mathbf{x}^{(\mathbf{b})} \triangleq \mathbf{x}^{[0,0,\ldots,0]} \odot \mathbf{x}^{[0,0,\ldots,0,1]} \odot \mathbf{x}^{[0,0,\ldots,0,1,0]} \odot \cdots \odot \mathbf{x}^{[\mathbf{b}']} . \tag{6}$$

If $\mathbf{b}$ is the all-zero vector, then $\mathbf{x}^{(\mathbf{b})}$ is the null vector. From these definitions it follows that $\mathbf{x}^{(\mathbf{b})} = u^{i-1}$, where $i = i(\mathbf{b})$ and $\mathbf{u} = \mathcal{A}(\mathbf{x})$.

B. Deletion Channel

Let $W(\mathbf{y}|\mathbf{x})$ denote the transition probability of N uses of the deletion channel with constant deletion rate δ. The input is denoted by $\mathbf{x} \in \mathcal{X}^N$ and the output $\mathbf{y}$ has a random length $M = |\mathbf{y}|$ supported on $\{0, 1, \ldots, N\}$. This channel is equivalent to a BEC with erasure probability δ followed by a device that removes all erasures from the output. Thus, $W(\mathbf{y}|\mathbf{x})$ equals the probability that $N - M$ deletions have occurred, which is $(1-\delta)^M \cdot \delta^{N-M}$, multiplied by the number of distinct deletion patterns that produce $\mathbf{y}$ from $\mathbf{x}$, see [4, Section 2].

We will also consider a trimmed deletion channel whose output is given by removing all leading and trailing zeros from the output of the standard deletion channel. See Section VII for details.

C. Trellis Definition

An N-segment *trellis* $\mathcal{T}$ is a labeled weighted directed graph $(\mathcal{V}, \mathcal{E})$. We assume that $\mathcal{V}$ can be partitioned into $\mathcal{V}_0, \ldots, \mathcal{V}_N$ so that $\mathcal{V}$ is the union of $N+1$ disjoint sets:

$$\mathcal{V} = \mathcal{V}_0 \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_{N-1} \cup \mathcal{V}_N \ ,$$

where $\cup$ denotes a disjoint union. For channels with memory, $\mathcal{V}_j$ represents the set of possible channel states after j channel inputs. Similarly, the edge set $\mathcal{E}$ is arranged into a sequence of N disjoint sets:

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \cdots \cup \mathcal{E}_{N-1} \cup \mathcal{E}_N \ .$$

An edge in $\mathcal{E}_j$ connects a vertex in $\mathcal{V}_{j-1}$ to a vertex in $\mathcal{V}_j$. We define $\sigma(e)$ and $\tau(e)$ to be the starting and terminating vertices of edge e. Thus, for $e = u \to v$, we have $\sigma(e) = u$ and $\tau(e) = v$. Then,

$$e \in \mathcal{E}_j \text{ implies } \sigma(e) \in \mathcal{V}_{j-1} \text{ and } \tau(e) \in \mathcal{V}_j \ .$$

A *trellis section* comprises two adjacent sets of vertices along with the edges that connect them. That is, for $1 \le j \le N$, section j comprises vertex sets $\mathcal{V}_{j-1}$ and $\mathcal{V}_j$, as well as edge set $\mathcal{E}_j$. See Fig. 1 for an example of a trellis with 4 sections.

Each edge $e \in \mathcal{E}$ has a weight $w(e) \in [0, 1]$ and a label $\ell(e) \in \mathcal{X}$. We also assume that $\mathcal{V}_0$ and $\mathcal{V}_N$ have weight functions,

$$q : \mathcal{V}_0 \to [0, 1] \quad \text{and} \quad r : \mathcal{V}_N \to [0, 1] \ ,$$

that are associated with the initial and final states.

A path through a trellis is a sequence of N edges, $e_1, e_2, \ldots, e_N$, which starts at a vertex in $\mathcal{V}_0$ and ends at a vertex in $\mathcal{V}_N$. Namely, $\sigma(e_1) \in \mathcal{V}_0$, $\tau(e_N) \in \mathcal{V}_N$, and for each $1 \le j \le N-1$, we have $\tau(e_j) = \sigma(e_{j+1})$. The weight of a path through the trellis is defined as the product of the weights on each edge in the path times the weights of the initial and final vertices. Namely, the weight of the above path is

$$q(\sigma(e_1)) \cdot r(\tau(e_N)) \times \prod_{j=1}^{N} w(e_j) \ .$$

Thus, an N-section trellis naturally defines a *path-sum* function $T\colon \mathcal{X}^N \to \mathbb{R}$, where $T(\mathbf{x})$ equals the sum of the path weights over all paths whose length-N label sequences match $\mathbf{x}$. That is,

$$T(\mathbf{x}) \triangleq \sum_{\substack{e_1 \in \mathcal{E}_1, \\ \ell(e_1) = x_1}} \sum_{\substack{e_2 \in \mathcal{E}_2, \\ \ell(e_2) = x_2}} \cdots \sum_{\substack{e_N \in \mathcal{E}_N, \\ \ell(e_N) = x_N}} q(\sigma(e_1))\, r(\tau(e_N)) \times \prod_{j=1}^{N} w(e_j) \times \prod_{j=1}^{N-1} [\tau(e_j) = \sigma(e_{j+1})] \ . \quad (7)$$

D. FAIM processes

In latter parts of this paper, for simplicity, we will often introduce key ideas by first framing them in the context of the uniform input distribution. That is, by first considering the case in which the input distribution is i.i.d. Bernoulli $1/2$. However, the uniform input distribution, or indeed any i.i.d. input distribution, is known to generally be sub-optimal with respect to the information rate between input and output, when transmitting over a deletion channel [4], [9]–[11]. Thus, we stand to benefit by considering a larger class of input distributions.

To this end, let $\mathcal{S}$ be a given finite set. Each element of $\mathcal{S}$ is a state of an input process. In the following[2] definition, we have for all $j \in \mathbb{Z}$ that $S_j \in \mathcal{S}$ and $X_j \in \mathcal{X}$.

Definition 1 (FAIM process)**.** *A strictly stationary process (S_j, X_j), $j \in \mathbb{Z}$ is called a* finite-state, aperiodic, irreducible, Markov *(FAIM) process if, for all j,*

$$P_{S_j, X_j | S_{-\infty}^{j-1}, X_{-\infty}^{j-1}} = P_{S_j, X_j | S_{j-1}} \ , \quad (8)$$

is independent of j and the sequence $(S_j), j \in \mathbb{Z}$ is a finite-state Markov chain that is stationary, irreducible, and aperiodic.

For a FAIM process, consider the sequence X_j, for $j \in \mathbb{Z}$. In principle, the distribution of this sequence can be computed by marginalizing the states of the FAIM process (S_j, X_j). Such a sequence is typically called a *hidden-Markov process*. In this paper, we sometimes add the term *regular* to emphasize that the hidden state process is a regular Markov chain.

Let us now connect the concept of a FAIM process to that of a trellis. Let a FAIM process (X_j, S_j) be given, and fix $N \ge 1$. We now define the corresponding trellis, having N stages. The vertex set is $\mathcal{V} = \mathcal{V}_0 \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_N$, where we define

$$\mathcal{V}_j = \{s_j : s \in \mathcal{S}\}$$

for $0 \le j \le N$ so that each $\mathcal{V}_j$ contains a distinct copy of $\mathcal{S}$. For each $x \in \mathcal{X}$, $1 \le j \le N$, $\alpha_{j-1} \in \mathcal{V}_{j-1}$, and $\beta_j \in \mathcal{V}_j$, define an edge e from α_{j-1} to β_j with label $\ell(e) = x$ and weight $w(e) = P_{S_j, X_j | S_{j-1}}(\beta, x | \alpha)$. Lastly, for all $\alpha_0 \in \mathcal{V}_0$ define $q(\alpha_0) = \pi(\alpha)$, where $\pi(\alpha)$ is the stationary probability of state α in the Markov process $(S_j)_{j \in \mathbb{R}}$, and define $r(\beta_N) = 1$ for all $\beta_N \in \mathcal{V}_N$. It follows that the probability of $(X_1, X_2, \ldots, X_N) = (x_1, x_2, \ldots, x_N) = \mathbf{x}$ equals $T(\mathbf{x})$, where T was defined in (7).

[2]The definition of FAIM and FAIM-derived processes here is a specialization of the definition given in [21]. Here, we are interested in FAIM-derived (i.e., hidden-Markov) input processes. However, the input-output process of a deletion channel is neither FAIM nor FAIM-derived.

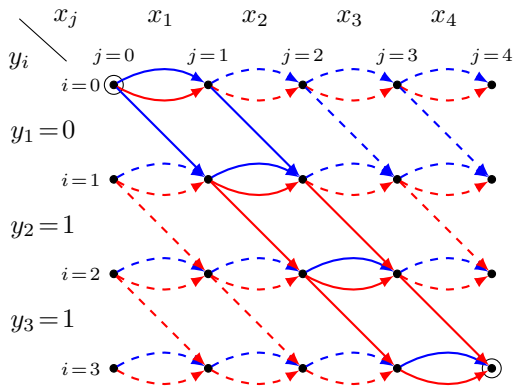

Fig. 1. A trellis for the binary deletion channel with uniform input, a codeword length of $N = 4$, and a received word $\mathbf{y} = (011)$ of length $M = 3$. Vertices are denoted $v_{i,j}$ with $0 \le i \le M$ and $0 \le j \le N$. All blue edges have label '0' while all red edges have label '1'. The horizontal edges are weighted by the probability $\delta/2$. Diagonal edges are weighted by the probability $(1-\delta)/2$. The two circled vertices have $q(v_{0,0}) = r(v_{M,N}) = 1$, while all other vertices in $\mathcal{V}_0$ and $\mathcal{V}_N$ have q and r values equal to 0, respectively. Edges that can be pruned without changing the function T in (7) are dashed.

III. Trellis Representation of Joint Probability

We have just seen that a trellis is instrumental in compactly representing a hidden-Markov input distribution. In fact, it is much more versatile than this. Namely, we will now show how a trellis can be used to represent the *joint* distribution of a hidden-Markov input process and the channel output.

A. Trellis for uniform input

This trellis representation for the deletion channel can also be found in [3].

As previously explained, it is generally beneficial to use an input distribution with memory. However, for the sake of an easy exposition, we will first consider the simplest possible input distribution, a uniform input distribution (i.e., i.i.d. and Bernoulli $1/2$).

The trellis representation will be used on the decoder side. Thus, when building the trellis, we will have already received the output vector $\mathbf{y}$. Hence, the primary role of the trellis is to evaluate the probabilities associated with possible input vectors $\mathbf{x}$, of length N. That is, the trellis will be used to calculate the joint probability of $\mathbf{x}$ and $\mathbf{y}$, denoted $P_{\mathbf{X}}(\mathbf{x}) \cdot W(\mathbf{y}|\mathbf{x})$, for $\mathbf{y}$ fixed. Recall that $W(\mathbf{y}|\mathbf{x})$ is the deletion channel law, and in this subsection $P_{\mathbf{X}}$ is the uniform input distribution.

We will shortly define the concept of a valid path in the trellis. Each valid path will correspond to a specific transmitted $\mathbf{x}$ and a specific deletion pattern that is compatible with the received $\mathbf{y}$ (see Fig. 1). We term this trellis the *base trellis*, as we will ultimately construct other trellises derived from it.

Recalling our notation, we have $\mathbf{x}$ as the unknown input vector, of known length N. The vector $\mathbf{y}$ is the known output, having known length $M = |\mathbf{y}|$. The deletion probability is δ. The base trellis is defined as follows.

Definition 2 (Base Trellis for Uniform Input)**.** *For N, δ, M, and $\mathbf{y} \in \mathcal{X}^M$:*

1) *The vertex set $\mathcal{V}$ equals the disjoint union*

$$\mathcal{V} = \mathcal{V}_0 \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_N \ ,$$

where, for $0 \le j \le N$,

$$\mathcal{V}_j = \{v_{i,j} : 0 \le i \le M\} \ . \tag{9}$$

2) *A path passing through vertex $v_{i,j}$ corresponds to the event where only i of the first j transmitted symbols were received. That is, from $x_1, x_2, \ldots, x_j$, the channel has deleted $j - i$ symbols*[3]*.*
3) *Vertices $v_{i,j}$ with $0 \le i \le M$ and $0 \le j < N$ each have up to three outgoing edges: two 'horizontal' edges, each corresponding to a deletion, and one 'diagonal' edge, corresponding to a non-deletion.*
4) *For $0 \le i \le M$ and $0 \le j < N$, there are two edges e, e' from $v_{i,j}$ to $v_{i,j+1}$. From 2) above, we deduce that these two 'horizontal' edges are associated with x_{j+1} being deleted by the channel. The first is associated with $x_{j+1} = 0$ and has $\ell(e) = 0$, while the second is associated with $x_{j+1} = 1$ and has $\ell(e') = 1$. Since the probability of deletion is δ, and in the uniform distribution $x_{j+1} = 0$ and $x_{j+1} = 1$ each occur with probability $1/2$, we set $w(e) = w(e') = \delta/2$.*
5) *For $0 \le i < M$ and $0 \le j < N$, there is a single edge e from $v_{i,j}$ to $v_{i+1,j+1}$. Recalling 2) above, we deduce that this 'diagonal' edge represents x_{j+1} not being deleted, and being observed as y_{i+1}. Thus, $\ell(e) = y_{i+1}$. Since the probability of sending x_{j+1} in the uniform case is $1/2$, regardless of its value, and the probability of a non-deletion is $1 - \delta$, we set $w(e) = (1-\delta)/2$.*
6) *We set $q(v_{0,0}) = 1$. All other vertices $v \in \mathcal{V}_0$ have $q(v) = 0$. Thus, with respect to (7), we effectively force all paths to start at $v_{0,0}$. Namely, when starting a path, no symbols have yet been transmitted, and hence no symbols have yet been received.*
7) *We set $r(v_{M,N}) = 1$. All other vertices $v \in \mathcal{V}_N$ have $r(v) = 0$. Thus, with respect to (7), we effectively force all paths to end at $v_{M,N}$. That is, at the end of a path, N symbols have been transmitted, and of these, M have been received.*

In line with the definitions above, let us call a path *valid* if it starts at $v_{0,0}$ and ends at $v_{M,N}$. For example, in Figure 1, valid paths are those that start at the circled vertex on the top left, end at the circled vertex on the bottom right, and hence contain only solid edges. Clearly, such a path is comprised of N edges, $e_1, e_2, \ldots, e_N$. Denote by $\mathbf{x} = (x_1, x_2, \ldots, x_N)$ the input vector corresponding to the above path, where $x_i = \ell(e_i)$. Each such $\mathbf{x}$ is consistent with our received $\mathbf{y}$. Indeed, tracing the path, the type of the corresponding edge (horizontal or diagonal) shows exactly which of the x_i to delete and which to keep in order to arrive at $\mathbf{y}$. Also, the probability of the input sequence $\mathbf{x}$ being transmitted and experiencing the above chain of deletion/no-deletion events is exactly equal to the product of the $w(e_i)$, times $q(v_{0,0}) \cdot r(v_{M,N}) = 1$.

From the above discussion, one has the following key lemma.

[3]Note that we could have optimized our definition of $\mathcal{V}_j$. Namely, only i in the range $\max\{0, M - N + j\} \le i \le \min\{j, M\}$ are actually consistent with the described event (i.e., only the solid edges in Figure 1). We leave such optimization to the practitioner and settle for the simpler description in (9).

Lemma 3. *Let $\mathcal{T}$ be a trellis as described in Definition 2. Then, for $\mathbf{x} \in \mathcal{X}^N$ and $T(\mathbf{x})$ as defined in (7), we have*

$$T(\mathbf{x}) = P_{\mathbf{X}}(\mathbf{x}) \cdot W(\mathbf{y}|\mathbf{x}) \ ,$$

where $P_{\mathbf{X}}$ is the uniform input distribution and W is the deletion channel law.

Proof: First, we observe that the weight of a trellis path equals the joint probability of $(\mathbf{x}, \mathbf{y})$ and the deletion pattern. Then, the claim follows from the fact that $T(\mathbf{x})$ sums the path weight over all paths through the trellis (i.e., all deletion patterns) consistent with the given $(\mathbf{x}, \mathbf{y})$ pair. ■

B. Trellises for hidden-Markov inputs

As explained earlier, a trellis is used on the decoding side, in order to capture the joint probability of $\mathbf{x}$ and $\mathbf{y}$. We now show how such a trellis is built for the more general case in which $\mathbf{x}$ is drawn from a regular hidden-Markov input process. Intuitively, this is done by simply "multiplying" the trellis corresponding to the input distribution, as described at the end of Section II, with the trellis defined for the uniform case (with the correction that the edge weights $\delta/2$ and $(1-\delta)/2$ are replaced by δ and $1-\delta$, respectively). A formal definition follows.

Definition 3 (Base Trellis for Hidden-Markov Input)**.** *For N, δ, M, $\mathcal{S}$, $P_{S_j,X_j|S_{j-1}}$, π, and $\mathbf{y} \in \mathcal{X}^M$:*

1) *The vertex set $\mathcal{V}$ equals the disjoint union*

$$\mathcal{V} = \mathcal{V}_0 \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_N \ ,$$

where, for $0 \le j \le N$,

$$\mathcal{V}_j = \{s_{i,j} : 0 \le i \le M \ , \ s \in \mathcal{S}\} \ . \tag{10}$$

Thus, $|\mathcal{V}_j| = (M+1) \cdot |\mathcal{S}|$.

2) *A path passes through vertex $s_{i,j}$ if exactly i of the first j transmitted symbols are not deleted and the state of the input process is $s \in \mathcal{S}$ after the j-th input (i.e., $S_j = s$).*
3) *Vertices $s_{i,j}$ with $0 \le i \le M$, $0 \le j < N$, and $s \in \mathcal{S}$ each have up to $3 \cdot |\mathcal{S}|$ outgoing edges.*
4) *For $0 \le i \le M$, $0 \le j < N$, and $\alpha, \beta \in \mathcal{S}$, there are two edges e, e' from $\alpha_{i,j}$ to $\beta_{i,j+1}$. From item 2, we deduce that these two 'horizontal' edges are associated with x_{j+1} being deleted by the channel. The first is associated with $x_{j+1} = 0$ and has $\ell(e) = 0$, while the second is associated with $x_{j+1} = 1$ and has $\ell(e') = 1$. Recalling that by stationarity $P_{S_{j+1},X_{j+1}|S_j} = P_{S_j,X_j|S_{j-1}}$, we set*

$$w(e) = \delta \cdot P_{S_j,X_j|S_{j-1}}(\beta, 0|\alpha) \tag{11}$$

and

$$w(e') = \delta \cdot P_{S_j,X_j|S_{j-1}}(\beta, 1|\alpha) \ . \tag{12}$$

That is, the probability of a deletion, times the probability implied by the underlying FAIM distribution.

5) *For $0 \le i < M$, $0 \le j < N$, and $\alpha, \beta \in \mathcal{S}$, there is a single edge e from $\alpha_{i,j}$ to $\alpha_{i+1,j+1}$. Recalling item 2 above, we deduce that this 'diagonal' edge represents x_{j+1} being observed (i.e., not deleted) as y_{i+1}. Thus, $\ell(e) = y_{i+1}$. We set*

$$w(e) = (1-\delta) \cdot P_{S_j,X_j|S_{j-1}}(\beta, y_{i+1}|\alpha) \ .$$

That is, the probability of a non-deletion, times the probability implied by the underlying FAIM distribution[4].

6) *For all $s_{0,0} \in \mathcal{V}_0$, where $s \in \mathcal{S}$, we set $q(s_{0,0}) = \pi(s)$. All other vertices $v \in \mathcal{V}_0$ have $q(v) = 0$. Thus, with respect to (7), we effectively force all paths to start at a vertex $s_{0,0}$, where $s \in \mathcal{S}$. Namely, when starting a path, no symbols have yet been transmitted, and hence no symbols have yet been received. Moreover, the probability of starting the path at $s_{0,0}$ is $\pi(s)$, the stationary probability of s in the FAIM input process.*
7) *For all $s_{M,N} \in \mathcal{V}_N$, we set $r(s_{M,N}) = 1$. All other vertices $v \in \mathcal{V}_N$ have $r(v) = 0$. Thus, with respect to (7), we effectively force all paths to end at a vertex $s_{M,N}$. That is, at the end of a path, N symbols have been transmitted, and of these, M have been received.*

As in the uniform case, we have the following lemma, which is easily proved.

Lemma 4. *Let $\mathcal{T}$ be a trellis as per Definition 3. Then, for $\mathbf{x} \in \mathcal{X}^N$ and $T(\mathbf{x})$ as defined in (7),*

$$T(\mathbf{x}) = P_{\mathbf{X}}(\mathbf{x}) \cdot W(\mathbf{y}|\mathbf{x}) \ ,$$

where $P_{\mathbf{X}}$ is the hidden-Markov input distribution and W is the deletion channel law.

Proof: First, we observe that the weight of a trellis path equals the joint probability of $(\mathbf{x}, \mathbf{y})$ and the deletion pattern. Then, the claim follows from the fact that $T(\mathbf{x})$ sums the path weight over all paths through the trellis (i.e., all deletion patterns) consistent with the given $(\mathbf{x}, \mathbf{y})$ pair. ■

C. Trellis for the trimmed deletion channel

For reasons that will shortly become clear, we will now consider a slight variation of the deletion channel. Namely, we now define the trimmed deletion channel (TDC). A TDC is a deletion channel that, after the deletion process, trims its output of leading and trailing '0' symbols. Thus, by definition, the output of a TDC is either an empty string, or a string that starts and ends with a '1' symbol.

We now show how to alter Definition 3 in order to account for this variation. The change turns out to be minimal.

Definition 4 (Base Trellis for Hidden-Markov Input and TDC)**.** *For N, δ, M, $\mathcal{S}$, $P_{S_j,X_j|S_{j-1}}$, π, and trimmed output $\mathbf{y}^* \in \mathcal{X}^M$, define the trellis $\mathcal{T}$ as in Definition 3, but with the following changes.*

- *The probability of an edge e from $\alpha_{0,j}$ to $\beta_{0,j+1}$ with $\ell(e) = 0$ must be changed to $w(e) = P_{S_j,X_j|S_{j-1}}(\beta, 0|\alpha)$. Namely, the δ factor in (11) is removed. In short, if the path is currently at vertex $\alpha_{0,j}$, then none of the j symbols $x_1, x_2, \ldots, x_j$ have made it to the output of the channel (they have either been deleted or trimmed). Thus, if $x_{j+1} = 0$, it will surely be either deleted, or else trimmed.*

[4] As in the uniform case, we have opted for simplicity of exposition over reduced algorithmic complexity. That is, as in the uniform case, we can take the index i in (10) to have range $\max\{0, M-N+j\} \le i \le \min\{j, M\}$. Also, edges e with probability $w(e) = 0$ can be removed from the trellis.

- *The probability of an edge e from $\alpha_{M,j}$ to $\beta_{M,j+1}$ with $\ell(e)=0$ must be changed to $w(e)=P_{S_j,X_j|S_{j-1}}(\beta,0|\alpha)$. Namely, the δ factor in (11) is removed. Note that the exact same reasoning from the previous point applies; the only difference is that now we are correcting for the trimming of the trailing '0' symbols.*

The result of the above altered trellis definition is the following lemma.

Lemma 5. *Let $\mathcal{T}$ be a trellis as described in Definition 4. Then, for $\mathbf{x}\in\mathcal{X}^N$ and $T(\mathbf{x})$ as defined in (7),*

$$T(\mathbf{x}) = P_{\mathbf{X}}(\mathbf{x})\cdot W^*(\mathbf{y}^*|\mathbf{x}) \ ,$$

where $P_{\mathbf{X}}$ is the hidden-Markov input distribution and W^* is the law of the TDC.

Proof: First, we observe that the weight of a trellis path equals the joint probability of $(\mathbf{x},\mathbf{y}^*)$ and the deletion/trimming event associated with that path. Then, the claim follows from the fact that $T(\mathbf{x})$ sums the path weight over all paths through the trellis (i.e., all deletion/trimming events) consistent with the given $(\mathbf{x},\mathbf{y}^*)$ pair. ∎

IV. Polarization operations on a trellis

Polar plus and minus transforms for channels with memory were first presented in [17], [18]. Let an input distribution on $\mathbf{x}^N$ be given, for N even. For this input distribution and a vector channel with input $\mathbf{x}\in\mathcal{X}^N$ and output $\mathbf{y}$, let $\mathcal{T}$ be a trellis with N sections whose path-sum function satisfies

$$T(\mathbf{x}) = \Pr(\mathbf{Y}=\mathbf{y},\mathbf{X}=\mathbf{x}) \ . \tag{13}$$

A. Minus transform

For a given path-sum function $T(\mathbf{x})$, where $\mathbf{x}\in\mathcal{X}^N$, the polar *minus transform* defines a new path-sum function $T^{[0]}(\mathbf{z})$, $\mathbf{z}\in\mathcal{X}^{N/2}$. Specifically, $T^{[0]}(\mathbf{z})$ is the marginalization of $T(\mathbf{x})$ over all $\mathbf{x}$ vectors satisfying

$$\mathbf{z}=\mathbf{x}^{[0]}=(x_1\oplus x_2,\ldots,x_{N-1}\oplus x_N) \ .$$

That is,

$$\begin{aligned} T^{[0]}(\mathbf{z}) &\triangleq \sum_{\mathbf{x}\in\mathcal{X}^N:\mathbf{x}^{[0]}=\mathbf{z}} T(\mathbf{x}) \\ &= \sum_{\mathbf{x}\in\mathcal{X}^N} T(\mathbf{x}) \prod_{j=1}^{N/2} [x_{2j-1}\oplus x_{2j}=z_j] \\ &= \Pr(\mathbf{Y}=\mathbf{y},\mathbf{X}^{[0]}=\mathbf{z}) \ , \end{aligned} \tag{14}$$

where the last equality follows under the assumption of (13). Due to the local nature of this reparameterization, there is a modified trellis $\mathcal{T}^{[0]}$ with $N/2$ sections that represents the new path-sum function.

Definition 5 (Minus Transform)**.** *Let $\mathcal{T}=\mathcal{T}(\mathcal{V},\mathcal{E},w,\ell,q,r)$ be a length-N trellis, where N is even. The trellis $\tilde{\mathcal{T}}=\tilde{\mathcal{T}}(\tilde{\mathcal{V}},\tilde{\mathcal{E}},\tilde{w},\tilde{\ell},\tilde{q},\tilde{r})=\mathcal{T}^{[0]}$ is defined as follows.*

- *The vertex set of $\tilde{\mathcal{T}}$ is*

$$\tilde{\mathcal{V}}=\tilde{\mathcal{V}}_0\cup\tilde{\mathcal{V}}_1\cup\cdots\cup\tilde{\mathcal{V}}_{N/2} \ ,$$

where

$$\tilde{\mathcal{V}}_j=\mathcal{V}_{2j} \ .$$

- *We next define the edge set $\tilde{\mathcal{E}}$ implicitly. Consider an edge $\tilde{e}=\alpha\to\gamma\in\tilde{\mathcal{E}}$ in section j of $\tilde{\mathcal{T}}$ with label $\tilde{\ell}(\tilde{e})=z$. Then,*

$$\alpha\in\tilde{\mathcal{V}}_{j-1}=\mathcal{V}_{2j-2} \quad \text{and} \quad \gamma\in\tilde{\mathcal{V}}_j=\mathcal{V}_{2j} \ .$$

The weight $\tilde{w}(\tilde{e})$ of this edge equals the sum of the product of the edge weights along each two-step path $\alpha\xrightarrow{e_1}\beta\xrightarrow{e_2}\gamma$ in $\mathcal{T}$ with $\ell(e_1)\oplus\ell(e_2)=z$. That is,

$$\begin{aligned}\tilde{w}(\tilde{e}) = \sum_{\substack{e_1\in\mathcal{E}_{2j-1}:\\ \sigma(e_1)=\alpha}} \sum_{\substack{e_2\in\mathcal{E}_{2j}:\\ \tau(e_2)=\gamma}} & w(e_1)\,w(e_2) \\ & \times[\tau(e_1)=\sigma(e_2)]\cdot[\ell(e_1)\oplus\ell(e_2)=z].\end{aligned}$$

Edges with weight 0 may be removed from $\tilde{\mathcal{T}}$.

- *The minus operation does not affect initial and final vertices and this implies that $\tilde{q}(s)=q(s)$ and $\tilde{r}(s)=r(s)$.*

The following lemma states that applying a minus transform to a trellis indeed results in a trellis whose corresponding path-sum function is the minus transform of the path-sum function of the initial trellis.

Lemma 6. *Let $\mathcal{T}$ be a trellis with N sections, where N is even. Denote the minus transform of $\mathcal{T}$ by $\mathcal{T}'=\mathcal{T}^{[0]}$ per Definition 5. Let T and T' be the path-sum functions corresponding to $\mathcal{T}$ and $\mathcal{T}'$, respectively, as defined in (7) . Then, T' equals $T^{[0]}$ as defined in (14).*

Proof: This follows from the fact that the minus trellis is constructed by merging adjacent trellis stages and then combining paths according to their $\mathbf{x}^{[0]}$ values. Finally, the new paths are relabeled by their $\mathbf{x}^{[0]}$ values. ∎

B. Plus transform

For a given path-sum function $T(\mathbf{x})$, where $\mathbf{x}\in\mathcal{X}^N$, the polar *plus transform* defines a new path-sum function $T^{[1]}(\mathbf{z}')$, $\mathbf{z}'\in\mathcal{X}^{N/2}$. This definition is always with respect to a vector $\mathbf{z}\in\mathcal{X}^{N/2}$, which is assumed to be fixed. Specifically, $T^{[1]}(\mathbf{z}')$ equals $T(\mathbf{x})$, where $\mathbf{x}$ is the unique vector satisfying

$$\begin{aligned}\mathbf{z}&=\mathbf{x}^{[0]}=(x_1\oplus x_2,\ldots,x_{N-1}\oplus x_N) \quad \text{and}\\ \mathbf{z}'&=\mathbf{x}^{[1]}=(x_2,x_4,\ldots,x_N) \ .\end{aligned}$$

That is,

$$\begin{aligned} T^{[1]}(\mathbf{z}') &\triangleq T(\mathbf{x})\big|_{\mathbf{x}:\mathbf{x}^{[0]}=\mathbf{z},\mathbf{x}^{[1]}=\mathbf{z}'} \\ &= \sum_{\mathbf{x}\in\mathcal{X}^N} T(\mathbf{x}) \prod_{j=1}^{N/2} [x_{2j-1}\oplus x_{2j}=z_j]\cdot[x_{2j}=z'_j] \\ &= \Pr(\mathbf{Y}=\mathbf{y},\mathbf{X}^{[0]}=\mathbf{z},\mathbf{X}^{[1]}=\mathbf{z}') \ , \end{aligned} \tag{15}$$

where the last equality follows under the assumption of (13).

As with the minus transform, there is a corresponding operation one can apply to the underlying trellis, which we now detail. Note that the plus-transform of a trellis is defined with respect to a fixed vector $\mathbf{z}$, which may not be specified explicitly when it is clear from the context.

Definition 6 (Plus Transform)**.** *Let $\mathcal{T} = \mathcal{T}(\mathcal{V}, \mathcal{E}, w, \ell, q, r)$ be a length-N trellis, where N is even and let $\mathbf{z} \in \mathcal{X}^{N/2}$ be given. The trellis $\tilde{\mathcal{T}} = \tilde{\mathcal{T}}(\tilde{\mathcal{V}}, \tilde{\mathcal{E}}, \tilde{w}, \tilde{\ell}, \tilde{q}, \tilde{r}) = \mathcal{T}^{[1]}$ is defined as follows.*

- *The vertex set of $\tilde{\mathcal{T}}$ is the same as the minus trellis $\mathcal{T}^{[0]}$. This is also the case for the functions $\tilde{q}$ and $\tilde{r}$.*
- *We next define the edge set $\tilde{\mathcal{E}}$ implicitly. Consider an edge $\tilde{e} = \alpha \to \gamma \in \tilde{\mathcal{E}}$ in section j of $\tilde{\mathcal{T}}$ with label $\tilde{\ell}(\tilde{e}) = z'$. Then,*

$$\alpha \in \tilde{\mathcal{V}}_{j-1} = \mathcal{V}_{2j-2} \quad \text{and} \quad \gamma \in \tilde{\mathcal{V}}_j = \mathcal{V}_{2j} \ .$$

The weight $\tilde{w}(\tilde{e})$ of this edge equals the sum of the product of the edge weights along each two-step path $\alpha \xrightarrow{e_1} \beta \xrightarrow{e_2} \gamma$ in $\mathcal{T}$ with $\ell(e_1) \oplus \ell(e_2) = z_j$ and $\ell(e_2) = z'$. That is,

$$\tilde{w}(\tilde{e}) = \sum_{\substack{e_1 \in \mathcal{E}_{2j-1}: \\ \sigma(e_1) = \alpha}} \sum_{\substack{e_2 \in \mathcal{E}_{2j}: \\ \tau(e_2) = \gamma}} w(e_1)\, w(e_2) \times [\tau(e_1) = \sigma(e_2)] \cdot [\ell(e_1) \oplus z' = z_j] \cdot [\ell(e_2) = z'] \ .$$

Edges with weight 0 may be removed from $\tilde{\mathcal{T}}$.

This lemma states the key property of plus transform.

Lemma 7. *Let $\mathcal{T}$ be a trellis with N sections where N is even, and let $\mathbf{z} \in \mathcal{X}^{N/2}$ be given. Denote the plus transform of $\mathcal{T}$ by $\mathcal{T}' = \mathcal{T}^{[1]}$ per Definition 6. Let T and T' be the path-sum functions corresponding to $\mathcal{T}$ and $\mathcal{T}'$, respectively, as defined in (7) . Then, T' equals $T^{[1]}$ as defined in (15).*

Proof: This follows from the fact that the plus trellis is constructed by merging adjacent trellis stages and then pruning paths that do not satisfy $\mathbf{x}^{[0]} = \mathbf{z}$. Finally, the remaining paths are relabeled with $\mathbf{x}^{[1]}$ values. ∎

C. Successive cancellation decoding

As in Arıkan's seminal paper [24], the transform defined above leads to a SC decoding algorithm. In brief, given $\mathbf{y}$ we first construct a base trellis $\mathcal{T}$. Then, there is a recursive decoder that, given $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda]}$, constructs $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda,0]}$ and calls itself with that argument. When this returns the decoded $\mathbf{x}^{[b_1,b_2,\ldots,b_\lambda,0]}$, it then builds $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda,1]}$ with respect to those hard decisions and calls itself to decode $\mathbf{x}^{[b_1,b_2,\ldots,b_\lambda,1]}$. Then, the two decoded vectors are combined to form $\mathbf{x}^{[b_1,b_2,\ldots,b_\lambda]}$ and the function returns. The following lemma makes this precise.

Lemma 8. *Let $\mathcal{T}$ be a base trellis with $N = 2^n$ sections corresponding to a received word $\mathbf{y}$ such that (13) holds for the corresponding path-sum function. For each $i \in [N]$ in order, let $\hat{u}_1^{i-1}$ be a vector of past decisions and $b_1, b_2, \ldots, b_n \in \{0,1\}$ satisfy $i(\mathbf{b}) = i$. Construct $\mathcal{T}^{[b_1,b_2,\ldots,b_n]}$ iteratively as follows. For $\lambda = 1, 2, \ldots, n$, let us define*

$$\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda]} \triangleq \begin{cases} (\mathcal{T}^{[b_1,b_2,\ldots,b_{\lambda-1}]})^{[b_\lambda]} & \text{if } \lambda \geq 2 \ , \\ \mathcal{T}^{[b_1]} & \text{if } \lambda = 1. \end{cases}$$

If $b_\lambda = 1$, then we apply the plus transform with respect to the fixed vector

$$\mathbf{z} = \mathcal{A}_{n-\lambda}^{-1}\left(\hat{u}_\tau^\theta\right) \ , \tag{16}$$

where $\hat{u}_\tau^\theta \triangleq (\hat{u}_\tau, \hat{u}_{\tau+1}, \ldots, \hat{u}_\theta)$ and

$$\theta = \sum_{j=1}^{\lambda} b_j 2^{n-j} \ , \quad \tau = \theta - 2^{n-\lambda} + 1 \ . \tag{17}$$

Then, for $\mathbf{U} = \mathcal{A}_n(\mathbf{X}) \in \mathcal{X}^N$, we have

$$T^{[b_1,b_2,\ldots,b_n]}(u) = \Pr(U_i = u, U_1^{i-1} = \hat{u}_1^{i-1}, \mathbf{Y} = \mathbf{y}) \ .$$

Proof: To facilitate a proof by induction, we actually prove a stronger claim. Namely, let $0 \leq \lambda \leq n$ be given. Define $\mathbf{b}_\lambda$ as the vector in $\{0,1\}^n$ whose first λ entries equal those of $\mathbf{b}$, while the remaining entries are all-zero. That is,

$$\mathbf{b}_\lambda = (b_1, b_2, \ldots, b_\lambda, 0, 0, \ldots, 0) \ . \tag{18}$$

Recalling the notation in (1)–(4) and (6), we will prove that for all $\boldsymbol{\mu} \in \mathcal{X}^{2^{n-\lambda}}$,

$$T^{[b_1,b_2,\ldots,b_\lambda]}(\boldsymbol{\mu}) = P(\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda]} = \boldsymbol{\mu}, \mathbf{X}^{(\mathbf{b}_\lambda)} = \hat{u}_1^{i(\mathbf{b}_\lambda)-1}, \mathbf{Y} = \mathbf{y}) \ . \tag{19}$$

Clearly, for $\lambda = n$, the reduces to the claimed lemma.

The proof of (19) proceeds by induction on λ. For the base case, take $\lambda = 0$, and note that (19) holds by assumption: the LHS is by definition $T(\boldsymbol{\mu})$ while the RHS is simply $P(\mathbf{X} = \boldsymbol{\mu}, \mathbf{Y} = \mathbf{y})$, and the two are equal by (13).

For the induction step, we assume that (19) is true for λ, and prove it to be true for $\lambda + 1$. Assume first that $b_{\lambda+1} = 0$. In this case, $\mathbf{b}_\lambda = \mathbf{b}_{\lambda+1}$. Recall that since $b_\lambda = 0$, we get the trellis $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]}$ by applying a minus transform (Definition 5) on $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda]}$. We must prove that (19) holds with $\lambda + 1$ in place of λ, and this is indeed the case by Lemma 6. Indeed, recall that by our recursive definition, $\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]} = \left(\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda]}\right)^{[0]}$, and apply Lemma 6, where in (13) and (14) we replace $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{y}$ with $\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda]}$, $(\mathbf{Y}, \mathbf{X}^{(\mathbf{b}_\lambda)})$, and $(y, \hat{u}_1^{i(\mathbf{b}_\lambda)-1})$, respectively.

Now, let us assume that $b_{\lambda+1} = 1$. Because of this, note that $\mathbf{b}_\lambda \neq \mathbf{b}_{\lambda+1}$. As before, we assume that (19) is true for λ, and prove it to be true for $\lambda + 1$. By definition, we get the trellis $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]}$ by applying a plus transform (Definition 6) on $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda]}$, with respect to the vector $\mathbf{z}$ defined in (16) and (17), with λ replaced by $\lambda + 1$. Thus, if we denote by T the probability function associated with $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda]}$, we get by Lemma 7 that the probability function associated with $\mathcal{T}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]}$, which we denote by T', satisfies

$$\begin{aligned} T'(\mathbf{z}') &= T(\boldsymbol{\mu}) \\ &= P(\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda]} = \boldsymbol{\mu}, \mathbf{X}^{(\mathbf{b}_\lambda)} = \hat{u}_1^{i(\mathbf{b}_\lambda)-1}, \mathbf{Y} = \mathbf{y}) \ , \end{aligned}$$

where $\boldsymbol{\mu}$ is the unique vector for which $\boldsymbol{\mu}^{[0]} = \mathbf{z}$ and $\boldsymbol{\mu}^{[1]} = \mathbf{z}'$. The condition $\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda]} = \boldsymbol{\mu}$ is equivalent to the pair of conditions

$$\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,0]} = \boldsymbol{\mu}^{[0]} \quad \text{and} \quad \mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,1]} = \boldsymbol{\mu}^{[1]} \ .$$

That is, to the pair of conditions

$$\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,0]} = \mathbf{z} \quad \text{and} \quad \mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]} = \mathbf{z}' \ .$$

We will shortly prove that the pair of conditions

$$\mathbf{X}^{(\mathbf{b}_\lambda)} = \hat{u}_1^{i(\mathbf{b}_\lambda)-1} \quad \text{and} \quad \mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,0]} = \mathbf{z} \tag{20}$$

can be simplified to

$$\mathbf{X}^{(\mathbf{b}_{\lambda+1})} = \hat{u}_1^{i(\mathbf{b}_{\lambda+1})-1}. \tag{21}$$

Once this is proved, the lemma follows, since the above implies that

$$T'(\mathbf{z}') = P(\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,b_{\lambda+1}]} = \mathbf{z}', \mathbf{X}^{(\mathbf{b}_{\lambda+1})} = \hat{u}_1^{i(\mathbf{b}_{\lambda+1})-1}, \mathbf{Y} = \mathbf{y}).$$

Let us now show that (20) is equivalent to (21). Since $b_{\lambda+1} = 1$, the set of transforms we need to add to $\mathbf{X}^{(\mathbf{b}_\lambda)}$ in order to get $\mathbf{X}^{(\mathbf{b}_{\lambda+1})}$ are those with prefix $(b_1, b_2, \ldots, b_\lambda, 0)$. That is, we are missing the $\mathcal{A}_{n-(\lambda+1)}$ transform of $\mathbf{X}^{[b_1,b_2,\ldots,b_\lambda,0]}$, and this transform must equal $\hat{u}_{i(\mathbf{b}_\lambda)}^{i(\mathbf{b}_{\lambda+1})-1}$. To see that this indeed is the case, we observe that $\mathbf{z}$ is defined by (16) and (17) with $\lambda+1$ in place of λ. Recalling (4) and (18), and keeping in mind that in (17) we replace λ by $\lambda+1$, we see that $\theta = i(\mathbf{b}_{\lambda+1}) - 1$ while $\tau = i(\mathbf{b}_\lambda)$. ∎

Actually, the above lemma is not unique to the deletion channel and it applies to any base trellis for which (13) holds. The above lemma also gives an efficient method for deciding the value of $\hat{u}_i$ at stage i, since

$$\Pr(U_i = u | U_1^{i-1} = \hat{u}_1^{i-1}, \mathbf{Y} = \mathbf{y}) = \frac{T^{[b_1,b_2,\ldots,b_n]}(u)}{\sum_{u' \in \mathcal{X}} T^{[b_1,b_2,\ldots,b_n]}(u')} \tag{22}$$

when $\Pr(U_1^{i-1} = \hat{u}_1^{i-1}, \mathbf{Y} = \mathbf{y}) > 0$.

D. Complexity

In [17], SC trellis decoding is generalized to finite-state channels with memory. For a finite-state channel with A states, the decoding complexity of a length-N code is shown to be $O(A^3 N \log N)$. While there are some connections between finite-state channels and deletion channels [10], it is not clear if this complexity result can be applied directly to the deletion channel. Using a different formulation, a SC decoder for polar codes on the deletion channel is defined in [13]. Its complexity is $O(N^4 \log N)$ for a constant deletion rate and a uniform input distribution[5].

In this section, we bound the complexity of computing the plus and minus transformations of a trellis. For a trellis $\mathcal{T}$ with N sections, let $P_2(j)$ be the number of distinct 2-step paths from states in $\mathcal{V}_{2j}$ to states in $\mathcal{V}_{2j+2}$ and define

$$C(\mathcal{T}) \triangleq \sum_{j=0}^{N/2-1} P_2(j).$$

From Definition 5, one can verify that the minus transform requires $C(\mathcal{T})$ multiplies and adds to compute $\mathcal{T}^{[0]}$. Similarly, from Definition 6, it follows that the plus transform requires at most $C(\mathcal{T})$ multiplies and adds to compute $\mathcal{T}^{[1]}$.

Consider a trellis $\mathcal{T}_\lambda$ at depth-λ in the decoding process. Such a trellis will have $2^{n-\lambda}$ sections each corresponding to 2^λ channel uses. For the deletion channel, we observe that each state in $\mathcal{V}_{2j}$ has at most $2(2^\lambda+1)|\mathcal{S}|$ outgoing edges. This is because each edge can be labeled by 0 or 1, the number of deletions (between 0 and 2^λ) determines the change in the channel state, and the input state can change to any of $|\mathcal{S}|$ possibilities. Combining these observations, and noting that the number of vertices in each segment is at most $2^n|\mathcal{S}|$, we see that

$$C(\mathcal{T}_\lambda) \le 2^n|\mathcal{S}| \cdot \left(2(2^\lambda+1)|\mathcal{S}|\right)^2 2^{n-\lambda} \le 2^{2n+2}(2^\lambda+3)|\mathcal{S}|^3.$$

Since the full decoder uses 2^λ plus and minus operations at depth λ, the overall decoding complexity is

$$\sum_{\lambda=0}^{n-1} 2^\lambda 2^{2n+2}(2^\lambda+3)|\mathcal{S}|^3 = O(|\mathcal{S}|^3 N^4),$$

which is lower than previous methods by a $\log N$ factor. This occurs because the $\lambda = n-1$ decoding step dominates the calculation and has $O(|\mathcal{S}|^3 N^4)$ complexity by itself.

The reader should happily note that the above quartic growth in N is *not* present in Theorem 1. The overall complexity of our scheme is much smaller because the guard bands allow the codeword to be separated into many smaller blocks whose trellises can be processed separately.

V. Information Rates

In this section, we will introduce and analyze various information rates related to polar codes on the deletion channel. For a given regular hidden-Markov input distribution, let $\mathbf{X}$ be an input vector of length N and let $\mathbf{Y}$ be the corresponding output vector (i.e., the observation of $\mathbf{X}$ through the deletion channel). The main goal of this paper is to show that our polar coding scheme achieves the information rate

$$\mathcal{I} = \lim_{N\to\infty} \frac{I(\mathbf{X};\mathbf{Y})}{N}, \tag{23}$$

where $\mathbf{X}$ and $\mathbf{Y}$ depend implicitly on N. This existence of this limit is well-known [2] but we revisit it here because the same argument will be used later with slight variations.

Lemma 9. *Fix a hidden-Markov input distribution. For a given N, let $\mathbf{X} = (X_1, X_2, \ldots, X_N)$ be a random vector with the above distribution. Let $\mathbf{Y}$ be the result of passing $\mathbf{X}$ through a deletion channel with deletion probability δ. Then, the following two limits exist,*

$$\lim_{N\to\infty} \frac{H(\mathbf{X})}{N} \quad \textit{and} \quad \lim_{N\to\infty} \frac{H(\mathbf{X}|\mathbf{Y})}{N}. \tag{24}$$

Proof: The proof of this lemma is detailed below for uniform inputs in Section V-A and hidden-Markov inputs in Section V-B. ∎

Once the limits in (24) are established, the limit in (23) follows because

$$\frac{I(\mathbf{X};\mathbf{Y})}{N} = \frac{H(\mathbf{X})}{N} - \frac{H(\mathbf{X}|\mathbf{Y})}{N}.$$

[5] As noted earlier, the complexity of the decoding algorithm in [13] is misstated as $O(d^2 N \log N)$ for d deletions but it is actually $O(d^3 N \log N)$.

A. Uniform input

In this subsection, we prove Lemma 9, for the restricted case in which the input distribution is i.i.d. and uniform.

Proof of Lemma 9 for Uniform Inputs: In such a setting, the first limit in (24) clearly exists and equals 1. To prove the second limit in (24), let us first define

$$\mathcal{H}_N = H(\mathbf{X}|\mathbf{Y}) \ , \quad |\mathbf{X}| = N \ . \tag{25}$$

Our plan is to show that the sequence $\mathcal{H}_N$ is superadditive, implying [25, Lemma 1.2.1, page 3] the existence of the second limit in (24). Indeed, let N_1 and N_2 be given, and let $\mathbf{X}$ and $\mathbf{X}'$ be distributed according to the input distribution, and having lengths N_1 and N_2, respectively. Denote the outputs corresponding to to $\mathbf{X}$ and $\mathbf{X}'$ by $\mathbf{Y}$ and $\mathbf{Y}'$, respectively. We have

$$\begin{aligned}
\mathcal{H}_{N_1+N_2} &= H(\mathbf{X}\odot\mathbf{X}'|\mathbf{Y}\odot\mathbf{Y}') \\
&\overset{(a)}{=} H(\mathbf{X},\mathbf{X}'|\mathbf{Y}\odot\mathbf{Y}') \\
&\geq H(\mathbf{X},\mathbf{X}'|\mathbf{Y}\odot\mathbf{Y}',\mathbf{Y},\mathbf{Y}') \\
&\overset{(b)}{=} H(\mathbf{X},\mathbf{X}'|\mathbf{Y},\mathbf{Y}') \\
&\overset{(c)}{=} H(\mathbf{X}|\mathbf{Y},\mathbf{Y}') + H(\mathbf{X}'|\mathbf{X},\mathbf{Y},\mathbf{Y}') \\
&\overset{(d)}{=} H(\mathbf{X}|\mathbf{Y}) + H(\mathbf{X}'|\mathbf{Y}') \\
&= \mathcal{H}_{N_1} + \mathcal{H}_{N_2} \ ,
\end{aligned}$$

where (a) holds because N_1 and N_2, the lengths of $\mathbf{X}$ and $\mathbf{X}'$, respectively, are constant parameters; (b) holds because $\mathbf{Y}\odot\mathbf{Y}'$ is a function of $\mathbf{Y}$ and $\mathbf{Y}'$; (c) follows by the chain rule; (d) holds because, for the i.i.d. uniform input distribution, the pair $(\mathbf{X},\mathbf{Y})$ is independent of the pair $(\mathbf{X}',\mathbf{Y}')$. Hence, the sequence $\mathcal{H}_N$ is indeed superadditive. ■

B. Hidden-Markov input

We now prove Lemma 9 for the case where the input distribution is a regular hidden-Markov process. Since now $\mathcal{H}_N$ is not generally superadditive, we will take an indirect route to prove Lemma 9. Indeed, the following lemma is proved by defining a related quantity, $\hat{\mathcal{H}}_N$, which is superadditive.

Lemma 10. *Fix a regular hidden-Markov input distribution. For a given N, let $\mathbf{X} = (X_1, X_2, \ldots, X_N)$ be a random vector with the above distribution. Let $\mathbf{Y}$ be the result of passing $\mathbf{X}$ through a deletion channel with deletion probability δ. Then, the following limit exists:*

$$\lim_{N\to\infty} \frac{H(\mathbf{X}|\mathbf{Y},S_0,S_N)}{N} \ . \tag{26}$$

Proof: Define

$$\hat{\mathcal{H}}_N = H(\mathbf{X}|\mathbf{Y},S_0,S_N) \ , \quad |\mathbf{X}| = N \ . \tag{27}$$

To borrow the terminology of [21], the above defines the *boundary-state-aware entropy*. Note that S_0 and S_N are the states just before transmission has started, and just after transmission has ended, respectively.

We now show that $\hat{\mathcal{H}}_N$ is superadditive. Indeed, let $\mathbf{X}$ and $\mathbf{X}'$ be consecutive input vectors of length N_1 and N_2, respectively. That is, $\mathbf{X}\odot\mathbf{X}'$ is a vector of length N_1+N_2 drawn from the input distribution. Denote by $\mathbf{Y}$ and $\mathbf{Y}'$ the output vectors corresponding to $\mathbf{X}$ and $\mathbf{X}'$, respectively. Then,

$$\begin{aligned}
\hat{\mathcal{H}}_{N_1+N_2} &= H(\mathbf{X}\odot\mathbf{X}'|\mathbf{Y}\odot\mathbf{Y}',S_0,S_{N_1+N_2}) \\
&\overset{(a)}{=} H(\mathbf{X},\mathbf{X}'|\mathbf{Y}\odot\mathbf{Y}',S_0,S_{N_1+N_2}) \\
&\overset{(b)}{\geq} H(\mathbf{X},\mathbf{X}'|\mathbf{Y},\mathbf{Y}',S_0,S_{N_1+N_2}) \\
&\geq H(\mathbf{X},\mathbf{X}'|\mathbf{Y},\mathbf{Y}',S_0,S_{N_1},S_{N_1+N_2}) \\
&\overset{(c)}{=} H(\mathbf{X}|\mathbf{Y},\mathbf{Y}',S_0,S_{N_1},S_{N_1+N_2}) \\
&\quad + H(\mathbf{X}'|\mathbf{X},\mathbf{Y},\mathbf{Y}',S_0,S_{N_1},S_{N_1+N_2}) \\
&\overset{(d)}{=} H(\mathbf{X}|\mathbf{Y},S_0,S_{N_1}) + H(\mathbf{X}'|\mathbf{Y}',S_{N_1},S_{N_1+N_2}) \\
&= \hat{\mathcal{H}}_{N_1} + \hat{\mathcal{H}}_{N_2} \ ,
\end{aligned}$$

where (a) holds because N_1 and N_2, the lengths of $\mathbf{X}$ and $\mathbf{X}'$, respectively, are constant parameters; (b) holds because $\mathbf{Y}\odot\mathbf{Y}'$ is a function of $\mathbf{Y}$ and $\mathbf{Y}'$; (c) follows by the chain rule; (d) holds because of conditional independence: given S_{N_1}, $(\mathbf{X},\mathbf{Y},S_0)$ is independent of $(\mathbf{X}',\mathbf{Y}',S_{N_1+N_2})$. Hence, the sequence $\hat{\mathcal{H}}_N$ is indeed superadditive, and the following limit exists by [25, Lemma 1.2.1, page 3],

$$\lim_{N\to\infty} \frac{\hat{\mathcal{H}}_N}{N} \ .$$

■

All that remains now is to account for the difference in the entropies of $\mathcal{H}_N$ and $\hat{\mathcal{H}}_N$, incurred by conditioning on S_0 and S_N. As will be made clear in the following proof, this difference can be bounded by a constant, and hence vanishes when we divide by N.

Proof of Lemma 9 for hidden-Markov inputs: We first note that the existence of the second limit in (24) implies the existence of the first limit. Indeed, taking the deletion probability δ equal to 1 makes the second limit equal the first. Hence, all that remains is to prove the existence of the second limit.

To show that the second limit in (24) exists, note that, for $|\mathbf{X}| = N$, we have on the one hand that

$$\begin{aligned}
H(\mathbf{X},S_0,S_N|\mathbf{Y}) &= H(\mathbf{X}|\mathbf{Y}) + H(S_0,S_N|\mathbf{X},\mathbf{Y}) \\
&\geq H(\mathbf{X}|\mathbf{Y}) \\
&= \mathcal{H}_N \ ,
\end{aligned}$$

and on the other hand that

$$\begin{aligned}
H(\mathbf{X},S_0,S_N|\mathbf{Y}) &= H(S_0,S_N|\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y},S_0,S_N) \\
&\leq 2\log_2|\mathcal{S}| + H(\mathbf{X}|\mathbf{Y},S_0,S_N) \\
&= 2\log_2|\mathcal{S}| + \hat{\mathcal{H}}_N \ .
\end{aligned}$$

Thus,

$$\mathcal{H}_N \leq \hat{\mathcal{H}}_N + 2\log_2|\mathcal{S}| \ .$$

Since it is easily seen that $\hat{\mathcal{H}}_N \leq \mathcal{H}_N$, we have that

$$\frac{\hat{\mathcal{H}}_N}{N} \leq \frac{\mathcal{H}_N}{N} \leq \frac{\hat{\mathcal{H}}_N}{N} + \frac{2\log_2|\mathcal{S}|}{N} \ . \tag{28}$$

We have already proved that the limit of the LHS of (28) exists, in Lemma 10. Since the limit of $(2\log_2|\mathcal{S}|)/N$ is 0, the limit of the RHS of (28) exists and equals that of the LHS. By the

sandwich property, the limit of the middle term exists as well, which is the desired result. ∎

We finish by restating the last part of the proof as a lemma.

Lemma 11. *Fix a hidden-Markov input distribution. For a given N, let $\mathbf{X} = (X_1, X_2, \ldots, X_N)$ be a random vector with the above distribution. Let $\mathbf{Y}$ be the result of passing $\mathbf{X}$ through a deletion channel with deletion probability δ. Then,*

$$\lim_{N\to\infty} \frac{H(\mathbf{X}|\mathbf{Y}, S_0, S_N)}{N} = \lim_{N\to\infty} \frac{H(\mathbf{X}|\mathbf{Y})}{N} . \tag{29}$$

VI. Weak polarization

In this section, we prove weak polarization for both the deletion channel and the trimmed deletion channel, as defined in Subsection III-C. As in [24], we will first prove that a certain process is submartingale, and then prove that it either converges to 0 or to 1.

As a first step, we will shortly define three entropies. These are defined with respect to an input $\mathbf{X}$ of length $N = 2^n$, which has a regular hidden-Markov input distribution, and $\mathbf{U} = \mathcal{A}_n(\mathbf{X})$. The corresponding output is denoted $\mathbf{Y}$. Recall that S_0 and S_N are the (hidden) states of the input process, just before $\mathbf{X}$ is transmitted and right after $\mathbf{X}$ is transmitted, respectively. Lastly, denote by $\mathbf{Y}^*$ the result of trimming all leading and trailing '0' symbols from $\mathbf{Y}$. Then, for a given n and $1 \le i \le N = 2^n$, define the following (deterministic) entropies:

$$h_i = H(U_i|U_1^{i-1}, \mathbf{Y}) , \tag{30}$$
$$\hat{h}_i = H(U_i|U_1^{i-1}, S_0, S_N, \mathbf{Y}) , \tag{31}$$
$$h_i^* = H(U_i|U_1^{i-1}, \mathbf{Y}^*) . \tag{32}$$

Clearly,

$$h_i^* \ge h_i \ge \hat{h}_i .$$

Note that in the case of a uniform input distribution, there is only one state, and hence h_i and $\hat{h}_i$ are equal.

Following [24], we show weak polarization by considering a sequence $B_1, B_2, \ldots$ of i.i.d. $\mathrm{Ber}(1/2)$ random variables. For any $n \in \mathbb{N}$, let $J_n = i(B_1, B_2, \ldots, B_n)$ be the random index defined by (4), with B_t in place of b_t. We will study the three related random processes defined for $n \in \mathbb{N}$ by

$$H_n = h_{J_n} , \tag{33}$$
$$\hat{H}_n = \hat{h}_{J_n} , \tag{34}$$
$$H_n^* = h_{J_n}^* . \tag{35}$$

The arguments below will show that $\hat{H}_n$ is a submartingale, converging to either 0 or 1. From this we will infer that H_n and H_n^* must converge to either 0 or 1 as well. Though neither H_n nor H_n^* are necessarily submartingales.

Theorem 12. *The sequence $\hat{H}_n$ converges (almost surely and in L^1) to a well-defined random variable $\hat{H}_\infty \in \{0, 1\}$ and, for any $\epsilon > 0$, it follows that*

$$\frac{1}{N} \left|\left\{i \in [N] \,|\, H(U_i|U_1^{i-1}, S_0, S_N, \mathbf{Y}) \in [\epsilon, 1-\epsilon]\right\}\right| \to 0. \tag{36}$$

Proof: Lemma 13 below shows that $\hat{H}_1, \hat{H}_2, \hat{H}_3, \ldots \in [0, 1]$ is a bounded submartingale with respect to J_n. This implies that the sequence $\hat{H}_n$ converges (almost surely and in L^1) to a limit that is denoted by $\hat{H}_\infty$ [26, p. 236]. Lemma 18 below shows that, for any $\epsilon > 0$, there is a $\Delta > 0$ such that $\hat{H}_n \in [\epsilon, 1-\epsilon]$ implies $\hat{H}_{n+1} > \hat{H}_n + \Delta$ with probability $\frac{1}{2}$. Thus, the sequence $\hat{H}_n$ cannot converge to the set $(0, 1)$ and hence $\hat{H}_\infty \in \{0, 1\}$.

From (31) and (34), we see that $\Pr\left(\hat{H}_n \in [\epsilon, 1-\epsilon]\right)$ equals

$$\frac{1}{N} \left|\left\{i \in [N] \,|\, H(U_i|U_1^{i-1}, S_0, S_N, \mathbf{Y}) \in [\epsilon, 1-\epsilon]\right\}\right| .$$

Since $\hat{H}_n$ converges almost surely to $\hat{H}_\infty$ and $\epsilon, 1-\epsilon$ are continuity points of $\Pr(\hat{H}_\infty \le x)$ [26, Ch. 4], it follows that

$$\lim_{n\to\infty} \Pr\left(\hat{H}_n \in [\epsilon, 1-\epsilon]\right) = \Pr\left(\hat{H}_\infty \in [\epsilon, 1-\epsilon]\right) = 0.$$

This completes the proof. ∎

Lemma 13. *For a hidden-Markov input distribution and a deletion channel with deletion probability δ, let $\hat{H}_n$ and J_n be as defined above. Then, the sequence $\hat{H}_1, \hat{H}_2, \hat{H}_3, \ldots$ is a bounded submartingale with respect to the $J_1, J_2, J_3, \ldots$ sequence.*

Proof: Since $\hat{H}_n$ is clearly bounded between 0 and 1, it remains to show that $E(\hat{H}_{n+1}|J_1, J_2, \ldots, J_n) \ge \hat{H}_n$. Let $\mathbf{X} \odot \mathbf{X}'$ be a length-$2N$ input to the channel. Denote by $\mathbf{Y} \odot \mathbf{Y}'$ the corresponding output, where $\mathbf{Y}$ only contains inputs from $\mathbf{X}$ and $\mathbf{Y}'$ only contains inputs from $\mathbf{X}'$. Recall that $\mathbf{U} = \mathcal{A}_n(\mathbf{X})$ and define $\mathbf{V} = \mathcal{A}_n(\mathbf{X}')$ and

$$\mathbf{F} = (U_1 \oplus V_1, V_1, U_2 \oplus V_2, V_2, \ldots, U_N \oplus V_N, V_N).$$

By (4), we have that $J_{n+1} = 2J_n - 1$ with probability $1/2$ and $J_{n+1} = 2J_n$ with probability $1/2$. Thus,

$$\begin{aligned}
&E(\hat{H}_{n+1}|J_1^n) \\
&= E\big(H(F_{J_{n+1}}|F_1^{J_{n+1}-1}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N})|J_1^n\big) \\
&= \frac{1}{2} H(F_{2J_n-1}|F_1^{2J_n-2}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\
&\quad + \frac{1}{2} H(F_{2J_n}|F_1^{2J_n-1}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\
&= \frac{1}{2} H(F_{2J_n-1}, F_{2J_n}|F_1^{2J_n-2}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\
&= \frac{1}{2} H(U_{J_n} \oplus V_{J_n}, V_{J_n}|F_1^{2J_n-2}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\
&= \frac{1}{2} H(U_{J_n}, V_{J_n}|U_1^{J_n-1}, V_1^{J_n-1}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\
&\overset{(a)}{\ge} \frac{1}{2} H(U_{J_n}, V_{J_n}|U_1^{J_n-1}, V_1^{J_n-1}, \mathbf{Y}, \mathbf{Y}', S_0, S_{2N}) \\
&\overset{(b)}{\ge} \frac{1}{2} H(U_{J_n}, V_{J_n}|U_1^{J_n-1}, V_1^{J_n-1}, \mathbf{Y}, \mathbf{Y}', S_0, S_N, S_{2N}) \\
&\overset{(c)}{=} \frac{1}{2} H(U_{J_n}|U_1^{J_n-1}, \mathbf{Y}, S_0, S_N) \\
&\quad + \frac{1}{2} H(V_{J_n}|V_1^{J_n-1}, \mathbf{Y}', S_N, S_{2N}) \\
&\overset{(d)}{=} \hat{H}_n.
\end{aligned}$$

The inequality (a) follows from the fact that $\mathbf{Y} \odot \mathbf{Y}'$ is a deterministic function of $\mathbf{Y}, \mathbf{Y}'$. Inequality (b) follows

since conditioning reduces entropy. Step (c) holds by the Markov property. Finally, (d) is due to stationarity: $\hat{H}_n = H(U_{J_n}|U_1^{J_n-1}, \mathbf{Y}, S_0, S_N) = H(V_{J_n}|V_1^{J_n-1}, \mathbf{Y}', S_N, S_{2N})$. ■

Since the sequence $\hat{H}_n$ is a bounded submartingale, it converges almost surely and in L_1 to a random variable $\hat{H}_\infty \in [0,1]$. To show that $\hat{H}_\infty \in \{0,1\}$ with probability 1, one can show that, if $\epsilon \leq \hat{H}_n \leq 1-\epsilon$, then there is a $\Delta = \Delta(\epsilon) > 0$ such that $\hat{H}_n^- - \hat{H}_n > \Delta(\epsilon)$, where

$$\hat{H}_n^- \triangleq H(U_{J_n} \oplus V_{J_n} | U_1^{J_n-1}, V_1^{J_n-1}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \ . \quad (37)$$

That is, a 'minus' operation applied to non-polarized entropy changes the entropy by at least Δ. Such a result indeed establishes the above, since it dictates that $\hat{H}_n$ cannot converge to anything other than either 0 or 1. As before, we first prove the above for the simple case of i.i.d. uniform input, and then generalize to a hidden-Markov input.

A. Uniform input

Lemma 14. *Let $\mathbf{X}$ and $\mathbf{X}'$ be independent vectors of length $N = 2^n$, both drawn from an i.i.d. uniform distribution. Let $\hat{H}_n$ and $\hat{H}_n^-$ be as defined in (31), (34), and (37), with S_0, S_N and S_{2N} being degenerate random variables always taking the value 1. Then, for every $\epsilon > 0$ there exists $\Delta(\epsilon) > 0$ such that if $\epsilon \leq \hat{H}_n \leq 1-\epsilon$, then $\hat{H}_n^- - \hat{H}_n > \Delta(\epsilon)$.*

Proof: Denote $i = J_n$, and assume a fixed ϵ for which $\epsilon \leq \hat{H}_n \leq 1-\epsilon$. Then, since S_0, S_N, and S_{2N} are degenerate, we observe that $(U_i, U_1^{i-1}, \mathbf{Y})$ is independent of $(V_i, V_1^{i-1}, \mathbf{Y}')$. It follows that

$$H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}')$$

is the entropy of the modulo-2 sum of the independent binary random variables U_i and V_i . Thus, Mrs. Gerber's Lemma [27, Lemma 2.2] implies that, for every $\epsilon > 0$, there is $\Delta > 0$ such that

$$H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}') - H(U_i | U_1^{i-1}, \mathbf{Y}) \geq \Delta \ .$$

Since

$$\begin{aligned} \hat{H}_{n+1}^- &= H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y} \odot \mathbf{Y}') \\ &\geq H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}'), \end{aligned}$$

the result follows. ■

B. Hidden-Markov input

The proof of Lemma 14 above relied on the mutual independence of $(U_i, U_1^{i-1}, \mathbf{Y})$ and $(V_i, V_1^{i-1}, \mathbf{Y}')$. To emulate[6] this property in a FAIM setting, we note that for s_0, s_N, and s_{2N} fixed, we indeed have that $(U_i, U_1^{i-1}, \mathbf{Y})$ and $(V_i, V_1^{i-1}, \mathbf{Y}')$ are independent, when conditioning on the event $S_0 = s_0$, $S_N = s_N$, $S_{2N} = s_{2N}$. Towards this end, for $s_0, s_N, s_{2N} \in \mathcal{S}$, we denote the probability of these three states occurring as

$$p(s_0, s_N, s_{2N}) = \Pr(S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}) \ . \quad (38)$$

[6]For independence, it is sufficient to condition on the event $S_N = s_N$. Conditioning on the more specific event $S_0 = s_0$, $S_N = s_N$, $S_{2N} = s_{2N}$ is needed for latter parts.

In the reminder of this subsection, we will assume that N is large enough such that the above probability is always positive. This is indeed possible, by the following lemma.

Lemma 15. *For $s \in \mathcal{S}$, denote by $\pi(s)$ the stationary probability of s. That is, the probability that $S_0 = s$. Let*

$$\pi_{\min} = \min_{s \in \mathcal{S}} \pi(s) \ ,$$

Then, $\pi_{\min} > 0$, and there exists a ν such that for all $N \geq 2^\nu$ and all $s_0, s_N, s_{2N} \in \mathcal{S}$ we have

$$\Pr(S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}) > \frac{(\pi_{\min})^3}{2} \ . \quad (39)$$

Proof: Since the underlying Markov chain is regular (i.e., finite-state, irreducible, and aperiodic), some power of the transition matrix must be strictly positive and this implies that $\pi_{\min} > 0$. Regularity further implies that S_0, S_N, S_{2N} become asymptotically independent as N increases. Thus, there must be an $N_0 = 2^{n_0}$ such that (39) holds for all $N \geq N_0$. ■

For (s_0, s_N, s_{2N}), we define the quantities $\alpha(s_0, s_N, s_{2N})$ and $\beta(s_0, s_N, s_{2N})$ as follows.

$$\begin{aligned} &\alpha(s_0, s_N, s_{2N}) \triangleq \quad (40) \\ &H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}', S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}) \end{aligned}$$

and

$$\beta(s_0, s_N, s_{2N}) \triangleq \frac{\gamma(s_0, s_N) + \gamma(s_N, s_{2N})}{2} \ , \quad (41)$$

where

$$\gamma(s_0, s_N) \triangleq H(U_i | U_1^{i-1}, \mathbf{Y}, S_0 = s_0, S_N = s_N) \ . \quad (42)$$

Note that by stationarity,

$$\gamma(s_N, s_{2N}) = H(V_i | V_1^{i-1}, \mathbf{Y}', S_N = s_N, S_{2N} = s_{2N}) \ .$$

The following lemma states how α and β are related to our quantities of interest, $\hat{H}_n$ and $\hat{H}_n^-$.

Lemma 16. *Let $N = 2^n > 2^\nu$, where ν was promised in Lemma 15. Then, for α and β as defined above, we have that*

$$\hat{H}_n^- \geq \sum_{s_0, s_N, s_{2N} \in \mathcal{S}} p(s_0, s_N, s_{2N}) \cdot \alpha(s_0, s_N, s_{2N}) \ , \quad (43)$$

and

$$\hat{H}_n = \sum_{s_0, s_N, s_{2N} \in \mathcal{S}} p(s_0, s_N, s_{2N}) \cdot \beta(s_0, s_N, s_{2N}) \ . \quad (44)$$

Furthermore, for all $s_0, s_N, s_{2N} \in \mathcal{S}$,

$$\alpha(s_0, s_N, s_{2N}) \geq \beta(s_0, s_N, s_{2N}) \ . \quad (45)$$

Proof: Define $i = J_n$. To prove (43), we proceed similarly to the proof in Lemma 13 and deduce that

$$\begin{aligned} \hat{H}_n^- &= H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y} \odot \mathbf{Y}', S_0, S_{2N}) \\ &\geq H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}', S_0, S_{2N}) \\ &\geq H(U_i \oplus V_i | U_1^{i-1}, V_1^{i-1}, \mathbf{Y}, \mathbf{Y}', S_0, S_N, S_{2N}) \\ &= \sum_{s_0, s_N, s_{2N} \in \mathcal{S}} p(s_0, s_N, s_{2N}) \cdot \alpha(s_0, s_N, s_{2N}) \ , \end{aligned}$$

The proof of (44) follows by stationarity. That is,

$$\hat{H}_n = H(U_i | U_1^{i-1}, \mathbf{Y}, S_0, S_N)$$

$$= \frac{H(U_i|U_1^{i-1}, \mathbf{Y}, S_0, S_N) + H(V_i|V_1^{i-1}, \mathbf{Y}', S_N, S_{2N})}{2}$$
$$= \sum_{s_0,s_N,s_{2N}\in\mathcal{S}} p(s_0, s_N, s_{2N}) \cdot \frac{\gamma(s_0, s_N) + \gamma(s_N, s_{2N})}{2}$$
$$= \sum_{s_0,s_N,s_{2N}\in\mathcal{S}} p(s_0, s_N, s_{2N}) \cdot \beta(s_0, s_N, s_{2N}) \ .$$

By (41), we deduce that (45) will follow from proving that

$$\alpha(s_0, s_N, s_{2N}) \geq \gamma(s_0, s_N) \tag{46}$$

and

$$\alpha(s_0, s_N, s_{2N}) \geq \gamma(s_N, s_{2N}) \tag{47}$$

W.l.o.g, we prove (46). Indeed, given that $S_N = s_N$, we have by the Markov property that $(S_0, U_1^{i-1}, U_i, \mathbf{Y})$ and $(V_1^{i-1}, V_i, \mathbf{Y}', S_{2N})$ are independent. Hence, for any s_{2N} we may also write γ, defined in (42), as

$$\gamma(s_0, s_N) = H(U_i|U_1^{i-1}, V_1^{i-1}, V_i, \mathbf{Y}, \mathbf{Y}', S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}) \ .$$

Lastly, note that in the above expression for γ, since we condition on V_i, we could have written $U_i \oplus V_i$ in place of U_i. This would give us the expression for α in (40), up to a further conditioning on V_i. Since conditioning reduces entropy, (46) follows. As noted, the proof of (47) is similar. Hence, we deduce (45). ∎

In light of Lemma 16, our plan is to show the existence of a triplet (s_0, s_N, s_{2N}) for which $\alpha(s_0, s_N, s_{2N})$ is substantially greater than $\beta(s_0, s_N, s_{2N})$. The next lemma assures us such a triplet indeed exists.

Lemma 17. *For every $\epsilon > 0$ there exists a $\Delta' = \Delta'(\epsilon)$ for which the following holds. Let $N = 2^n > 2^\nu$, where ν was promised in Lemma 15. Then, if $\epsilon \leq \hat{H}_n \leq 1 - \epsilon$, then there exists a triplet s_0, s_N, s_{2N} such that*

$$\alpha(s_0, s_N, s_{2N}) > \beta(s_0, s_N, s_{2N}) + \Delta' \ . \tag{48}$$

Proof: By definition of γ in (42), we have that

$$\hat{H}_n = \sum_{s_0,s_N\in\mathcal{S}} \Pr(S_0 = s_0, S_N = s_N) \cdot \gamma(s_0, s_N) \tag{49}$$
$$= \sum_{s_N,s_{2N}\in\mathcal{S}} \Pr(S_N = s_N, S_{2N} = s_{2N}) \cdot \gamma(s_N, s_{2N}) \ ,$$

where the second equality follows by stationarity. A crucial point will be to show the existence of a triplet (s_0, s_N, s_{2N}) for which $(\hat{H}_n - \gamma(s_0, s_N)) \cdot (\hat{H}_n - \gamma(s_N, s_{2N})) \leq 0$. In other words, either

$$\gamma(s_0, s_N) \leq \hat{H}_n \quad \text{and} \quad \gamma(s_N, s_{2N}) \geq \hat{H}_n \ , \tag{50}$$

or

$$\gamma(s_0, s_N) \geq \hat{H}_n \quad \text{and} \quad \gamma(s_N, s_{2N}) \leq \hat{H}_n \ . \tag{51}$$

To show this by contradiction, we start by supposing that this is not the case. Then, for all $s_0, s_N, s_{2N} \in \mathcal{S}$, it must be that

$$(\hat{H}_n - \gamma(s_0, s_N)) \cdot (\hat{H}_n - \gamma(s_N, s_{2N})) > 0 \ . \tag{52}$$

Fix some arbitrary $a, b \in \mathcal{S}$. By specializing s_0 to a and s_N to b in (52), we deduce that $\hat{H}_n \neq \gamma(a, b)$. Assume w.l.o.g. that $\gamma(a, b) < \hat{H}_n$. We now claim that for all $c, d \in \mathcal{S}$,

$$\gamma(c, d) < \hat{H}_n \ . \tag{53}$$

Indeed, let $c, d \in \mathcal{S}$ be given. By setting $s_0 = a$, $s_N = b$, $s_{2N} = c$, we deduce from (52) that $\gamma(b, c) < \hat{H}_n$. Hence, if we set $s_0 = b$, $s_N = c$, $s_{2N} = d$ in (52), we deduce (53).

From the above paragraph, we conclude that for all $s_0, s_N \in \mathcal{S}$, we must have that $\gamma(s_0, s_N) < \hat{H}_n$. However, recalling from (49) that $\hat{H}_n$ is a weighted average of such γ terms, we arrive at a contradiction. Hence, there exists a triplet (s_0, s_N, s_{2N}) for which either (50) or (51) holds. This is the triplet we are searching for. Indeed, since we have assumed that $\epsilon \leq \hat{H}_n \leq 1 - \epsilon$, the above triplet satisfies

$$\min\{\gamma(s_0, s_N), \gamma(s_N, s_{2N})\} \leq 1 - \epsilon$$

and

$$\max\{\gamma(s_0, s_N), \gamma(s_N, s_{2N})\} \geq \epsilon \ .$$

Our result now follows by combining part (i) of [27, Lemma 2.2] with[7] [20, Lemma 11]. ∎

Combining Lemmas 16 and 17 gives the following key result.

Lemma 18. *For every $\epsilon > 0$ there exists $\Delta = \Delta(\epsilon)$ for which the following holds. Let $N = 2^n > 2^\nu$, where ν was promised in Lemma 15. Then, if $\epsilon < \hat{H}_n \leq 1 - \epsilon$, then*

$$\hat{H}_n^- - \hat{H}_n > \Delta(\epsilon)$$

Proof: Take

$$\Delta = \frac{\Delta' \cdot (\pi_{\min})^3}{2} \ ,$$

where Δ' is as defined in Lemma 17. Now, simply combine (39), (43), (44), (45) and the existence of triplet s_0, s_N, s_{2N} for which (48) holds, to yield the claim. ∎

The following lemma will be useful.

Lemma 19. *For $n \in \mathbb{N}$, let A_n and B_n be real random variables defined on a common probability space. Suppose B_n converges in L^1 to B_∞ and $E(A_n)$ converges to $E(B_\infty)$. If $A_n \geq B_n$ for all $n \in \mathbb{N}$, then A_n converges in L^1 to B_∞.*

Proof: By definition, B_n converges to B_∞ in L^1 if and only if $E(|B_n - B_\infty|) \to 0$. Thus, by the triangle inequality,

$$\begin{aligned} E(|A_n - B_\infty|) &\leq E(|A_n - B_n|) + E(|B_n - B_\infty|) \\ &= E(A_n - B_n) + E(|B_n - B_\infty|) \\ &= E(A_n) - E(B_n) + E(|B_n - B_\infty|). \end{aligned}$$

In the limit, the first two terms converge to $E(B_\infty)$ and the last term converges to 0. Thus, $E(|A_n - B_\infty|) \to 0$. ∎

The following theorem claims weak polarization for the three cases discussed earlier.

Theorem 20. *Fix $\epsilon \in (0, 1)$ and let $N = 2^n$. For a given hidden-Markov input distribution, let $\mathbf{X} = (X_1, X_2, \ldots, X_N)$*

[7] The first two strict inequalities in the statement of [20, Lemma 11] are essentially typos: they should both be replaced by weak inequalities, as is evident from reading the beginning of the proof.

be a random vector with the above distribution. Let $\mathbf{Y}$ *be the result of passing* $\mathbf{X}$ *through a deletion channel with deletion probability* δ*. Denote* $\mathbf{U} = \mathcal{A}(\mathbf{X})$*. Let* S_0 *and* S_N *be as in Definition 1. Then,*

$$\lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}, S_0, S_N) < \epsilon\right\}\right|}{N} \tag{54a}$$
$$= \lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}) < \epsilon\right\}\right|}{N} \tag{54b}$$
$$= \lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}^*) < \epsilon\right\}\right|}{N} \tag{54c}$$
$$= 1 - \lim_{n\to\infty} \frac{H(\mathbf{X}|\mathbf{Y})}{N} \tag{54d}$$

and

$$\lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}, S_0, S_N) > 1-\epsilon\right\}\right|}{N} \tag{55a}$$
$$= \lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}) > 1-\epsilon\right\}\right|}{N} \tag{55b}$$
$$= \lim_{n\to\infty} \frac{\left|\left\{i : H(U_i|U_1^{i-1}, \mathbf{Y}^*) > 1-\epsilon\right\}\right|}{N} \tag{55c}$$
$$= \lim_{n\to\infty} \frac{H(\mathbf{X}|\mathbf{Y})}{N} \tag{55d}$$

Proof: For simplicity, the proof is split into 4 parts.

Part I: (54d) and (55d) are well defined: Recall from Lemma 9 that $\lim_{n\to\infty} H(\mathbf{X}|\mathbf{Y})/N$ exists. Thus, the right hand sides of both (54d) and (55d) are well defined.

Part II: (54a)=(54d) and (55a)=(55d): Since the Arıkan transform is invertible, it follows that $\hat{\mathcal{H}}_N = H(\mathbf{X}|\mathbf{Y}, S_0, S_N) = H(\mathbf{U}|\mathbf{Y}, S_0, S_N)$, where $\hat{\mathcal{H}}_N$ is defined in (27). Thus, from the chain rule for entropy, we observe that

$$\begin{aligned} E(\hat{H}_n) &= \frac{1}{N}\sum_{i=1}^{N} H(U_i|U_1^{i-1}, \mathbf{Y}, S_0, S_N) \\ &= \frac{1}{N} H(\mathbf{U}|\mathbf{Y}, S_0, S_N) \\ &= \frac{1}{N}\hat{\mathcal{H}}_N. \end{aligned}$$

From Theorem 12, we see that $\hat{H}_n$ converges in L^1 to $\hat{H}_\infty \in \{0,1\}$. This implies that $E(\hat{H}_\infty) = \lim_{n\to\infty} E(\hat{H}_n)$ which exists and equals $\lim_{N\to\infty} \hat{\mathcal{H}}_N/N$ by Lemma 10. Since $\hat{H}_\infty \in \{0,1\}$, observing that $E(\hat{H}_\infty) = \Pr(\hat{H}_\infty = 1)$ shows that

$$(55a) = \lim_{n\to\infty} \Pr(\hat{H}_n > 1-\epsilon) = \Pr(\hat{H}_\infty = 1) = \lim_{n\to\infty} \frac{1}{N}\hat{\mathcal{H}}_N,$$

where the second equality holds because convergence in L^1 implies convergence in distribution and $1-\epsilon$ is a continuity point of $\Pr(\hat{H}_\infty \le x)$ [26, Ch. 4]. Since Lemma 11 shows that $\lim_{N\to\infty} \hat{\mathcal{H}}_N/N$ equals (55d), it follows that (55a) equals (55d). The last step is observing that

$$(54a) = \lim_{n\to\infty} \Pr(\hat{H}_n < \epsilon) = \Pr(\hat{H}_\infty = 0) = 1 - \Pr(\hat{H}_\infty = 1)$$

holds because convergence in L^1 implies convergence in distribution and ϵ is a continuity point of $\Pr(\hat{H}_\infty \le x)$. Thus, (54a) equals (54d).

Part III: (54c)=(54d) and (55c)=(55d): To prove these equalities, we will apply Lemma 19 to the sequences $A_n = H_n^*$ and $B_n = \hat{H}_n$. Theorem 12 shows that $\hat{H}_n$ converges in L^1 to $\hat{H}_\infty$ and we established in the previous part that $E(\hat{H}_\infty)$ equals (55d). From the definitions in (34) and (35), it follows that $H_n^* \ge \hat{H}_n$ for all $n \in \mathbb{N}$. The only other element required for Lemma 19 is that $E(H_n^*) \to E(\hat{H}_\infty)$ and this will be shown below. Assuming this for now, we observe Lemma 19 implies that H_n^* converges in L^1 to $\hat{H}_\infty$ and gives the desired result

$$(54c) = \lim_{n\to\infty} \Pr(H_n^* < \epsilon) = \Pr(\hat{H}_\infty < \epsilon) = (54d)$$
$$(55c) = \lim_{n\to\infty} \Pr(H_n^* > 1-\epsilon) = \Pr(\hat{H}_\infty > 1-\epsilon) = (55d),$$

where the second equality on each line holds because convergence in L^1 implies convergence in distribution and $\epsilon, 1-\epsilon$ are continuity points of $\Pr(\hat{H}_\infty \le x)$ [26, Ch. 4].

To show that $E(H_n^*) \to E(\hat{H}_\infty)$, we will use the fact that

$$\begin{aligned} &H(\mathbf{U}|\mathbf{Y}, S_0, S_N) \le H(\mathbf{U}|\mathbf{Y}^*) \le \\ &\quad H(\mathbf{U}|\mathbf{Y}, S_0, S_N) + 2\log_2|\mathcal{S}| + 2\log_2(N+1)\,. \end{aligned} \tag{56}$$

Indeed, the first inequality holds because $\mathbf{Y}^*$ is a function of $\mathbf{Y}$. The second inequality follows from first noting that

$$H(\mathbf{U}|\mathbf{Y}^*) \le H(\mathbf{Y}, S_0, S_N, \mathbf{U}|\mathbf{Y}^*)\,.$$

And then observing that

$$\begin{aligned} &H(\mathbf{Y}, S_0, S_N, \mathbf{U}|\mathbf{Y}^*) \\ &\quad = H(\mathbf{Y}|\mathbf{Y}^*) + H(S_0, S_N|\mathbf{Y}, \mathbf{Y}^*) + H(\mathbf{U}|\mathbf{Y}, \mathbf{Y}^*, S_0, S_N) \\ &\quad \overset{(a)}{=} H(\mathbf{Y}|\mathbf{Y}^*) + H(S_0, S_N|\mathbf{Y}, \mathbf{Y}^*) + H(\mathbf{U}|\mathbf{Y}, S_0, S_N) \\ &\quad \overset{(b)}{\le} H(\mathbf{Y}|\mathbf{Y}^*) + 2\log_2|\mathcal{S}| + H(\mathbf{U}|\mathbf{Y}, S_0, S_N) \\ &\quad \overset{(c)}{\le} 2\log_2(N+1) + 2\log_2|\mathcal{S}| + H(\mathbf{U}|\mathbf{Y}, S_0, S_N)\,, \end{aligned}$$

where (a) follows from $\mathbf{Y}^*$ being a function of $\mathbf{Y}$, (b) follows by S_0 and S_N each having a support of size $|\mathcal{S}|$, and (c) follows since in order to construct $\mathbf{Y}$ from $\mathbf{Y}^*$, it suffices to be told how many '0' symbols have been trimmed from each side of $\mathbf{Y}$, and both numbers are always between 0 and N. Combining the above two displayed equations yields the RHS of (56).

Finally, we divide both sides of (56) by N and take the limit as $N \to \infty$. Since the left-most and right-most terms converge to $E(\hat{H}_\infty)$, the sandwich property implies that the center term, $E(H_n^*)$ also converges to this quantity.

Part IV: (54a)=(54b)=(54c) and (55a)=(55b)=(55c): Note that, for $1 \le i \le N$, we have

$$H(U_i|U_1^{i-1}, \mathbf{Y}, S_0, S_N) \le H(U_i|U_1^{i-1}, \mathbf{Y}) \le H(U_i|U_1^{i-1}, \mathbf{Y}^*)\,.$$

We have already proved that (54a)=(54c) and (55a)=(55c). Thus, by the sandwich property, (54a)=(54b)=(54c) and (55a)=(55b)=(55c). ∎

VII. Strong polarization

To rigorously claim a coding scheme for the deletion channel, one must also show strong polarization. For this, Theorem 20 is not sufficient and, so far, we have been unable to prove strong polarization for the *standard* polar code construction. Thus, we will modify the standard coding scheme to proceed.

A. Overview of Coding Scheme

Fix a deletion probability δ and a regular hidden Markov input distribution. Recall that our goal is to achieve the information rate $\mathcal{I}$ given in (23). For didactic reasons, we first consider a simplified setting in which this goal is easily attained. Specifically, let N_0 be given parameter, and consider a block-TDC with block length N_0 and deletion probability δ. That is, for each input block $\mathbf{X}(\phi)$ of length N_0, where $\phi = 1, 2, \ldots$, the channel outputs $\mathbf{Y}^*(\phi)$, which is the result of passing $\mathbf{X}(\phi)$ through a TDC with deletion probability δ. The crucial point to note is that, contrary to a deletion channel, the output of a block-TDC *contains commas between segments*. That is, we know exactly which output segment corresponds to which input block.

How would one code for such a channel and achieve a rate approaching $\mathcal{I}$? For this, we will assume that

$$N_0 = 2^{n_0} \ , \tag{57}$$

and that we can choose N_0 to be arbitrarily large. Let

$$\Phi = 2^{n_1} \tag{58}$$

be the number of blocks we will transmit through the channel. Consider the following input distribution: each block $\mathbf{X}(\phi)$ will be distributed according to the input distribution that we have fixed at the start of this subsection, and the input blocks $\mathbf{X}(1), \mathbf{X}(2), \ldots, \mathbf{X}(\Phi)$ will be *i.i.d.* In a nutshell, this suffices to achieve a coding rate of $\mathcal{I}$ with vanishing probability of error for the following two reasons. First, Theorem 20 shows weak polarization for each block and, in each block, we have the required fractions of high-entropy/low-entropy indices. Second, the independence between blocks implies that strong polarization will occur.

We now back the above claim with a few more details. We denote the output of the encoder — the concatenation of the above blocks — by

$$\mathbf{X} = \mathbf{X}(1) \odot \mathbf{X}(2) \odot \cdots \odot \mathbf{X}(\Phi) \ . \tag{59}$$

This output has length

$$N = N_0 \cdot \Phi = 2^{n_0+n_1} = 2^n \ . \tag{60}$$

We will use a sans-serif font to denote a vector whose elements are 'blocks'. Thus, we will denote the partitioning of the above $\mathbf{X}$ into blocks of length N_0 by

$$\mathsf{X} = (\mathbf{X}(1), \mathbf{X}(2), \ldots, \mathbf{X}(\Phi)) \ . \tag{61}$$

The corresponding output of the block-TDC is denoted

$$\mathsf{Y}^* = (\mathbf{Y}^*(1), \mathbf{Y}^*(2), \ldots, \mathbf{Y}^*(\Phi)) \ . \tag{62}$$

That is, Y^* is comprised of Φ distinguishable blocks — it is *not* simply the concatenation of the $\mathbf{Y}^*(\phi)$. The superscript '$*$' in Y^* suggest that trimming operation is applied *blockwise*.

We first consider the polar transform of $\mathbf{X}(\phi)$, denoted[8]

$$\mathbf{V}(\phi) = \mathcal{A}(\mathbf{X}(\phi)) \ , \tag{63}$$

where $1 \le \phi \le \Phi$. Note that $\mathbf{V}(\phi)$ is a binary vector of length N_0,

$$\mathbf{V}(\phi) = (V_1(\phi), V_2(\phi), \ldots, V_{N_0}(\phi)) \ .$$

Recall that $\mathbf{Y}^*(\phi)$ is the output corresponding to $\mathbf{X}(\phi)$, and note that since we have assumed that the $\mathbf{X}(\phi)$ are i.i.d., then this must also hold for triplets $(\mathbf{X}(\phi), \mathbf{V}(\phi), \mathbf{Y}^*(\phi))$, when ranging over $1 \le \phi \le \Phi$.

For a fixed $1 \le \phi \le \Phi$ and a given $1 \le i_0 \le N_0$, consider the pair of entropies

$$H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi), \mathbf{Y}^*(\phi)) \ \text{ and } \ H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi)) \ . \tag{64}$$

We now make two important observations. First, since we have already established that the $(\mathbf{X}(\phi), \mathbf{V}(\phi), \mathbf{Y}^*(\phi))$ are i.i.d. over ϕ, we deduce that (64) is independent of ϕ. Second, both entropies in (64) exhibit slow polarization, in the sense of Theorem 20. That is, on one hand, we deduce that (54c)=(54d) and (55c)=(55d), if in both (54c) and (55c) we replace U_i, U_1^{i-1}, $\mathbf{Y}^*$, n and N by $V_{i_0}(\phi)$, $V_1^{i_0-1}(\phi)$, $\mathbf{Y}^*(\phi)$, n_0 and N_0, respectively. These statements hold for all $\delta \in [0, 1]$. For the special case of $\delta = 1$, one gets a degenerate channel where $\mathbf{Y}^*(\phi)$ always equals the empty string. Thus, on the other hand, the same claim of (54c)=(54d) and (55c)=(55d), under the above substitutions continues to hold, with $\mathbf{Y}$ and $\mathbf{Y}^*$ removed from these equations.

Since the first entropy in (64) is always less than or equal to the second, we deduce from the above paragraph and the first half of Theorem 20 that for $\epsilon \in (0, 1)$ fixed, the fraction of indices i_0 for which

$$H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi), \mathbf{Y}^*(\phi)) < \epsilon \quad \text{and} \quad H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi)) \ge \epsilon$$

tends to

$$\left(1 - \lim_{n_0 \to \infty} \frac{H(\mathbf{X}(\phi)|\mathbf{Y}(\phi)))}{N_0}\right) - \left(1 - \lim_{n_0 \to \infty} \frac{H(\mathbf{X}(\phi))}{N_0}\right) = \mathcal{I} \ ,$$

as $n_0 \to \infty$. For simplicity of exposition, let us further restrict ϵ to $\epsilon \in (0, 1/2)$. By both halves of Theorem 20, we deduce that the fraction of indices i_0 for which

$$\epsilon \le H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi)) \le 1 - \epsilon$$

vanishes. The conclusion is stated as a lemma, for future reference.

Lemma 21. *For $\epsilon \in (0, 1/2)$ fixed, the fraction of indices $1 \le i_0 \le N_0$ for which*

[8] We reserve the letter U, commonly used to denote the result of a polar transform, for a related yet distinct definition that is yet to appear.

$$H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi),\mathbf{Y}^*(\phi)) < \epsilon \quad \textit{and} \quad H(V_{i_0}(\phi)|V_1^{i_0-1}(\phi)) > 1-\epsilon \tag{65}$$

tends to $\mathcal{I}$, as $n_0 \to \infty$, and is the same for every $1 \le \phi \le \Phi$.

We now note that for a given ϕ and i_0, we have an efficient method of calculating the probabilities corresponding to (65). Namely, this is achieved by using the base trellis defined for a TDC in Subsection III-C, applying a series of plus and minus polarization operations on it, according to the binary representation of $i_0 - 1$, and then invoking (22). That is, the only thing stopping us from applying the Honda-Yamamoto scheme [28] at this point is the fact that the above ϵ is fixed.

Informally, we overcome the above problem as follows. Take ϵ 'small' and n_0 as well as n_1 'large'. Consider a 'good' index i_0. That is, an index i_0 for which (65) holds. This will be the case for a fraction of indices 'very close' to $\mathcal{I}$. Next, recall the definition of $\mathbf{X}$ in (59), and denote its polar transform as

$$\mathbf{U} = \mathcal{A}(\mathbf{X}) \ .$$

Consider the subvector $U_{(i_0-1)\cdot\Phi+1}^{i_0\cdot\Phi}$. It is not hard to prove that

$$U_{(i_0-1)\cdot\Phi+1}^{i_0\cdot\Phi} = \mathcal{A}((V_{i_0}(1), V_{i_0}(2), \ldots, V_{i_0}(\Phi))) \ . \tag{66}$$

That is, the LHS of (66) is gotten by applying the Arıkan transform to the vector $(V_{i_0}(1), V_{i_0}(2), \ldots, V_{i_0}(\Phi))$. Since each entry of this vector satisfies (65), 'almost all' indices i of $\mathbf{U}$, where $(i_0-1)\cdot\Phi + 1 \le i \le i_0 \cdot \Phi$ are strongly polarized. That is, satisfy

$$Z(U_i|U_1^{i-1},\mathsf{Y}^*) < 2^{-n_1\beta} \quad \text{and} \quad K(U_i|U_1^{i-1}) < 2^{-n_1\beta} \tag{67}$$

where Z and K are the conditional Bhattacharyya parameter and the conditional total variation (see Definitions 7 and 8 in Appendix A), $\beta < 1/2$ is some fixed constant, and Y^* is the block-TDC output vector defined in (62). That is, the overall fraction of useful indices $1 \le i \le N_0\Phi$ with respect to the Honda-Yamamoto scheme will be 'very close' to $\mathcal{I}$, and the error of the scheme will approach 0 at a rate of roughly $2^{-\sqrt{N_1}}$.

The reader may not be surprised to learn that the above informal statements can be made rigorous and proven[9]. Indeed, this will be done as part of the proof of Theorem 1. However, one important point remains to be addressed. That is, the channel we will in fact be coding for is the deletion channel, and *not* the block-TDC. Hence, in the above description, we have implicitly assumed a genie which has manufactured the punctuated vector Y^* for us. The purpose of the guard-bands, defined shortly, is to approximate such a genie in practice.

Our actual coding scheme will be as follows. For the encoding step, we will first use the Honda-Yamamoto scheme with respect to the block-TDC. I.e., the information bits will be placed in indices j of $\mathbf{U}$ for which (67) holds. The resulting codeword will be $\mathbf{X}$. Then, we will add to $\mathbf{X}$ runs of '0' symbols in key locations, and transmit the resulting word (which will be longer than $\mathbf{X}$) on the deletion channel. On the decoder side, a preliminary step will be to deduce the punctuated vector Y^* from the received vector $\mathbf{Y}$. That is, we will remove the guard bands (and trim the $\mathbf{Y}(\phi)$ into $\mathbf{Y}^*(\phi)$ in the process), thus producing Y^*. Then, the decoder will be applied on Y^* to yield $\mathbf{U}$, and thus the information bits.

[9]Such a proof is not a straightforward adaptation of the ideas in [24] and [29]. Namely, it requires the use of [30, Lemma 40], which we indeed invoke in the proof of Theorem 1.

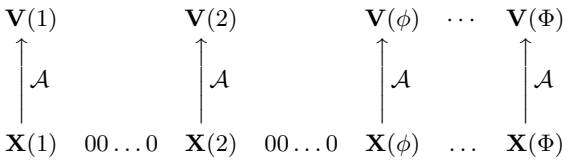

Fig. 2. The $\Phi = N/N_0$ blocks, denoted $\mathbf{X}(1), \mathbf{X}(2), \ldots, \mathbf{X}(\Phi)$, have length $N_0 = 2^{n_0}$, are i.i.d., and each is distributed according to the regular hidden-Markov input distribution. Their polar transforms are $\mathbf{V}(1), \mathbf{V}(2), \ldots, \mathbf{V}(\Phi)$. An additional $n - n_0$ polarization steps (not shown) will be applied to $\mathbf{V}(1), \mathbf{V}(2), \ldots, \mathbf{V}(\Phi)$, resulting in $\mathbf{U}$. The transmitted codeword is gotten by separating consecutive $\mathbf{X}(\cdot)$ vectors by a 'guard band'. That is, by a string of '0' symbols. The length of the guard bands is not constant. For example, the middle guard band is always the longest, while the first and last guard bands are always the shortest.

B. Guard bands

In this subsection, we first describe how the guard bands are added to $\mathbf{X}$ on the encoder side. We then explain how the decoder deduces the punctuated vector Y^* from the received vector $\mathbf{Y}$.

We start by defining how guard bands are added between the blocks $\mathbf{X}(1), \mathbf{X}(2), \ldots, \mathbf{X}(\Phi)$, see Figure 2. That is, we define how $\mathbf{X}$ is transformed into $g(\mathbf{X})$. This is done in a simple recursive manner. Informally, let $\mathbf{x}$ be a vector of length 2^n. If this length is greater than the designated block-length N_0, we halve $\mathbf{x}$, add ℓ_n '0' symbols in the middle, and then apply g recursively to each original half. Namely, for $\mathbf{x} = \mathbf{x}_{\mathrm{I}} \odot \mathbf{x}_{\mathrm{II}} \in \mathcal{X}^{2^n}$ with

$$\mathbf{x}_{\mathrm{I}} = x_1^{2^{n-1}} \in \mathcal{X}^{2^{n-1}} \ , \quad \mathbf{x}_{\mathrm{II}} = x_{2^{n-1}+1}^{2^n} \in \mathcal{X}^{2^{n-1}}$$

being the first and second halves of $\mathbf{x}$, respectively, we define

$$g(\mathbf{x}) \triangleq \begin{cases} \mathbf{x} & \text{if } n \le n_0 \\ g(\mathbf{x}_{\mathrm{I}}) \odot \overbrace{00\ldots0}^{\ell_n} \odot g(\mathbf{x}_{\mathrm{II}}) & \text{if } n > n_0, \end{cases} \tag{68}$$

and

$$\ell_n \triangleq \lfloor 2^{(1-\xi)(n-1)} \rfloor, \tag{69}$$

where $\xi \in (0, 1/2)$ is a yet-to-be-specified 'small' constant. The parameter ξ controls the rate penalty of adding guard bands, on one hand, and the probability of the decoder successfully removing the guard bands, on the other hand. We will require that $n_0 > 1$, so that the inequality

$$\ell_n > 2^{(n-1)(1-\xi)-1} \tag{70}$$

used later on will hold for all relevant n, i.e., for $n > n_0$. Note the above specifically implies that $\ell_n > 0$.

We now explain how the guard bands are removed, from the received word $\mathbf{Y}$, in order to produce the punctuated sequence Y^* defined in (62). Equivalently, we now show a procedure with the following outcome: for each block index $1 \le \phi < \Phi$,

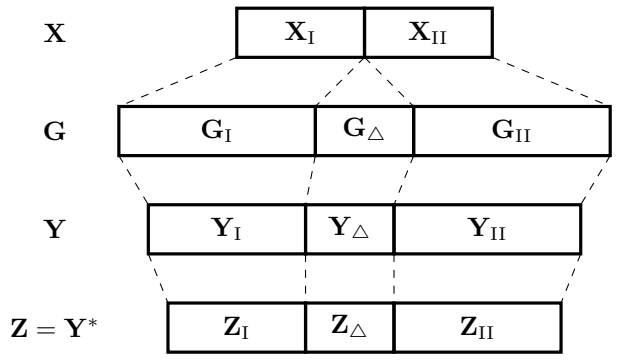

Fig. 3. The random variables $\mathbf{X}$, $\mathbf{G}$, $\mathbf{Y}$, and $\mathbf{Z}$.

we will produce the trimmed vector $\mathbf{Y}^*(\phi)$ corresponding to the block $\mathbf{X}(\phi)$. Before explaining how this is done, we first mention that our method has a small yet non-zero probability of failing. That is, there is a non-zero probability that our method will fail to produce Y^*. This probability will be analyzed at a later stage.

Our procedure for producing Y^* will have a preliminary step, and will then involve a recursion. The preliminary step is simple: we trim the received vector $\mathbf{Y}$ of leading and trailing zeros to produce $\mathbf{Y}^*$. We stress that, generally, $\mathbf{Y}^*$ does *not* equal the punctuated sequence Y^* defined in (62). In order to introduce notation required later on, let us now define the above operation more verbosely. Let $\mathbf{X}_{\mathrm{I}}$ and $\mathbf{X}_{\mathrm{II}}$ be the left and right halves of $\mathbf{X}$, see Figure 3. Thus, the transmitted word is $g(\mathbf{X}) = \mathbf{G}_{\mathrm{I}} \odot \mathbf{G}_{\triangle} \odot \mathbf{G}_{\mathrm{II}}$, where $\mathbf{G}_{\mathrm{I}} = g(\mathbf{X}_{\mathrm{I}})$, $\mathbf{G}_{\mathrm{II}} = g(\mathbf{X}_{\mathrm{II}})$, and $\mathbf{G}_{\triangle}$ is the middle guard band of length ℓ_n, where n is $\log_2$ of the length of $\mathbf{X}$. Clearly, $\mathbf{G}_{\mathrm{I}}$ and $\mathbf{G}_{\mathrm{II}}$ are of equal length. Denote the parts of $\mathbf{Y}$ corresponding to $\mathbf{G}_{\mathrm{I}}$, $\mathbf{G}_{\triangle}$ and $\mathbf{G}_{\mathrm{II}}$ by $\mathbf{Y}_{\mathrm{I}}$, $\mathbf{Y}_{\triangle}$, and $\mathbf{Y}_{\mathrm{II}}$, respectively. Note that at this stage, the decoder sees $\mathbf{Y}$, but can only make an informed guess as to what parts of $\mathbf{Y}$ constitute $\mathbf{Y}_{\mathrm{I}}$, $\mathbf{Y}_{\triangle}$, and $\mathbf{Y}_{\mathrm{II}}$. We remove from the received word $\mathbf{Y}$ all leading and trailing '0' symbols and denote the resulting vector $\mathbf{Z} = \mathbf{Y}^*$. We denote the parts of $\mathbf{Z}$ corresponding to $\mathbf{Y}_{\mathrm{I}}$, $\mathbf{Y}_{\triangle}$, and $\mathbf{Y}_{\mathrm{II}}$ by $\mathbf{Z}_{\mathrm{I}}$, $\mathbf{Z}_{\triangle}$, and $\mathbf{Z}_{\mathrm{II}}$, respectively. In order to build up the reader's intuition, we note that in a 'typical case', $\mathbf{Z}_{\mathrm{I}}$ is $\mathbf{Y}_{\mathrm{I}}$ after the leading zeros have been removed, $\mathbf{Z}_{\mathrm{II}}$ is $\mathbf{Y}_{\mathrm{II}}$ after the trailing zeros have been removed, and $\mathbf{Z}_{\triangle}$ is simply $\mathbf{Y}_{\triangle}$. As explained, the production of $\mathbf{Z}$ from $\mathbf{Y}$ constitutes the preliminary step of our method.

We will now specify how the punctuated vector Y^* is recursively produced from $\mathbf{Z}$. For the base case, note that if $\Phi = 1$, then Y^* is simply $\mathbf{Z}$. Our procedure hinges on the assumption that the middle index of $\mathbf{Z}$ originated from a guard band symbol. Specifically, we will assume that the middle index of $\mathbf{Z}$ (rounding down) belongs to $\mathbf{Z}_{\triangle}$. As explained, there is a probability of this assumption being false, and this will be analyzed at a later stage. For now, consider the case in which the assumption holds. In this case, the crucial observation is that $\mathbf{Y}_{\mathrm{I}}^*$ equals the first half of $\mathbf{Z}$, trimmed, while $\mathbf{Y}_{\mathrm{II}}^*$ equals the second half of $\mathbf{Z}$, trimmed. Namely, if ζ is the length of $\mathbf{Z}$, then

$$\mathbf{Y}_{\mathrm{I}}^* = (Z_1, Z_2, \ldots, Z_{\lfloor \zeta/2 \rfloor})^* \,, \tag{71}$$

$$\mathbf{Y}_{\mathrm{II}}^* = (Z_{\lfloor \zeta/2 \rfloor + 1}, Z_{\lfloor \zeta/2 \rfloor + 1}, \ldots, Z_{\zeta})^* \,, \tag{72}$$

since the guard band $\mathbf{Z}_{\triangle}$ has been 'trimmed out'. Thus, we have reduced our original problem of producing Y^* from $\mathbf{Y}^*$ into two equivalent problems, each half the size of the original: find the first half of Y^*, namely $\mathbf{Y}^*(1), \mathbf{Y}^*(2), \ldots, \mathbf{Y}^*(\Phi/2)$, from $\mathbf{Y}_{\mathrm{I}}^*$ and the second half of Y^* from $\mathbf{Y}_{\mathrm{II}}^*$. Thus, we continue recursively: we apply our method first to the RHS (71) and then to the RHS of (72). If, during all these recursive invocations, our assumptions on the middle index being part of the middle guard band were indeed correct, then we will have succeeded in producing Y^*. Note that the recursion depth is $n - n_0$.

There are two points that must be addressed. First, recall that adding guard bands makes the transmitted word longer. We must show that this has a vanishingly small effect on the rate of our scheme. Second, we must show that our scheme of producing Y^* from $\mathbf{Y}$ has a vanishingly small probability of failing. Once this is done, the proof of Theorem 1 will follow easily.

C. Auxiliary lemmas

In this section, we state and prove a number of lemmas key to the proof of Theorem 1.

In the sequel, we will choose a fixed $\nu \in (0, \frac{1}{3}]$ and set $n_0 = \lfloor \nu n \rfloor$. The parameter ν will trade-off reliability and decoding complexity (e.g., see Theorem 1). Recall that both ξ, the parameter through which ℓ_n is defined in (69), and ν are positive and fixed (not a function of n). Thus, the following lemma ensures that the rate penalty of adding guard bands is negligible as $n \to \infty$.

Lemma 22. *Let $\mathbf{x}$ be a vector of length $|\mathbf{x}| = 2^n$. Then,*

$$|\mathbf{x}| \le |g(\mathbf{x})| < \left(1 + \frac{2^{-(\xi \cdot n_0 + 1)}}{1 - 2^{-\xi}}\right) \cdot |\mathbf{x}| \,. \tag{73}$$

Proof: From the definition of $g(\mathbf{x})$, induction shows

$$|g(\mathbf{x})| = \begin{cases} 2^n & \text{if } n \le n_0 \\ 2^n + \sum_{t=n_0+1}^{n} 2^{n-t} \cdot \ell_t & \text{otherwise.} \end{cases} \tag{74}$$

Thus, the lower bound in (73) is trivial, since $|\mathbf{x}| = 2^n$, and every term in the sum in (74) is non-negative, by (69). The upper bound in (73) is trivially true for $n \le n_0$. For the case $n > n_0$, we have that

$$\begin{aligned} |g(\mathbf{x})|/|\mathbf{x}| &\overset{(a)}{=} 1 + \sum_{t=n_0+1}^{n} 2^{-t} \cdot \ell_t \\ &\overset{(b)}{\le} 1 + \sum_{t=n_0+1}^{n} 2^{-t} \cdot 2^{(1-\xi)\cdot(t-1)} \\ &= 1 + \sum_{t=n_0+1}^{n} 2^{-\xi\cdot(t-1)-1} \\ &< 1 + \sum_{t=n_0+1}^{\infty} 2^{-\xi\cdot(t-1)-1} \\ &\overset{(c)}{=} 1 + \frac{2^{-(\xi\cdot n_0+1)}}{1-2^{-\xi}} \,. \end{aligned}$$

where (a) follows from $|\mathbf{x}| = 2^n$ and (74); (b) follows from (69); (c) is simply the sum of geometric series. ∎

A key idea enabling the 'genie' described earlier is the recursive processing of each half of the received sequence. This processing will be successful if the middle symbol of the received sequence is a '0' originating from the outermost guard band, as per the recursive definition in (68). The following lemma shows that this is indeed the case, with very high probability.

Lemma 23. *Let the guard-band length ℓ_n in (69) use a fixed $\xi \in (0, 1/2)$. Fix the channel deletion probability δ and a regular hidden-Markov input distribution. Let $n > n_0 > 1$ and let $\mathbf{X}$ be a random vector of length $N = 2^n$ distributed according to the modified input distribution described above: i.i.d. blocks of length $N_0 = 2^{n_0}$, each distributed according to the specified input distribution. Denote by $\mathbf{Y}$ the result of transmitting $g(\mathbf{X})$ through the deletion channel. Then, there exists a constant $\theta > 0$, dependent only on the input distribution and the deletion probability such that, for n_0 large enough, the probability that the middle symbol of $\mathbf{Y}^*$ (rounding down) is not a '0' from the outer guard band of length ℓ_n is at most $2^{-\theta \cdot 2^{(1-2\xi)n_0}}$.*

Proof: Let $\mathbf{G} = g(\mathbf{X})$ (see Fig. 3). Recall that we denote the first and second halves of $\mathbf{X}$ by $\mathbf{X}_{\mathrm{I}}$ and $\mathbf{X}_{\mathrm{II}}$, respectively. Let $\mathbf{G}_{\mathrm{I}} = g(\mathbf{X}_{\mathrm{I}})$ and $\mathbf{G}_{\mathrm{II}} = g(\mathbf{X}_{\mathrm{II}})$, and denote by $\mathbf{G}_{\triangle}$ the guard band comprised of ℓ_n '0' symbols between $\mathbf{G}_{\mathrm{I}}$ and $\mathbf{G}_{\mathrm{II}}$. Hence, by (68),

$$\mathbf{G} = \mathbf{G}_{\mathrm{I}} \odot \mathbf{G}_{\triangle} \odot \mathbf{G}_{\mathrm{II}} \,.$$

Denote by $\mathbf{Y}$ the (untrimmed) result of passing $\mathbf{G}$ through the deletion channel. Let $\mathbf{Y}_{\mathrm{I}}$, $\mathbf{Y}_{\mathrm{II}}$, and $\mathbf{Y}_{\triangle}$ be the parts of $\mathbf{Y}$ corresponding to $\mathbf{G}_{\mathrm{I}}$, $\mathbf{G}_{\mathrm{II}}$, and $\mathbf{G}_{\triangle}$, respectively. Let $\mathbf{Z} = \mathbf{Y}^*$ be the trimmed $\mathbf{Y}$. Define $\mathbf{Z}_{\mathrm{I}}$, $\mathbf{Z}_{\mathrm{II}}$, and $\mathbf{Z}_{\triangle}$, as the parts of $\mathbf{Z}$ corresponding to $\mathbf{G}_{\mathrm{I}}$, $\mathbf{G}_{\mathrm{II}}$, and $\mathbf{G}_{\triangle}$, respectively.

For $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_t)$ with $t \geq 1$, the middle index of $\mathbf{Z}$ (rounding down) is $s = \lfloor (t+1)/2 \rfloor$. A sufficient condition for Z_s belonging to $\mathbf{Z}_{\triangle}$ is

$$|\mathbf{Z}_{\mathrm{I}}| < |\mathbf{Z}_{\triangle}| + |\mathbf{Z}_{\mathrm{II}}| \,, \quad |\mathbf{Z}_{\mathrm{II}}| < |\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}| \,. \tag{75}$$

To see that this is sufficient, we observe that $|\mathbf{Z}_{\mathrm{I}}| < |\mathbf{Z}_{\triangle}| + |\mathbf{Z}_{\mathrm{II}}|$ implies that the middle index does not fall in $\mathbf{Z}_{\mathrm{I}}$ because then

$$\begin{aligned} \lfloor (|\mathbf{Z}|+1)/2 \rfloor &= \lfloor (|\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}| + |\mathbf{Z}_{\mathrm{II}}| + 1)/2 \rfloor \\ &\geq \lfloor (|\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\mathrm{I}}| + 2)/2 \rfloor = |\mathbf{Z}_{\mathrm{I}}| + 1. \end{aligned}$$

Similarly, if $|\mathbf{Z}_{\mathrm{II}}| < |\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}|$, then the middle index does not fall in $\mathbf{Z}_{\mathrm{II}}$ because then

$$\begin{aligned} \lfloor (|\mathbf{Z}|+1)/2 \rfloor &= \lfloor (|\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}| + |\mathbf{Z}_{\mathrm{II}}| + 1)/2 \rfloor \\ &\leq \lfloor (|\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}| + |\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}|)/2 \rfloor = |\mathbf{Z}_{\mathrm{I}}| + |\mathbf{Z}_{\triangle}|. \end{aligned}$$

Now, we will analyze the probability of (75). Denote by α, β, and γ the following length differences between the three parts of $\mathbf{G}$ and the three corresponding parts of $\mathbf{Y}$,

$$\begin{aligned} \alpha &= |\mathbf{G}_{\mathrm{I}}| - |\mathbf{Y}_{\mathrm{I}}| \,, \\ \beta &= |\mathbf{G}_{\triangle}| - |\mathbf{Y}_{\triangle}| \,, \\ \gamma &= |\mathbf{G}_{\mathrm{II}}| - |\mathbf{Y}_{\mathrm{II}}| \,. \end{aligned}$$

Also, denote by α', β', and γ' the length differences resulting from trimming,

$$\begin{aligned} \alpha' &= |\mathbf{Y}_{\mathrm{I}}| - |\mathbf{Z}_{\mathrm{I}}| \,, \\ \beta' &= |\mathbf{Y}_{\triangle}| - |\mathbf{Z}_{\triangle}| \,, \\ \gamma' &= |\mathbf{Y}_{\mathrm{II}}| - |\mathbf{Z}_{\mathrm{II}}| \,. \end{aligned}$$

Suppose that the trimming on both sides stopped short of the guard band. In this case, $\beta' = 0$. Since $|\mathbf{G}_{\mathrm{I}}| = |\mathbf{G}_{\mathrm{II}}|$ and $|\mathbf{G}_{\triangle}| = \ell_n$, condition (75) would reduce to

$$\alpha + \alpha' < \gamma + \gamma' + \ell_n - \beta \,, \tag{76}$$

$$\gamma + \gamma' < \alpha + \alpha' + \ell_n - \beta \,. \tag{77}$$

Our aim is to show that, with very high probability, both (76) and (77) hold, as well as the assumption leading to their formulation.

Recall that δ is the channel deletion probability and let

$$\hat{\ell} = \ell_n \cdot (1-\delta)/2 \,. \tag{78}$$

We define the following 'good' events on the random variables α, α', β, β', γ, and γ:

$$A \;:\; \delta|\mathbf{G}_{\mathrm{I}}| - \hat{\ell}/4 < \alpha < \delta|\mathbf{G}_{\mathrm{I}}| + \hat{\ell}/4 \tag{79}$$

$$A' \;:\; 0 \leq \alpha' < \hat{\ell}/4 \tag{80}$$

$$B \;:\; 0 \leq \beta < \delta \cdot \ell_n + \hat{\ell} \tag{81}$$

$$B' \;:\; \beta' = 0 \tag{82}$$

$$C \;:\; \delta|\mathbf{G}_{\mathrm{II}}| - \hat{\ell}/4 < \gamma < \delta|\mathbf{G}_{\mathrm{II}}| + \hat{\ell}/4 \tag{83}$$

$$C' \;:\; 0 \leq \gamma' < \hat{\ell}/4 \tag{84}$$

First, we note that the total number of symbols deleted or trimmed from $\mathbf{G}_{\mathrm{I}}$ is given by $|\mathbf{G}_{\mathrm{I}}| - |\mathbf{Z}_{\mathrm{I}}| = \alpha + \alpha'$. If A and A' hold, then this is bounded by

$$\begin{aligned} \alpha + \alpha' &< \delta|\mathbf{G}_{\mathrm{I}}| + \hat{\ell}/4 + \hat{\ell}/4 \\ &= \delta|\mathbf{G}_{\mathrm{I}}| + \hat{\ell}/2 \,. \end{aligned} \tag{85}$$

By (73), $|\mathbf{G}_{\mathrm{I}}| = 2^{n-1} + t$, where $t \geq 0$. We now show that if A and A' hold, then $\alpha + \alpha' < |\mathbf{G}_{\mathrm{I}}|$. Indeed, by (69) and (78),

$$\begin{aligned} \delta|\mathbf{G}_{\mathrm{I}}| + \hat{\ell}/2 &< \delta|\mathbf{G}_{\mathrm{I}}| + \hat{\ell} \\ &= \delta(2^{n-1} + t) + 2^{-1}(1-\delta)\lfloor 2^{(1-\xi)(n-1)} \rfloor \\ &< \delta(2^{n-1} + t) + (1-\delta)2^{n-2} \\ &= \delta 2^{n-1} + (1-\delta)2^{n-2} + \delta t \\ &< 2^{n-1} + \delta t \\ &< 2^{n-1} + t = |\mathbf{G}_{\mathrm{I}}| \,. \end{aligned}$$

The analogous claim also holds for C, C', and $\mathbf{G}_{\mathrm{II}}$. Thus, if A, A', C, and C' hold, then some parts of $\mathbf{G}_{\mathrm{I}}$ and $\mathbf{G}_{\mathrm{II}}$ must remain in $\mathbf{Z}_{\mathrm{I}}$ and $\mathbf{Z}_{\mathrm{II}}$ after deletion and trimming. Hence, the trimming has stopped short of the guard band, which implies B'.

If, in addition, B occurs, then both (76) and (77) must also hold. To verify that (76) holds, note that

$$\begin{aligned} \gamma + \gamma' + \ell_n - \beta &\overset{(a)}{>} \delta|\mathbf{G}_{\mathrm{II}}| - \hat{\ell}/4 + \ell_n - \delta \cdot \ell_n - \hat{\ell} \\ &= \delta|\mathbf{G}_{\mathrm{II}}| - \hat{\ell}/4 + (1-\delta)\ell_n - \hat{\ell} \end{aligned}$$

$$\begin{aligned}&\overset{(b)}{=} \delta|\mathbf{G}_{\rm II}| - \hat{\ell}/4 + 2\hat{\ell} - \hat{\ell} \\ &= \delta|\mathbf{G}_{\rm II}| + 3\hat{\ell}/4 \\ &\overset{(c)}{>} \delta|\mathbf{G}_{\rm II}| + \hat{\ell}/2\,,\end{aligned}$$

where (a) follows from (82), (83), and (84); (b) follows from (78); (c) follows since ℓ_n is positive, by (70), and thus so is $\hat{\ell}$, by (78). Next, observe that $|\mathbf{G}_{\rm I}| = |\mathbf{G}_{\rm II}|$, and apply (85). The proof of (77) is the same except that the upper and lower bounds are swapped for $\alpha + \alpha'$ and $\gamma + \gamma'$.

To recap, the occurrence of all the 'good' events in (79)–(84) implies that the middle index falls inside $\mathbf{Z}_{\triangle}$. Hence, the next step is to show that each of the above events occurs with very high probability, if n is large enough.

We now recall Hoeffding's bound [31, Theorem 2] [32, proof of Lemma 4.13] and apply it to the deletion channel with deletion probability δ. Namely, let D be a random variable equal to the number of deletions after N channel uses. Hence, $E[D] = \delta N$, and for $t \geq 0$ we have by Hoeffding's bound that

$$\Pr(D \geq \delta N + t) \leq e^{-2t^2/N}\,, \tag{86}$$

$$\Pr(D \leq \delta N - t) \leq e^{-2t^2/N}\,. \tag{87}$$

Recalling that $\xi > 0$, we now require that n_0 be large enough that the bracketed term in (73) is at most 2. That is, we assume that n_0 is large enough such that, for $n > n_0$, we have

$$|\mathbf{G}_{\rm I}| \leq 2 \cdot 2^{n-1}\,. \tag{88}$$

Applying both (86) and (87), we deduce that, for $n > n_0$, we have

$$\begin{aligned}1 - \Pr(A) &\leq 2e^{-2(\hat{\ell}/4)^2/|\mathbf{G}_{\rm I}|} \\ &= 2e^{-2(\ell_n(1-\delta)/8)^2/|\mathbf{G}_{\rm I}|} \\ &\overset{(a)}{<} 2e^{-2(2^{(n-1)\cdot(1-\xi)-1}(1-\delta)/8)^2/|\mathbf{G}_{\rm I}|} \\ &\overset{(b)}{\leq} 2e^{-2(2^{(n-1)\cdot(1-\xi)-1}(1-\delta)/8)^2/(2\cdot 2^{n-1})} \\ &= 2e^{-\left(\frac{(1-\delta)^2}{256}\right)\cdot 2^{(n-1)(1-2\xi)}} \\ &\overset{(c)}{\leq} 2e^{-\left(\frac{(1-\delta)^2}{256}\right)\cdot 2^{n_0\cdot(1-2\xi)}}\,,\end{aligned} \tag{89}$$

where (a) follows from (70); (b) holds by (88); and (c) follows from $n > n_0$. Exactly the same bound applies to $1 - \Pr(C)$. For $\Pr(B)$, we again use (86) to deduce that

$$\begin{aligned}1 - \Pr(B) &\leq e^{-2\hat{\ell}^2/\ell_n} \\ &\overset{(a)}{=} e^{-2\left(\frac{\ell_n(1-\delta)}{2}\right)^2/\ell_n} \\ &= e^{-2\left(\frac{(1-\delta)}{2}\right)^2\cdot\ell_n} \\ &\overset{(b)}{<} e^{-2\left(\frac{(1-\delta)}{2}\right)^2\cdot 2^{(n-1)(1-\xi)-1}} \\ &= e^{-\left(\frac{(1-\delta)^2}{4}\right)\cdot 2^{(n-1)(1-\xi)}} \\ &\overset{(c)}{\leq} e^{-\left(\frac{(1-\delta)^2}{4}\right)\cdot 2^{n_0\cdot(1-\xi)}}\,,\end{aligned} \tag{90}$$

where (a) follows from (78); (b) follows from (70); and (c) holds because $n > n_0$.

We now bound $1 - \Pr(A' \cap C')$ from above. Consider $\mathbf{G}_{\rm I}$ and $\mathbf{Y}_{\rm I}$ first. Next, recall that by the recursive definition of g in (68), the prefix of length $N_0 = 2^{n_0}$ of $\mathbf{G}_{\rm I}$ is distributed according to the underlying regular Markov input distribution (it does not contain a guard band). Denote this prefix as $X_1, X_2, \ldots, X_{N_0}$, and denote the state of the process at time 0 as S_0. Since our input distribution is not degenerate, there exists an integer $\tau > 0$ and a probability $0 < p < 1$ such that for any $s \in \mathcal{S}$,

$$\Pr\left((X_1, X_2, \ldots, X_\tau) = (0, 0, \ldots, 0) | S_0 = s\right) < p\,. \tag{91}$$

Let

$$\tilde{\ell} = \ell_{n_0+1} \cdot (1-\delta)/2\,. \tag{92}$$

Since $n > n_0$, we have by (69) and (78) that $\tilde{\ell} \leq \hat{\ell}$ and that

$$\tilde{\ell}/4 < 2^{n_0}\,.$$

Let

$$\rho = \tau \cdot \left\lfloor \frac{\tilde{\ell}/4}{\tau} \right\rfloor\,,$$

and partition $X_1, X_2, \ldots X_\rho$ into consecutive segments of length τ. Then, we define event A'' to occur if there exists a segment that is not an all-zero vector of length τ, and its first non-zero entry has not been deleted. We define C'' as the analogous event, with respect to $\mathbf{G}_{\rm II}$ and $\mathbf{Y}_{\rm II}$, the only difference being that we are now considering the length ρ suffix of $\mathbf{X}_{\rm II}$, and considering the last non-zero entry of a segment. By construction, if A'' and C'' hold, then A' and C' must hold. That is, if event A'' occurs, then the number of symbols trimmed from the left of $\mathbf{G}_{\rm I}$ is strictly less than $\tilde{\ell}/4$, since the above non-zero non-deleted symbol is not trimmed, and this assures that the "trimming from the left" stops before it. A similar claim holds with respect to C''. Thus, $1 - \Pr(A' \cap C') \leq 1 - \Pr(A'' \cap C'')$.

Since (91) holds for all $s \in \mathcal{S}$, we have by the Markov property that

$$1 - \Pr(A'') < \left(1 - (1-p)(1-\delta)\right)^{\rho/\tau}\,. \tag{93}$$

Indeed, if A'' does not hold, this means that we have "failed" on each of the ρ/τ blocks, in the sense that each such block was either all-zero, or its first non-zero symbol was deleted. Since the probability of "success" conditioned on any given string of past failures is always greater than $(1-p)(1-\delta)$, the above follows.

Define

$$\zeta = -\log_e\left(1 - (1-p)(1-\delta)\right)\,,$$

and note that $\zeta > 0$. Next, we bound ρ as

$$\begin{aligned}\rho &> \tilde{\ell}/4 - \tau \\ &= \ell_{n_0+1} \cdot (1-\delta)/8 - \tau \\ &> \left(2^{(1-\xi)\cdot n_0 - 1}\right) \cdot (1-\delta)/8 - \tau,\end{aligned}$$

where the second inequality follows from (70). Thus,

$$1 - \Pr(A'') < e^{-\frac{\zeta}{\tau}\left(\left(2^{(1-\xi)\cdot n_0 - 1}\right)\cdot(1-\delta)/8 - \tau\right)}\,.$$

Of course, exactly the same bound holds for $1 - \Pr(C'')$. Hence, by the union bound, and recalling that $A'' \cap C''$ implies $A' \cap C'$, we have that

$$1 - \Pr(A' \cap C') < 2e^{-\frac{\zeta}{\tau}\left(\left(2^{(1-\xi)\cdot n_0 - 1}\right)\cdot(1-\delta)/8 - \tau\right)}\,. \tag{94}$$

Putting (89), (90), and (94) together, and applying the union bound proves the lemma. ∎

We conclude this section with the proof of our main theorem. Note that both the encoding and decoding schemes are specified in the proof.

Proof of Theorem 1: Our proof is divided into two parts. In the first part, we consider the 'idealized' random vectors $\mathbf{X}$ and $\mathbf{Y}$. That is, $\mathbf{X}$ is drawn from the probability distribution defined in Lemma 23 (there is no encoding of date) and $\mathbf{Y}$ is the result of transmitting $g(\mathbf{X})$ through our deletion channel. We will show that by previously proven lemmas, the rate penalty of expanding $\mathbf{X}$ to $g(\mathbf{X})$ is negligible and the probability of deducing Y^* from $\mathbf{Y}$ is very high. We conclude the first part by discussing the polarization of $\mathbf{U} = \mathcal{A}(\mathbf{X})$.

In the second part of the proof, we consider the actual case at hand. That is, we show how encoding and decoding are carried out, discuss the encoding and decoding complexity, prove that the rate of our coding scheme approaches the information rate $\mathcal{I}$, and prove that the probability of misdecoding tends to 0.

Recall that $0 < \nu' < \nu \leq 1/3$ are fixed parameters. We let

$$n_0 = \lfloor \nu n \rfloor \tag{95}$$

and

$$\nu'' = \frac{\nu + \nu'}{2} \,, \tag{96}$$

implying that

$$0 < \nu' < \nu'' < \nu \leq \frac{1}{3} \,. \tag{97}$$

Then, set ξ for the guard-band length ℓ_n defined in (69) to

$$\xi = \frac{1 - \frac{1+\nu''/\nu}{2}}{2} = \frac{1 - \nu''/\nu}{4} \,. \tag{98}$$

Note that by (60),

$$n_1 = n - \lfloor \nu n \rfloor = \lceil (1-\nu) n \rceil \,. \tag{99}$$

We start with the first part of the proof: let $\mathbf{X}$ and $\mathbf{Y}$ be defined as in Lemma 23 (as yet, no coding of information).

Sub-claim 1. *The rate penalty incurred by adding guard bands becomes negligible as $n \to \infty$. Namely, $|g(\mathbf{X})|/|\mathbf{X}|$ tends to 1 as $n \to \infty$.*

This follows by Lemma 22, which shows that the rate penalty incurred by adding guard bands becomes negligible as $n_0 \to \infty$, and the connection between n_0 and n given in (95).

Sub-claim 2. *The probability of making a mistake during the partitioning of $\mathbf{Y}$ into the $\Phi = 2^{n-n_0}$ trimmed blocks $\mathbf{Y}(1)^*$, $\mathbf{Y}(2)^*$,…,$\mathbf{Y}(\Phi)^*$ is less than $\frac{1}{3} \cdot 2^{-2^{\nu'' n}}$, for $N = 2^n$ large enough.*

This follows from Lemma 23 and the union bound. Specifically, recalling the recursive nature of our algorithm to produce Y^*, we note that an error is made only if the relevant portion of the received vector $\mathbf{Y}$, after that portion has been trimmed, is such that the middle symbol (rounding down) does not belong to the outermost guard band. Each such probability can be bounded by using Lemma 23. Since we produce Φ blocks, our recursion is applied $\Phi - 1$ times. Hence, for n_0 large enough, the probability of failing to produce Y^* is at most

$$\begin{aligned}(\Phi - 1) \cdot 2^{-\theta \cdot 2^{(1-2\xi)n_0}} \\ = (2^{n - \lfloor \nu n \rfloor} - 1) \cdot 2^{-\theta \cdot 2^{\lfloor \nu n \rfloor \cdot ((1+\nu''/\nu)/2)}} \,,\end{aligned} \tag{100}$$

where the equality follows from (58) and (95)–(99). Recalling (95), we may take n large enough such that n_0 is indeed large enough for the above to hold. Moreover, since $0 < \nu'' < \nu$, it is straightforward to show that the RHS of (100) is less than $\frac{1}{3} \cdot 2^{-2^{\nu'' n}}$ for large enough n, as required.

Sub-claim 3. *For $\mathbf{U} = \mathcal{A}(\mathbf{X})$, the fraction of indices $1 \leq i \leq N$ for which the Bhattacharyya parameter satisfies*

$$Z(U_i | U_1^{i-1}, \mathbf{Y}(1)^*, \mathbf{Y}(2)^*, \ldots, \mathbf{Y}(\Phi)^*) < \frac{1}{3N} \cdot 2^{-2^{\nu'' n}} \tag{101}$$

and the total variation parameter (see Definition 8 in the appendix) satisfies

$$K(U_i | U_1^{i-1}) < \frac{1}{3N} \cdot 2^{-2^{\nu'' n}} \tag{102}$$

tends to $\mathcal{I}$, as $n \to \infty$.

Informally, $H \approx 0$ iff $Z \approx 0$ and $H \approx 1$ iff $K \approx 0$. For a formal statement, see e.g. [21, Lemma 1]. Thus, Lemma 21 continues to hold if we replace (65) by the condition

$$\begin{aligned}Z(V_{i_0}(\phi) | V_1^{i_0-1}(\phi), \mathbf{Y}^*(\phi)) < \epsilon \quad \text{and} \\ K(V_{i_0}(\phi) | V_1^{i_0-1}(\phi)) < \epsilon \,.\end{aligned} \tag{103}$$

That is, at the end of n_0 polarization stages, the fraction of indices $1 \leq i_0 \leq N_0$ satisfying the 'weak polarization' in (103) tends to $\mathcal{I}$ for any $\epsilon > 0$. To get from the 'weak polarization' implied by (103) to the 'strong polarization' implied by (101) and (102), we employ [30, Lemma 40], as follows.

For $\mathbf{b} = (b_1, b_2, \ldots, b_n)$, recall from (4) the definition of $i(\mathbf{b})$, and denote

$$i_0(\mathbf{b}) \triangleq 1 + \sum_{j=1}^{n_0} b_j 2^{n_0 - j} \,.$$

Thus, we may think of the random process by which $i(B_1, B_2, \ldots, B_n)$ is chosen as first selecting i_0, which is in fact a function of $B_1, B_2, \ldots, B_{n_0}$, and then completing the choice of i according to a new process $\tilde{B}_1, \tilde{B}_2, \ldots, \tilde{B}_{n_1}$, where

$$\tilde{B}_1 = B_{n_0+1}, \tilde{B}_2 = B_{n_0+2}, \ldots, \tilde{B}_{n_1} = B_{n_0+n_1} \,, \tag{104}$$

recalling that $n_0 + n_1 = n$, by (95) and (99).

Fix $\epsilon > 0$ to a value that will shortly be specified. Next, for now, let us fix an index i_0 for which (103) holds. We define two processes related to (104), denoted $\tilde{Z}_1, \tilde{Z}_2, \ldots, \tilde{Z}_{n_1}$ and $\tilde{K}_1, \tilde{K}_2, \ldots, \tilde{K}_{n_1}$. Recall that by definition, the $(\mathbf{X}(\phi), \mathbf{Y}(\phi))$ are i.i.d. over $1 \leq \phi \leq \Phi$. Hence, this must also be the case for $(V_{i_0}(\phi), V_1^{i_0-1}(\phi), \mathbf{Y}^*(\phi))$, by (63). The first process is the evolution of the conditional Bhattacharyya parameter as we apply the n_1 polar transforms implied by (104), to $(\tilde{X}_\phi, \tilde{Y}_\phi)_{\phi=1}^{\Phi}$, where

$$\tilde{X}_\phi = V_{i_0}(\phi) \;\text{ and }\; \tilde{Y}_\phi = (V_1^{i_0-1}(\phi), \mathbf{Y}^*(\phi)) \,.$$

The second process is defined similarly, but now we consider the evolution of the conditional total variation parameter as we apply n_1 polar transforms to $(\tilde{X}_\phi, \tilde{\tilde{Y}}_\phi)_{\phi=1}^{\Phi}$, where

$$\tilde{\tilde{Y}}_\phi = V_1^{i_0-1}(\phi) \ .$$

By our assumption of i_0 satisfying (103),

$$\tilde{Z}_1 = Z(\tilde{X}_1|\tilde{Y}_1) < \epsilon \ \text{ and } \ \tilde{K}_1 = K(\tilde{X}_1|\tilde{\tilde{Y}}_1) < \epsilon \ .$$

Since $(\tilde{X}_\phi, \tilde{Y}_\phi)$ are i.i.d. over ϕ, and the same holds for $(\tilde{X}_\phi, \tilde{\tilde{Y}}_\phi)$, we have by [24, Proposition 5] that

$$\tilde{Z}_{t+1} \leq \begin{cases} 2\tilde{Z}_t & \text{if } \tilde{B}_t = 0 \\ \tilde{Z}_t^2 & \text{if } \tilde{B}_t = 1 \end{cases}$$

and by [21, Proposition 4] that

$$\tilde{K}_{t+1} \leq \begin{cases} \tilde{K}_t^2 & \text{if } \tilde{B}_t = 0 \\ 2\tilde{K}_t & \text{if } \tilde{B}_t = 1. \end{cases}$$

Lastly, it follows from (66) that $\tilde{Z}_{n_1}$ equals the LHS of (101) while $\tilde{K}_{n_1}$ equals the LHS of (102), where i is defined in (4), with B_j instead of b_j.

To prove the sub-claim, we must show that, for every $\xi > 0$, there exists a threshold such that, if n is larger than the threshold, then the fraction of indices i satisfying both (101) and (102) is at least $\mathcal{I}-\xi$. We will do this by choosing an ϵ and n_0 such that the fraction of indices satisfying (103) is at least $\mathcal{I} - \xi/3$. Of these weakly polarized indices, we will choose n_1 such that at least a fraction $1-2\xi/3$ satisfy both (101) and (102). This is sufficient because $(\mathcal{I}-\xi/3)(1-2\xi/3) \geq \mathcal{I}-\xi$. To make a proper argument, however, we will work in reverse.

First, we will set the parameters for strong polarization assuming sufficient weak polarization. In particular, we define

$$\beta = 3(\nu + \nu'')/4 \tag{105}$$

and observe that (97) implies $0 < \beta < 1/2$. Then, we let $\psi = \xi/3$ be the maximum fraction of weakly polarized indices that can fail to strongly polarize and apply [30, Lemma 40] to determine a valid maximum for ϵ and minimum for n_1 (in [30], ψ, ϵ, and n_1 are denoted δ, η, and n, respectively). This lemma implies the existence of an $\epsilon > 0$ such that if (103) holds for an index i_0, then the fraction of i values $((i_0-1)\cdot\Phi + 1 \leq i \leq i_0 \cdot \Phi)$ for which both $\tilde{Z}_i < 2^{-2^{\beta n_1}}$ and $\tilde{K}_i < 2^{-2^{\beta n_1}}$ is at least $1-2\xi/3$, for all n_1 large enough[10]. Conceptually, we need to apply the lemma twice – once for (101) and once for (102). Thus, the fraction of weakly polarized indices that fail to satisfy both (101) and (102) is at most $2\psi = 2\xi/3$.

Next, for the ϵ determined above, we find the minimum n_0 to guarantee that (103) holds for at least a fraction $\mathcal{I}-\xi/3$ of the i_0 indices. Lastly, we recall that n_0 and n_1 are monotonically increasing functions of n, by (95) and (99). Hence, for all large enough n, the parameters n_0 and n_1 will exceed the bounds computed earlier and the fraction of indices satisfying (101) and (102), where in both cases we replace the RHS by $2^{-2^{\beta n_1}}$, is at least $\mathcal{I}-\xi$.

[10]Crucially, ϵ and the n_1 threshold do not depend on the choice of i_0.

In order to prove the sub-claim, all that remains is to show that, for all large enough n, we have

$$2^{-2^{\beta n_1}} < \frac{1}{3N} \cdot 2^{-2^{\nu'' n}} \ , \tag{106}$$

the latter term being RHS of (101) and (102). Indeed, by (99) we have that $n_1 \geq (1-\nu)n$, and recalling from (97) that $\nu \leq 1/3$, we deduce that $n_1 \geq 2n/3$. Hence, to prove (106), it suffices to show that

$$2^{-2^{2\beta n/3}} < \frac{1}{3N} \cdot 2^{-2^{\nu'' n}} \ . \tag{107}$$

Indeed, by (97) and (105) we have that $2\beta/3 > \nu''$. Thus, recalling that $N = 2^n$, we deduce that (107) holds for all n large enough.

We now move to the second part of our proof. Let us first discuss how data is encoded. We produce $\mathbf{u} = u_1^N$ successively, starting from u_1 and ending in u_N. If the current index i satisfies (101) and (102), then u_i is set to an information bit, where the information bits are assumed i.i.d. and Bernoulli$(1/2)$. Otherwise, u_i is randomly picked according to the distribution $P(U_i = u_i|U_1^{i-1} = u_1^{i-1})$, where u_1^{i-1} are the realizations occurring in previous stages. The random picks in this case are assumed to be from a random source common to both the encoder and the decoder. Typically, this is implemented using a pseudo-random number generator, common to both sides: if the pseudo-random number $0 \leq r_i \leq 1$ drawn for this stage is such that $P(U_i = 0|U_1^{i-1} = u_1^{i-1}) \leq r_i$, we set $u_i = 0$. Otherwise, we set $u_i = 1$. These are essentially the 'frozen-bits' from the seminal paper [24]. Transforming $\mathbf{u}$ to $\mathbf{x} = \mathcal{A}_n^{-1}(\mathbf{u})$ and adding guard bands to $\mathbf{x}$ is as described before.

The following sub-claim proves a key part of our theorem and is an immediate consequence of Subclaims 1 and 3.

Sub-claim 4. *The rate of our coding scheme approaches $\mathcal{I}$, as $n \to \infty$.*

Note that the probability distribution of our encoded $\mathbf{u}$ does *not* generally equal that of the random variable $\mathbf{U}$ used throughout this paper. Namely, denote by $\tilde{p}$ the probability distribution corresponding to the above encoding process: the probability of the encoder producing the vector $\mathbf{u}$ is $\tilde{p}(\mathbf{u})$. Next, denote by p the probability distribution of $\mathbf{U}$. That is, the probability we would get if we were to set u_i to 0 with probability $P(U_i = 0|U_1^{i-1} = u_1^{i-1})$, irrespective of whether i satisfies (101) and (102) or not. Our plan is to show that the difference between p and $\tilde{p}$ is 'small'. However, we must first address a subtle point stemming from this difference in distributions. Specifically, the probability $P(U_i = 0|U_1^{i-1} = u_1^{i-1})$ used at stage i might be undefined, since we might be conditioning on an event with probability 0. In this case, we define the above probability to be $1/2$.

We decode as previously explained: we first recursively partition the received vector into $\mathbf{y}(1)^*, \mathbf{y}(2)^*, \ldots, \mathbf{y}(\Phi)^*$. Then, we employ successive cancellation decoding. That is, we produce our estimate $\hat{\mathbf{u}} = \hat{u}_1^N$ of $\mathbf{u}$ by first producing $\hat{u}_1$, then $\hat{u}_2$, etc., up to $\hat{u}_N$. If index i is such that both (101) and (102) hold, then we set $\hat{u}_i$ to the value maximizing

$$P(U_i = \hat{u}_i | U_1^{i-1} = \hat{u}_1^{i-1}, \mathbf{Y}(1)^* = \mathbf{y}(1)^*, \mathbf{Y}(2)^* = \mathbf{y}(2)^*, \ldots, \mathbf{Y}(\Phi)^* = \mathbf{y}(\Phi)^*) \ . \quad (108)$$

Otherwise, if i does not satisfy both (101) and (102), we set $\hat{u}_i$ is accordance with the common randomness. That is, in the pseudo-random number implementation, we set $\hat{u}_i = 0$ if

$$P(U_i = 0 | U_1^{i-1} = \hat{u}_1^{i-1}) \leq r_i \ . \quad (109)$$

Otherwise, we set $\hat{u}_i = 1$.

We stress that the probabilities in (108) and (109) are calculated according to the probability distribution of the random vector $\mathbf{U}$ used throughout this paper. That is, although $\mathbf{u}$ has been encoded according to the probability $\tilde{p}$, we decode it 'as if' it had been encoded using p. This discrepancy will shortly be addressed. However, as a first step, the following sub-claim considers the case in which there is no discrepancy.

Sub-claim 5. *If $\mathbf{u}$ were chosen according to the probability distribution p, then the probability of misdecoding would be less than $\frac{2}{3} \cdot 2^{-2^{\nu'' n}}$, for large enough n.*

To see this, note that if the above were the case, then $\mathbf{u}$ and $\mathbf{U}$ would have the same probability distribution. Thus, Subclaim 2 would apply, and would imply that the probability of our partitioning algorithm failing to produce the correct $\mathbf{y}(1)^*, \mathbf{y}(2)^*, \ldots, \mathbf{y}(\Phi)^*$ from the received vector would be less than $\frac{1}{3} \cdot 2^{-2^{\nu'' n}}$, for large enough n. Also, if a 'genie' were to give us the correct $\mathbf{y}(1)^*, \mathbf{y}(2)^*, \ldots, \mathbf{y}(\Phi)^*$, we have from (101) that the probability of misdecoding $\mathbf{u}$ would be less than $\frac{1}{3} \cdot 2^{-2^{\nu'' n}}$ for large enough n, using exactly[11] the same arguments as given in [24, Proof of Theorem 2] to bound the probability of the successive cancellation decoder failing. The result follows by applying the union bound.

For $\mathbf{u}$ such that $p(\mathbf{u}) > 0$, denote by $P_{\mathrm{e}}(\mathbf{u})$ the probability that our decoder fails, given that $\mathbf{u}$ was encoded. Otherwise, if $p(\mathbf{u}) = 0$, define[12] $P_{\mathrm{e}}(\mathbf{u}) = 1$. We have just shown that for large enough n,

$$\sum_{\mathbf{u} \in \mathcal{X}^N} p(\mathbf{u}) P_{\mathrm{e}}(\mathbf{u}) < \frac{2}{3} \cdot 2^{-2^{\nu'' n}} \ . \quad (110)$$

However, recall that our ultimate goal is to upper bound the LHS, after $p(\mathbf{u})$ is replaced by $\tilde{p}(\mathbf{u})$. Informally, a similar bound holds for this case as well, since p and $\tilde{p}$ are 'close'. The two following sub-claims makes this statement precise.

Sub-claim 6.

$$\sum_{\mathbf{u} \in \mathcal{X}^N} |\tilde{p}(\mathbf{u}) - p(\mathbf{u})| < \frac{1}{3} \cdot 2^{-2^{\nu'' n}}$$

[11] Since [24] considers the Bhattacharyya parameter for the case of a channel with uniform input, we also need to claim that our Z upper bounds the probability of maximum-aposteriori misdecoding in the more general setting where the channel input is non-uniform. This is well known, see e.g. [21, Remark 1] for a proof of a slightly stronger claim.

[12] Note that we are being conservative. We could have simply defined $P_{\mathrm{e}}(\mathbf{u})$ as the probability that our decoder fails, given that $\mathbf{u}$ was encoded. However, if our input distribution is such that some vectors $\mathbf{u}$ are given a probability of 0, say in order to satisfy a constraint on the input, we should treat the event of the encoder producing a $\mathbf{u}$ not satisfying this constraint as an error.

To see this, we use the following result from [33, Lemma 3.5]:

$$A_1^N - B_1^N = \sum_{i=1}^{N} B_1^{i-1} (A_i - B_i) A_{i+1}^N$$

where, here, A_i^j denotes the product $A_i^j = A_i \cdot A_{i+1} \cdots A_j$, and $A_1^0 = A_{N+1}^N \triangleq 1$. We now take

$$A_i = A_i(\mathbf{u}) = \tilde{p}(u_i | u_1^{i-1}) \quad \text{and} \quad B_i = B_i(\mathbf{u}) = p(u_i | u_1^{i-1}) \ .$$

Recall that we have defined B_i to be $1/2$ if $p(u_1^{i-1}) = 0$. Similarly, we define A_i to be $1/2$ if $\tilde{p}(u_1^{i-1}) = 0$. We deduce that

$$\begin{aligned}
&\sum_{\mathbf{u} \in \mathcal{X}^N} |\tilde{p}(\mathbf{u}) - p(\mathbf{u})| \\
&= \sum_{\mathbf{u} \in \mathcal{X}^N} |A_1^N - B_1^N| \\
&= \sum_{\mathbf{u} \in \mathcal{X}^N} \left| \sum_{i=1}^{N} B_1^{i-1} (A_i - B_i) A_{i+1}^N \right| \\
&\leq \sum_{\mathbf{u} \in \mathcal{X}^N} \sum_{i=1}^{N} |B_1^{i-1} (A_i - B_i) A_{i+1}^N| \\
&= \sum_{i=1}^{N} \sum_{\mathbf{u} \in \mathcal{X}^N} |B_1^{i-1} (A_i - B_i) A_{i+1}^N| \ , \quad (111)
\end{aligned}$$

where the first equality follows by the chain rule and the first inequality follows from the triangle inequality. Next, fix i, and consider the internal sum in (111),

$$\sum_{\mathbf{u} \in \mathcal{X}^N} |B_1^{i-1} (A_i - B_i) A_{i+1}^N| \ . \quad (112)$$

If i is an index for which both (101) and (102) hold, then $A_i = A_i(\mathbf{u}) = 1/2$ for all $\mathbf{u}$. For this case, we get from (102) and Lemma 24 in Appendix A that

$$\begin{aligned}
&\sum_{\mathbf{u} \in \mathcal{X}^N} |B_1^{i-1} (A_i - B_i) A_{i+1}^N| \\
&= \sum_{\mathbf{u} \in \mathcal{X}^N} B_1^{i-1} \cdot |A_i - B_i| \cdot A_{i+1}^N \\
&= \sum_{\mathbf{u} \in \mathcal{X}^N} p(u_1^{i-1}) \cdot \left| \frac{1}{2} - p(u_i | u_1^{i-1}) \right| \cdot \tilde{p}(u_{i+1}^n | u_1^i) \\
&= \sum_{u_1^i \in \mathcal{X}^i} p(u_1^{i-1}) \cdot \left| \frac{1}{2} - p(u_i | u_1^{i-1}) \right| \sum_{u_{i+1}^n \in \mathcal{X}^{N-i}} \tilde{p}(u_{i+1}^n | u_1^i) \\
&= \sum_{u_1^i \in \mathcal{X}^i} p(u_1^{i-1}) \cdot \left| \frac{1}{2} - p(u_i | u_1^{i-1}) \right| \\
&= K(U_i | U_1^{i-1}) < \frac{1}{3N} \cdot 2^{-2^{\nu'' n}} \ .
\end{aligned}$$

Otherwise, if i is an index for which either (101) or (102) do not hold, then $A_i = B_i$ for all $\mathbf{u}$, and thus (112) equals 0. The sub-claim follows.

We are now ready to state our bound on the probability of misdecoding.

Sub-claim 7. *For large enough n,*

$$\sum_{\mathbf{u}\in\mathcal{X}^N} \tilde{p}(\mathbf{u})P_{\mathrm{e}}(\mathbf{u}) < 2^{-2^{\nu'' n}} .$$

To show this, we use the two previous sub-claims as follows,

$$\begin{aligned}\sum_{\mathbf{u}\in\mathcal{X}^N} \tilde{p}(\mathbf{u})P_{\mathrm{e}}(\mathbf{u}) &= \sum_{\mathbf{u}\in\mathcal{X}^N} (p(\mathbf{u}) + \tilde{p}(\mathbf{u}) - p(\mathbf{u}))P_{\mathrm{e}}(\mathbf{u}) \\ &\le \sum_{\mathbf{u}\in\mathcal{X}^N} (p(\mathbf{u}) + |\tilde{p}(\mathbf{u}) - p(\mathbf{u})|)P_{\mathrm{e}}(\mathbf{u}) \\ &\le \sum_{\mathbf{u}\in\mathcal{X}^N} p(\mathbf{u})P_{\mathrm{e}}(\mathbf{u}) + \sum_{\mathbf{u}\in\mathcal{X}^N} |\tilde{p}(\mathbf{u}) - p(\mathbf{u})| \\ &< \frac{2}{3}\cdot 2^{-2^{\nu'' n}} + \frac{1}{3}\cdot 2^{-2^{\nu'' n}} ,\end{aligned}$$

which holds for a large enough n.

Recall that in the statement of our theorem, we have denoted the length of our codeword (after adding the guard bands) as Λ. The following subclaim proves another key part of our theorem.

Sub-claim 8. *For large enough n, the probability of misdecoding is less than $2^{-\Lambda^{\nu' n}}$.*

The proof follows by (96), Subclaim 1, and Subclaim 7.

All that remains now is to discuss the encoding and decoding complexity of our algorithms.

Sub-claim 9. *The encoding complexity is $O(\Lambda \log \Lambda)$.*

Like the complexity of successive cancellation decoding, the complexity of producing $\mathbf{u}$, and from it $\mathbf{x}$ is $O(N \log N)$. Adding the guard bands is a simple recursive process whose total time is $O(\Lambda)$. Since $\Lambda \ge N$, the result follows.

Sub-claim 10. *The decoding complexity is $O(\Lambda^{1+3\nu})$.*

The complexity of partitioning the received vector $\mathbf{y}$ into the Φ trimmed blocks $\mathbf{y}(1)^*, \mathbf{y}(2)^*, \ldots, \mathbf{y}(\Phi)^*$ is $O(\Lambda)$. Next, consider step i of the decoding algorithm, in which we decide on the value of $\hat{u}_i$. The key step is to calculate the probability

$$\begin{aligned}P(U_i = 0 | U_1^{i-1} = \hat{u}_1^{i-1}, \mathbf{Y}(1)^* = \mathbf{y}(1)^*, \\ \mathbf{Y}(2)^* = \mathbf{y}(2)^*, \ldots, \mathbf{Y}(\Phi)^* = \mathbf{y}(\Phi)^*) .\end{aligned}$$

This is done in two stages. Recall (66) and the discussion below it. First, for each $1 \le \phi \le \Phi$, we calculate the probabilities

$$P(V_{i_0}(\phi) = 0 | V_1^{i-1}(\phi) = \hat{v}_1^{i-1}(\phi), \mathbf{Y}(\phi)^* = \mathbf{y}(\phi)^*) ,$$

where i_0 is the unique integer for which

$$(i_0 - 1)\Phi + 1 \le i \le i_0 \Phi$$

and $\hat{v}_1^{i_0-1}(\phi)$ is related to $\hat{u}_1^{i-1}$ through (66). That is, we have just calculated the probabilities corresponding to the first n_0 polarization stages. Recall that by Subsection III-C, this can be done using Φ trellises. Next, we apply the remaining $n - n_0$ polarization steps to these probabilities. That is, the standard SC decoder is run for the last $n - n_0$ stages, and can be thought of as effectively operating on a code of length $N_1 = 2^{n_1} = 2^{n-n_0}$.

The total running time of the second stage is well known to be $O(N_1 \log N_1)$, which is indeed $O(\Lambda^{1+3\nu})$. Recalling the discussion in Subsection IV-D, the total running time of the first stage is

$$O(\Phi \cdot |\mathcal{S}|^3 N_0^4) ,$$

where $|\mathcal{S}|$ is the number of states in the Markov chain through which the input distribution is defined (and which we treat as a constant), $N_0 = 2^{n_0} = 2^{\lfloor n\nu \rfloor}$ and $\Phi = 2^{n-n_0} = 2^{n - \lfloor n\nu \rfloor}$. Since $N = 2^n \le \Lambda$, the result follows.

■

APPENDIX

A. Conditional Bhattacharyya and Total Variation

In this section we define the conditional Bhattacharyya parameter $Z(X|Y)$ and the conditional total variation $K(X|Y)$. See [21, Section III] for various connections between these and other measures, as well as for their relation to polarization transforms.

Definition 7 (The conditional Bhattacharyya parameter)**.** *Let $X \in \mathcal{X}$ be a binary random variable and $Y \in \mathcal{Y}$ be a discrete random variable. Let their joint distribution be $P_{X,Y}$. We denote*

$$\begin{aligned}Z(X|Y) &= 2\sum_{y\in\mathcal{Y}} \sqrt{P_{X,Y}(0,y)\cdot P_{X,Y}(1,y)} \\ &= 2\sum_{y\in\mathcal{Y}} P_Y(y)\sqrt{P_{X|Y}(0|y)\cdot P_{X|Y}(1|y)} .\end{aligned}$$

Definition 8 (The conditional total variation)**.** *Let $X \in \mathcal{X}$ be a binary random variable and $Y \in \mathcal{Y}$ be a discrete random variable. Let their joint distribution be $P_{X,Y}$. We denote*

$$\begin{aligned}K(X|Y) &= \sum_{y\in\mathcal{Y}} |P_{X,Y}(0,y) - P_{X,Y}(1,y)| \\ &= \sum_{y\in\mathcal{Y}} P_Y(y)\cdot |P_{X|Y}(0|y) - P_{X|Y}(1|y)| .\end{aligned}$$

The following lemma shows that if $K(X|Y)$ is 'small', then $P(X|Y)$ is 'close' to the Bernoulli$(1/2)$ distribution.

Lemma 24. *Let $X \in \mathcal{X}$ be a binary random variable and $Y \in \mathcal{Y}$ be a discrete random variable. Let their joint distribution be $P_{X,Y}$. Then*

$$\sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} P_Y(y)\cdot |P_{X|Y}(x|y) - 1/2| = K(X|Y) .$$

Proof.

$$\begin{aligned}&\sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} P_Y(y)\cdot |P_{X|Y}(x|y) - 1/2| \\ &= \sum_{y\in\mathcal{Y}} P_Y(y)\cdot \big(|P_{X|Y}(0|y) - 1/2| + |P_{X|Y}(1|y) - 1/2|\big) \\ &= \sum_{y\in\mathcal{Y}} P_Y(y)\cdot \big(|P_{X|Y}(0|y) - P_{X|Y}(1|y)|\big) \\ &= K(X|Y) ,\end{aligned}$$

where the penultimate equality is easily seen to hold if we denote $P_{X|Y}(0|y) = 1/2 + \delta(y)$, from which it follows that $P_{X|Y}(1|y) = 1/2 - \delta(y)$. □

B. Capacity-Achieving Inputs for the Deletion Channel

In [2], Dobrushin proves a capacity result for a class of synchronization error channels that includes the binary deletion channel. That paper also shows that the capacity can be approached by a sequence of finite-order Markov input distributions. Unfortunately, the Markov input distribution in Dobrushin's construction is not irreducible [2, Lemma 4]. Thus, Dobrushin's result falls slightly short of what is required by the polar coding construction in this paper. In [22], Li and Tan study the capacity of the concatenation of a deletion channel and a finite-state channel. For this setup, they prove a capacity result and show that the capacity can be approached by a sequence of finite-order Markov input distributions that are irreducible and aperiodic. As they note in their paper, their result is sufficient to prove that the polar coding scheme in this paper can achieve capacity.

In this section, we describe a regular hidden-Markov input distribution that also achieves capacity on the deletion channel. Though this is not required, given [22], we include it for completeness and because the argument is somewhat different.

Denote by P_{X^N} an input distribution over binary vectors of length N, which we will shortly optimize over. Let $\underline{X} \triangleq (X_1, \ldots, X_N)$ be a random binary vector of length N drawn according to P_{X^N}. Take $\underline{X}$ as the input sequence to a binary deletion channel with deletion probability $\delta \in (0,1)$ and let $\underline{Y} \triangleq (Y_1, \ldots, Y_M)$ be the corresponding output sequence where the random variable M is the output length. The maximum mutual information for a length-N input is denoted by

$$C_N \triangleq \max_{P_{X^N}} \frac{1}{N} I(\underline{X}; \underline{Y}). \tag{113}$$

It is well-known [34, proof of Theorem II.1] that NC_N is a subadditive sequence and this implies [25, Lemma 1.2.1, page 3] that

$$C = \lim_{N\to\infty} C_N = \inf_{N \geq 1} C_N$$

exists and satisfies $C \leq C_N$ for $N \geq 1$. Thus, for the optimal P_{X^N} we have

$$\frac{1}{N} I(\underline{X}; \underline{Y}) \geq C\,. \tag{114}$$

We begin with the standard approach [35] of using an optimal P_{X^N} from (113) to generate a length-kN random input $\mathbf{X} = \mathbf{X}(1) \odot \cdots \odot \mathbf{X}(k)$ where each $\mathbf{X}(i)$ is a length-N block drawn independently from P_{X^N} and using $\odot$ to represent vector concatenation. For this input, we denote the output by $\mathbf{Y} = \mathbf{Y}(1) \odot \cdots \odot \mathbf{Y}(k)$ where $\mathbf{Y}(i)$ contains the output symbols associated with the input $\mathbf{X}(i)$. Thus, for each i, the pair $\mathbf{X}(i), \mathbf{Y}(i)$ has the same distribution as the pair $\underline{X}, \underline{Y}$. The random variables $M_i = |\mathbf{Y}(i)|$, for $i \in [k]$, are chosen to equal the number of output symbols generated by the input block $\mathbf{X}(i)$.

Using the chain rule for mutual information, we note that

$$\begin{aligned} I\big(\mathbf{X}; \mathbf{Y}, M_1^k\big) &= I(\mathbf{X}; \mathbf{Y}) + I\big(\mathbf{X}; M_1^k | \mathbf{Y}\big) \\ &\leq I(\mathbf{X}; \mathbf{Y}) + k \log_2(N+1), \end{aligned}$$

where inequality follows from $I\big(\mathbf{X}; M_1^k | \mathbf{Y}\big) \leq \sum_{i=1}^k H\big(M_i\big)$ and $0 \leq M_i \leq N$. Thus, it follows that

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &\geq -k \log_2(N+1) + I\big(\mathbf{X}; \mathbf{Y}, M_1^k\big) \\ &\overset{(a)}{=} -k \log_2(N+1) + I\big(\mathbf{X}; \mathbf{Y}(1), \ldots, \mathbf{Y}(k)\big) \\ &= -k \log_2(N+1) + \sum_{i=1}^k I\big(\mathbf{X}; \mathbf{Y}(i) | \mathbf{Y}(1), \ldots, \mathbf{Y}(i-1)\big) \\ &\overset{(b)}{=} -k \log_2(N+1) + \sum_{i=1}^k I\big(\mathbf{X}(i); \mathbf{Y}(i)\big) \\ &= -k \log_2(N+1) + kI(\underline{X}; \underline{Y}) \\ &= kN \left(\frac{1}{N} I(\underline{X}; \underline{Y}) - \frac{\log_2(N+1)}{N} \right) \\ &\overset{(c)}{\geq} kN \left(C - \frac{\log_2(N+1)}{N} \right), \end{aligned}$$

where (a) holds because there is an invertible mapping from $\mathbf{Y}, M_1^k$ to $\mathbf{Y}(1), \ldots, \mathbf{Y}(k)$, (b) follows from the pairs $(\mathbf{X}(i), \mathbf{Y}(i))_{i=1}^k$ being i.i.d., and (c) follows from (114). After normalizing by the input length, this gives

$$\frac{1}{kN} I(\mathbf{X}; \mathbf{Y}) \geq C - \frac{\log_2(N+1)}{N}.$$

Thus, the information rate can be made arbitrarily close to C by choosing N large enough.

However, the infinite input distribution formed by concatenating length-N blocks cannot be generated by a regular hidden-Markov process. In order to explain how to overcome this, we will first describe this input distribution as a hidden-Markov process with state set

$$\mathcal{S} \triangleq \bigcup_{j=0}^{N-1} \big\{ x \in \{0,1\}^j \,\big|\, P_{X^j}(x) \neq 0 \big\},$$

where the set $\{0,1\}^i$ represents all possible states after i input symbols from the length-N input distribution P_{X^N}. We denote the initial state by the empty string $\varepsilon \triangleq \{0,1\}^0$ and let $P_{X^0}(\varepsilon) = 1$ by convention. To generate multiple blocks, we define the underlying Markov chain to start in the ε state and return to the ε state with probability 1 after generating N outputs. Thus, the underlying Markov chain is irreducible because we have only included states with positive probability and there is a path with positive probability from ε to any $x \in \mathcal{S}$.

Notice that the state implicitly encodes the current input position in the length-N block distribution. For example, if $s \in \{0,1\}^j$, then next symbol is drawn according to $P_{X^{j+1}|X^j}(x|s)$. Thus, the underlying Markov chain is periodic with period N. To make it aperiodic, we will introduce one additional state, which we denote by τ, that is used to dither the input block between length-N and length-$(N+1)$. State τ always outputs a dither bit whose value is 0 and then transitions to state ε. The idea is that, after a length-N input block, a fair coin is used to determine if the next block will start immediately (e.g., the underlying Markov chain transitions to state ε) or be delayed by one symbol (e.g., the underlying Markov chain transitions to state τ). After this, the modified Markov chain will be aperiodic because the transition graph has loops of length N and $N+1$. The period of a Markov chain is the greatest common divisor of the lengths of all loops in the transition graph. Since N and $N+1$ are relatively prime, the period is 1 and the chain is aperiodic. We also note that

the new Markov chain is still irreducible because there is still a path with positive probability between any two states.

Let S_0 be initial state of the underlying Markov chain. In the current formulation, we have $S_0 = \varepsilon$ with probability 1 and the Markov chain is not stationary. One can make this Markov chain stationary by drawing the initial state S_0 from the stationary distribution of the underlying Markov chain. After this change, we have constructed a regular hidden-Markov input derived from our original P_{X^N} block distribution.

Now, let $\mathbf{X}$ be a length-$k(N+1)$ input drawn from the constructed hidden-Markov process. This input can be broken into segments by adding commas before the inputs generated by the state ε. A complete segment is delimited by commas on both sides, and thus has length either N or $N+1$. Note that $\mathbf{X}$ contains at least k segments, and by discarding the first segment we get at least $k-1$ complete segments. We call the length-N prefix of a complete segment a block. Thus, we have at least $k-1$ blocks, $\mathbf{X}(2), \ldots, \mathbf{X}(k)$, where each block can be associated with an independent draw from P_{X^N}. Let $T_i \in \{0,1\}$ be the side-information random variable that indicates, for the i-th (possibly incomplete) segment, whether or not state τ was visited during that segment. Given S_0 and T_1^k, it is always possible to compute the locations of the commas described above and separate $\mathbf{X}$ into the $k-1$ blocks $\mathbf{X}(2), \ldots, \mathbf{X}(k)$. This is because S_0 gives the initial offset into the first segment and T_i indicates whether or not each segment has the additional dither bit.

Similarly, the output $\mathbf{Y}$ can be separated into subvectors associated with the above blocks by adding commas to separate outputs generated by different segments and removing any outputs caused by dither bits. Namely, we let $M_i \in \{0, \ldots, N+1\}$ be the side-information random variable that indicates the number of outputs generated by the i-th *segment* and $R_i \in \{0,1\}$ be the side-information random variable that indicates whether the last output in a subvector is due to a dither bit. Given M_1^k and R_1^k, it is always possible to separate $\mathbf{Y}$ into $\mathbf{Y}(2), \ldots, \mathbf{Y}(k)$ where each $\mathbf{Y}(i)$ is the output associated with the block $\mathbf{X}(i)$. Thus, each pair $(\mathbf{X}(i), \mathbf{Y}(i))$ has the same distribution as $(\underline{X}, \underline{Y})$. Using this setup, the chain rule of mutual information and cardinality upper bounds imply that

$$\begin{aligned}
&I\big(\mathbf{X}, T_1^k; \mathbf{Y}, M_1^k, R_1^k | S_0\big) = I\big(\mathbf{X}, T_1^k; \mathbf{Y}, M_1^k, R_1^k\big) \\
&\quad + I\big(\mathbf{X}, T_1^k; S_0 | \mathbf{Y}, M_1^k, R_1^k\big) - I\big(\mathbf{X}, T_1^k; S_0\big) \\
&\le I\big(\mathbf{X}, T_1^k; \mathbf{Y}, M_1^k, R_1^k\big) + I\big(\mathbf{X}, T_1^k; S_0 | \mathbf{Y}, M_1^k, R_1^k\big) \\
&\overset{(a)}{\le} I\big(\mathbf{X}, T_1^k; \mathbf{Y}, M_1^k, R_1^k\big) + N \\
&= I\big(\mathbf{X}; \mathbf{Y}, M_1^k, R_1^k\big) + I\big(T_1^k; \mathbf{Y}, M_1^k, R_1^k | \mathbf{X}\big) + N \\
&\overset{(b)}{\le} I\big(\mathbf{X}; \mathbf{Y}, M_1^k, R_1^k\big) + k + N \\
&= I\big(\mathbf{X}; \mathbf{Y}\big) + I\big(\mathbf{X}; M_1^k, R_1^k | \mathbf{Y}\big) + k + N \\
&\overset{(c)}{\le} I\big(\mathbf{X}; \mathbf{Y}\big) + k \log_2(N+2) + k + k + N, \qquad (115)
\end{aligned}$$

where (a) follows from $\log_2 |\mathcal{S}| = \log_2 \left(1 + \sum_{j=0}^{N-1} 2^j\right) = N$, (b) holds because $T_i \in \{0,1\}$, and (c) follows from $0 \le M_i \le N+1$ and $R_i \in \{0,1\}$.

Based on the decompositions described above, the data processing inequality implies that

$$\begin{aligned}
&I\big(\mathbf{X}, T_1^k; \mathbf{Y}, M_1^k, R_1^k | S_0\big) \\
&\quad \ge I\big(\mathbf{X}(2), \ldots, \mathbf{X}(k); \mathbf{Y}(2), \ldots, \mathbf{Y}(k) \big| S_0\big) \\
&\quad = I\big(\mathbf{X}(2), \ldots, \mathbf{X}(k); \mathbf{Y}(2), \ldots, \mathbf{Y}(k)\big) \\
&\quad = \sum_{i=2}^{k} I\big(\mathbf{X}(i); \mathbf{Y}(i)\big) = (k-1) I(\underline{X}; \underline{Y}). \qquad (116)
\end{aligned}$$

Combining (114)–(116), we have

$$I(\mathbf{X}; \mathbf{Y}) \ge -k \log_2(N+2) - 2k - N + (k-1)CN.$$

To lower bound the information rate, we can normalize by the input length to see that

$$\begin{aligned}
&\frac{1}{k(N+1)} I(\mathbf{X}; \mathbf{Y}) \\
&\qquad \ge \frac{(k-1)N}{k(N+1)} \left(C - \frac{1}{k-1}\right) - \frac{2 + \log_2(N+2)}{N+1}.
\end{aligned}$$

By choosing k and N large enough, the information rate can be made arbitrarily close to C. Thus, we have constructed a sequence of regular hidden-Markov input distributions that achieve capacity on the binary deletion channel.

In closing, we note that this argument works without change for channels with independent insertions, deletions, and substitutions.

REFERENCES

[1] R. Gallager, "Sequential decoding for binary channels with noise and synchronization errors," 1961, lincoln Lab Group Report.

[2] R. L. Dobrushin, "Shannon's theorems for channels with synchronization errors," *Problemy Peredachi Informatsii*, vol. 3, no. 4, pp. 18–36, 1967.

[3] M. C. Davey and D. J. MacKay, "Reliable communication over channels with insertions, deletions, and substitutions," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 687–698, 2001.

[4] M. Mitzenmacher, "A survey of results for deletion channels and related synchronization channels," *Probability Surveys*, vol. 6, pp. 1–33, 2009.

[5] D. Fertonani and T. M. Duman, "Novel bounds on the capacity of the binary deletion channel," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2753–2765, 2010.

[6] H. Mercier, V. Tarokh, and F. Labeau, "Bounds on the capacity of discrete memoryless channels corrupted by synchronization and substitution errors," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4306–4330, 2012.

[7] A. R. Iyengar, P. H. Siegel, and J. K. Wolf, "Modeling and information rates for synchronization error channels," in *Proc. IEEE Int. Sym. on Information Theory*. IEEE, 2011, pp. 380–384.

[8] ——, "On the capacity of channels with timing synchronization errors," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, pp. 793–810, 2015.

[9] M. Rahmati and T. M. Duman, "Upper bounds on the capacity of deletion channels using channel fragmentation," *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 146–156, 2015.

[10] J. Castiglione and A. Kavcic, "Trellis based lower bounds on capacities of channels with synchronization errors," in *Information Theory Workshop*. Jeju, South Korea: IEEE, 2015, pp. 24–28.

[11] M. Cheraghchi, "Capacity upper bounds for deletion-type channels," *Journal of the ACM (JACM)*, vol. 66, no. 2, p. 9, 2019.

[12] E. K. Thomas, V. Y. F. Tan, A. Vardy, and M. Motani, "Polar coding for the binary erasure channel with deletions," *IEEE Communications Letters*, vol. 21, no. 4, pp. 710–713, April 2017.

[13] K. Tian, A. Fazeli, A. Vardy, and R. Liu, "Polar codes for channels with deletions," in *55th Annual Allerton Conference on Communication, Control, and Computing*, 2017, pp. 572–579.

[14] K. Tian, A. Fazeli, and A. Vardy, "Polar coding for deletion channels: Theory and implementation," in *IEEE International Symposium on Information Theory*, 2018, pp. 1869–1873.

[15] ——, "Polar coding for deletion channels," 2018, submitted to IEEE Transactions on Information Theory.

[16] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

[17] R. Wang, R. Liu, and Y. Hou, "Joint successive cancellation decoding of polar codes over intersymbol interference channels," 2014, arXiv preprint arXiv:1404.3001.

[18] R. Wang, J. Honda, H. Yamamoto, R. Liu, and Y. Hou, "Construction of polar codes for channels with memory," in *2015 IEEE Information Theory Workshop*, October 2015, pp. 187–191.

[19] R. A. Wagner and M. J. Fischer, "The string-to-string correction problem," *Journal of the ACM (JACM)*, vol. 21, no. 1, pp. 168–173, 1974.

[20] E. Şaşoğlu and I. Tal, "Polar coding for processes with memory," *IEEE Trans. Inform. Theory*, vol. 65, no. 4, pp. 1994–2003, April 2019.

[21] B. Shuval and I. Tal, "Fast polarization for processes with memory," *IEEE Trans. Inform. Theory*, vol. 65, no. 4, pp. 2004–2020, April 2019.

[22] Y. Li and V. Y. F. Tan, "On the capacity of channels with deletions and states," *arXiv preprint arXiv:1911.04473*, 2019.

[23] E. Şaşoğlu, "Polar Coding Theorems for Discrete Systems," Ph.D. dissertation, IC, Lausanne, 2011.

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

[25] J. M. Steele, *Probability Theory and Combinatorial Optimization*. Philadelphia, PA: SIAM, 1997, vol. 69, CBMF-NSF Regional Conference Series in Applied Mathematics.

[26] R. Durrett, *Probability: Theory and Examples*. Cambridge University Press, 2019, vol. 49.

[27] E. Şaşoğlu, "Polarization and polar codes," in *Found. and Trends in Commun. and Inform. Theory*, vol. 8, no. 4, 2012, pp. 259–381.

[28] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 7829–7838, December 2013.

[29] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. IEEE Int. Sym. on Information Theory*, June 2009, pp. 1493–1495.

[30] B. Shuval and I. Tal, "Universal polarization for processes with memory," 2018, arXiv:1811.05727v1.

[31] W. Hoeffding, "Probability inequalities for sums of random variables," *Journal of the American Statistical Association*, vol. 53, no. 301, pp. 13–30, March 1963.

[32] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomizition and Probabilistic Techniques in Algorithms and Data Analysis*, 2nd ed. Cambridge, UK: Cambridge University Press, 2005.

[33] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, Ecole Polytechnique Fédérale de Lausanne, 2009.

[34] Y. Kanoria and A. Montanari, "Optimal coding for the binary deletion channel with small deletion probability," *IEEE Trans. Inform. Theory*, vol. 59, no. 10, pp. 6192–6219, 2013.

[35] J. Chen and P. H. Siegel, "Markov processes asymptotically achieve the capacity of finite-state intersymbol interference channels," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1295–1303, 2008.