Probabilistic Shaping for Trellis-Coded Modulation with CRC-Aided List Decoding

Linfang Wang, Dan Song, Felipe Areces, Thomas Wiegart, and Richard D. Wesel

***Abstract*—This paper applies probabilistic amplitude shaping (PAS) to cyclic redundancy check (CRC)-aided tail-biting trellis-coded modulation (TCM). CRC-TCM-PAS produces practical codes for short block lengths on the additive white Gaussian noise (AWGN) channel. In the transmitter, equally likely message bits are encoded by a distribution matcher (DM) generating amplitude symbols with a desired distribution. A CRC is appended to the sequence of amplitude symbols, and this sequence is then encoded and modulated by TCM to produce real-valued channel input signals. This paper proves that the sign values produced by the TCM are asymptotically equally likely to be positive or negative. The CRC-TCM-PAS scheme can thus generate channel input symbols with a symmetric capacity-approaching probability mass function. The paper provides an analytical upper bound on the frame error rate of the CRC-TCM-PAS system over the AWGN channel. This FER upper bound is the objective function used for jointly optimizing the CRC and convolutional code. Additionally, this paper proposes a multi-composition DM, which is a collection of multiple constant-composition DMs. The optimized CRC-TCM-PAS systems achieve frame error rates below the random coding union (RCU) bound in AWGN and outperform the short-blocklength PAS systems with various other forward error correction codes studied in [2].**

***Index Terms*—reliable communication, short blocklength, probabilistic shaping, trellis-coded modulation, tail-biting convolutional code, CRC, list decoding, distribution matcher.**

I. Introduction

This paper explores reliable communications over the additive white Gaussian noise (AWGN) channel with high spectral efficiency for short block lengths. To closely approach theoretical limits, it is helpful to use shaping so that signal points are not equally likely, not equally spaced, or both [3]–[9]. Recently, a new technique called probabilistic amplitude shaping (PAS) [10], [11] employs a distribution matcher (DM) [12] before the forward error correction (FEC) encoder and channel-signaling mapping function to accomplish optimal or almost optimal shaping.

A PAS system as in [10], [11] decomposes a channel input sequence into a magnitude symbol sequence and a sign sequence. The magnitude symbol sequence is generated by a DM. The output of the DM is provided as input to a systematic FEC code where the parity check bits indicate the signs of the channel inputs. A channel-signaling mapping function maps the amplitude symbol sequence and the sign-bit sequence to the corresponding sequence of transmitted signal points.

A distribution matcher [12]–[17] maps a binary input sequence onto a symbol sequence that determines the magnitudes of the transmitted symbols. The binary input sequence typically has equally likely ones and zeros. However, the output symbols from the distribution matcher are not equally likely. Specifically, the distribution matcher is designed such that the PAS system can generate channel inputs with a capacity-approaching probability mass function (PMF).

Even though it is well-known that a continuous Gaussian probability density function (PDF) is a capacity-achieving distribution for the power-constrained additive Gaussian white noise (AWGN) channel, a carefully designed finite-cardinality PMF can deliver performance that is almost indistinguishable from that of a Gaussian PDF and facilitates practical implementation. In [6], Kschischang *et. al.* use Maxwell-Boltzmann distribution to optimize the PMF of equally-spaced pulse-amplitude modulation (PAM) or quadrature amplitude modulation (QAM) constellations. Xiao *et. al.* use dynamic Blahut-Arimoto (DAB) to identify minimum-cardinality capacity-approaching input PMFs for PAM constellations [9]. The empirical distribution of the output symbols of a good distribution matcher will closely resemble the target PMF as determined, for example, according to [6] or [9]. The shell-mapping (SM) DM [13], [14] is optimal under the metric of normalized Kullback-Leibler (KL) divergence. Schulte *et al.* in [12] propose an asymptotically optimal distribution matcher, the constant composition (CC) DM. Some other distribution matchers include those of [15]–[17].

An important design choice for a PAS system is the selection of an FEC code. In the long blocklength regime, Böcherer *et. al.* in [10] use low-density parity-check (LDPC) codes for the PAS system. In the short blocklength regime, Coşkun *et. al.* in [2] investigate PAS systems with various FEC choices, including binary LDPC codes, non-binary LDPC codes and polar codes.

Recently, convolutional codes with cyclic redundancy code (CRC)-aided list decoding have shown excellent performance in the short blocklength regime [18]–[21]. Yang *et al.* in [18] show that a tail-biting convolutional code (TBCC) with CRC-aided list decoding can achieve frame error rate (FER) performance very close to the short-blocklength random coding union (RCU) bound [22]. King. *et al.* in [23] provide an example where a TBCC outperforms a polar code in the AWGN channel when both are decoded using CRC-aided list

This paper was presented in part at IEEE ICC 2022. [1]

This work was supported by the National Science Foundation (NSF) under Grant CCF-1911166 and CCF-1955660.

A portion of this paper was accepted to IEEE GLOBECOM 2022.

Linfang Wang, Dan Song, Felipe Areces, Richard Wesel are with the Department of Electrical and Computer Engineering, University of California, Los Angeles, Los Angeles, CA, 90095 USA. Email: {lfwang,dansong,fareces99,wesel}@ucla.edu.

Thomas Wiegart is with the Institute for Communications Engineering, Technical University of Munich (TUM), Munich, 80333, Germany (e-mail: thomas.wiegart@tum.de).

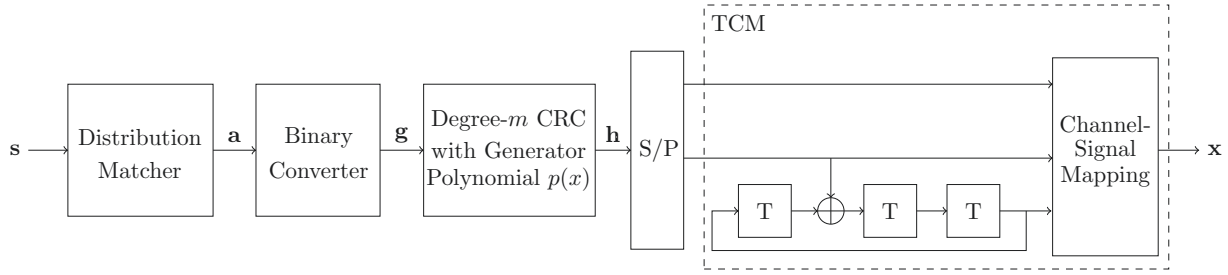


Fig. 1. Diagram of the CRC-TCM-PAS transmitter. In the diagram, $\mathbf{s} \in \mathbb{F}_2^k$, $\mathbf{a} \in \mathcal{C}_{\rm DM} \subseteq \mathcal{A}^l$, $\mathbf{g} \in \mathbb{F}_2^{k_0 l}$, $\mathbf{h} \in \mathbb{F}_2^{k_0 l+m}$, $\mathbf{x} \in \mathcal{X}^n$, and $n = l + \frac{m}{k_0}$. The transmission rate of the system is $\frac{k}{n}$ bits/real channel use. The TCM in this figure uses a rate-$\frac{2}{3}$ TBCC.

decoding.

In this paper, we propose a PAS system designed for the AWGN channel in the short-blocklength regime. The proposed PAS system uses a CRC-aided, rate-$\frac{k_0}{k_0+1}$, systematic, recursive TBCC as the FEC code. The TBCC and the channel-signal mapping function constitute the TCM [24]. We refer to the proposed PAS system as CRC-TCM-PAS. Fig. 1 describes the transmitter of the CRC-TCM-PAS system. A CRC-TCM-PAS system can be designed as follows:

1) Using [6] or [9], identify the capacity-approaching PMF for the PAM constellation under AWGN, which induces the PMF for the corresponding magnitudes.
2) Assuming an ideal distribution matcher that generates magnitude sequences whose symbols are independent and identically distributed (i.i.d.) according to the distribution calculated in 1), optimize the CRC and TBCC using the FER upper bound developed in Section V.
3) Replace the ideal distribution matcher with a practical one.

The contributions of this paper are summarized as follows:

- *CRC-TCM-PAS transmission system.* This paper presents the paradigm of the CRC-TCM-PAS system.
- *Multi-composition distribution matcher (MCDM).* This paper proposes a multi-composition distribution matcher (MCDM) matcher which can be seen as a collection of CCDMs. We note that the proposed distribution matcher is a generalization of the MCDM in [25], which limits the cardinality of the output alphabet to 2. We investigate two rules to select the CCDMs, which are related to high-probability sets and typical sets in information theory.
- *CRC-TCM-PAS Decoder.* We propose automorphism enabled decoding [26] to achieve near-maximum-likelihoood performance with low time complexity.
- *Properties of CRC-TCM-PAS transmission system.* This paper proves that, asymptotically, the sign values produced by the TCM are equally likely to be positive or negative. This yields channel input symbols that have a symmetric capacity-approaching distribution.
- *Optimization of CRC-TCM-PAS parameters.* This paper derives an upper bound on the FER of CRC-TCM-PAS systems and uses this bound as an objective function to jointly optimize the CRC and TBCC. The optimized CRC-TCM-PAS systems achieve FERs below the random coding union (RCU) bound in AWGN and outperform the short-blocklength PAS systems with various other forward error correction codes studied in [2].

The remainder of this paper is organized as follows: Section II reviews CCDM and presents MCDM. Section III presents CRC-TCM-PAS system architecture. Section IV proves the symmetric capacity-approaching distribution of the output of the CRC-TCM-PAS system. Section V derives the FER upper bound, and Section VI presents the simulation results of CRC-TCM-PAS systems with different input lengths and transmission rates. Section VII concludes our work.

In this paper, we use the italic upper case letter A to denote a random variable. We use $A^l = [A_1, \ldots, A_l]$ to denote a random vector. We use the italic lowercase letter a to denote a realization of A or a variable. We use the straight bold lowercase letter $\mathbf{a}$ to denote either a realization of A^l or a column vector. Specifically, $[\mathbf{a}]_m$ is a vector that contains last m elements in $\mathbf{a}$. Finally, we use the straight, bold upper case letter $\mathbf{A}$ to denote a matrix.

II. Multi-Composition Distribution Matcher

The section reviews CCDM and presents a multi-composition distribution matcher (MCDM).

A. Preliminaries

A fixed-to-fixed distribution matcher is an injective function f_{DM} that maps a binary length-k source sequence $\mathbf{s} \in \mathbb{F}_2^k$ to a length-l symbol sequence $\mathbf{a} \in \mathcal{A}^l$, i.e., $f_{DM} : \{0,1\}^k \to \mathcal{A}^l$. $\mathcal{A} = \{0, 1, ..., |\mathcal{A}| - 1\}$ is the output symbol set. In this paper, we limit $\log_2 |\mathcal{A}| = k$ to be some integer. The range of $f_{\rm DM}$ is the codebook of the distribution matcher, which is denoted by $\mathcal{C}_{\rm DM}$. Because $f_{\rm DM}$ is an one-to-one mapping, it has $|\mathcal{C}_{\rm DM}| = 2^k$. Additionally, because the input bits of the DM are equally likely, it has $P_{A^l}(\mathbf{a}) = 2^{-k}$, for $\mathbf{a} \in \mathcal{C}_{\rm DM}$. Let $P(\bar{A})$ be the empirical distribution of a DM with codebook $\mathcal{C}_{\rm DM}$.

The quality of a DM can be measured as its KL divergence with a *theoretically* optimal DM, which is referred to as a random DM. The random DM uses the construction method of Shannon's random code [27]. Given the desired probability $P(\hat{A})$, in each transmission, the random DM randomly generates a codebook that contains 2^k codewords of length l according to the distribution $P_{\hat{A}^l}(\mathbf{a}) = \prod_{i=1}^{l} P_{\hat{A}}(a_i)$. The KL

TABLE I
COMPARION OF VARIOUS DMS TARGETING FOR DISTRIBUTION $P(\hat{A}) = (0.072, 0.165, 0.321, 0.442)$.
ALL DMS HAVE 96 INPUT BITS AND 63 OUTPUT SYMBOLS.

	ESS	MCDM with $\mathcal{C}_{\rm HP}$	MCDM with $\mathcal{C}_{\rm TS}$	CCDM
normalized KL divergence	0.074	0.077	0.096	0.213
required storage (bits)	3.6e5	3e5	3e4	24

divergence between a practical DM with $\mathcal{C}_{\rm DM}$ and a random DM is calculated by [12]:

$$D_{\rm KL}\left(P(A^l)||P(\hat{A}^l)\right) = \frac{1}{2^k}\log_2\left(\sum_{\mathbf{a}\in\mathcal{C}_{\rm DM}}\frac{1}{P_{\hat{A}^l}(\mathbf{a})}\right) - k, \tag{1}$$

In this paper, we follow the convention in [12], and use the normalized KL divergence, $\frac{1}{l}D_{\rm KL}\left(P(A^l)||P(\hat{A}^l)\right)$, as the metric to evaluate the distribution matcher.

A DM with a small normalized KL divergence is desired. One well-known DM with simple encoding and decoding algorithm is CCDM, whose codebook, $\mathcal{C}_{\rm CCDM}$, contains the sequences that have the same *type*, which is defined as follows [27, Chapter 11]:

Definition 1. *The type (or empirical distribution) $P_{\mathbf{a}}$ of a sequence $\mathbf{a} = [a_0, a_1, \ldots, a_{l-1}]$ is the relative proportion of occurrence of each symbol in $\mathcal{A}$, i.e., $P_{\mathbf{a}}(i) = \frac{\sum_{j=0}^{l-1}\mathbb{1}(a_j=i)}{l}$, $i \in \mathcal{A}$. Define the set of sequences of length l and type P as set class of P, denoted by $\mathcal{T}_P^l$:*

$$\mathcal{T}_P^l = \{\mathbf{a} \in \mathcal{A}^l : P_{\mathbf{a}} = P\}. \tag{2}$$

Based on Definition 1, the codebook of CCDM is a subset of a set class of some type P. The type P is chosen such that $2^k \le |\mathcal{T}_P^l|$, and normalized KL divergence is minimized in the meanwhile. Because all codewords in $\mathcal{C}_{\rm CCDM}$ have the same type P, the empirical distribution of CCDM $P(\bar{A}) = P$. There are two major advantages to CCDM. First, the CCDM is asymptotically optimal, i.e., $\lim_{l\to\infty}\frac{1}{l}D_{\rm KL}\left(P(A^l)||P(\hat{A}^l)\right) = 0$. Second, a CCDM can use arithmetic coding to sequentially generate the codewords in $\mathcal{C}_{\rm CCDM}$ [12]. However, the normalized KL-divergence of CCDM is large in the short-blocklength regime [12].

B. Multi-Composition Distribution Matcher

In this section, we propose a multi-composition distribution matcher (MCDM) that delivers a small normalized KL divergence in the short blocklength regime. The MCDM codebook can been seen as a union of multiple CCDM codebooks. The codebook of an MCDM, $\mathcal{C}_{\rm MCDM}$, has the following properties:

1) $\mathcal{C}_{\rm MCDM}$ is a union of τ disjoint children codebooks, i.e., $\mathcal{C}_{\rm MCDM} = \bigcup_{i=1}^{\tau}\mathcal{C}_i$, and $\mathcal{C}_i \bigcap \mathcal{C}_j = \varnothing$, for $i \neq j$.
2) The codewords in a child codebook have the same type, i.e., $\mathcal{C}_i \subseteq \mathcal{T}_{P_{A_i}}^l$, $i = 1, 2, ..., \tau$. No two different children codebooks share the same type.
3) Let $k_i = \left\lfloor \log_2(\mathcal{T}_{P_{A_i}}) \right\rfloor$ for $i = 1, \ldots, \tau$, then $|\mathcal{C}_i| = 2^{k_i}$, for $i = 1, 2, ..., \tau-1$, and $|\mathcal{C}_\tau| = 2^k - \sum_{i=1}^{\tau-1}2^{k_i}$.

Let b_i be the cardinality of the union of the first i codebooks, i.e., $b_i = \sum_{m=1}^{i}|\mathcal{C}_i|$, where $i = 1, ..., \tau$. Specifically, define $b_0 = 0$. Given a binary input $\mathbf{s}$, the encoding algorithm for MCDM is summarized as follows. First, choose the child CCDM $\mathcal{C}_i$ associated with input sequence $\mathbf{s}$, i is selected such that $b_{i-1} \le s < b_i$, where s is the decimal representation of $\mathbf{s}$. Second, Calculate the child CCDM input as $\mathbf{c} = [\mathbf{s} - \mathbf{b}_{i-1}]_{k_i}$, where $\mathbf{b}_i$ to denote the binary representation of b_i and the operator $[\cdot]_{k_i}$ returns last k_i bits. Finally, Perform CCDM encoding with the child CCDM $\mathcal{C}_i$ using input $\mathbf{c}$, and generate the output sequence.

The MCDM decoding process is as follows: For any $\mathbf{a} \in \mathcal{A}^l$, the decoder first checks whether the type of $\mathbf{a}$ is one of the types in $\mathcal{C}_{\rm MCDM}$. If so, the decoder checks whether $\mathbf{a}$ is in $\mathcal{C}_{\rm MCDM}$. Otherwise, the decoder declares that $\mathbf{a} \notin \mathcal{C}_{\rm MCDM}$.

An important design question regarding MCDM is the selection of children codebooks $\mathcal{C}_i$, $i = 1, ..., \tau$. Given a target distribution $P(\hat{A})$, we investigate two rules for choosing $\mathcal{C}_i$, namely, high-probability rule and typical-set rule:

Rule 1: High-probability Rule:

$$P(A_i) = \underset{P(A^*)\in\mathcal{P}\setminus\{P(A_1),..,P(A_{i-1})\}}{\operatorname{argmax}} \sum_{a=1}^{|\mathcal{A}|} P_{A^*}(a)\log P_{\hat{A}}(a). \tag{3}$$

Rule 2: Typical-set Rule:

$$P(A_i) = \underset{P(A^*)\in\mathcal{P}\setminus\{P(A_1),..,P(A_{i-1})\}}{\arg\min} \mathrm{D}_{\rm KL}(P(A^*)||P(\hat{A})). \tag{4}$$

$\mathcal{P}$ is the set of all possible types of length-l symbol sequences. Rule 1 chooses the types whose sequences occur with the highest probability according to $P(\hat{A})$. On the other hand, rule 2 chooses the types that are most similar to $P(\hat{A})$. The codebooks built using rules 1 and 2 are related to the concept of high-probability set and typical set in information theory [27, Chapter 3.3], respectively. We use $\mathcal{C}_{\rm HP}$ and $\mathcal{C}_{\rm TS}$ to denote the codebooks built using high-probability and typical-set rules, respectively.

C. Comparison

In this subsection, we compare the performance of various distribution matchers in terms of the normalized KL divergence and required memory. We design the distribution matcher with 96 input bits and 63 output symbols from an 4-ary alphabet. The target distribution is $P(\hat{A}) = (0.072, 0.165, 0.321, 0.442)$.

Additional to the MCDM and CCDM, we also consider a DM called enumerative sphere shaping (ESS) [28]. ESS has an excellent performance in the short block length regime. Given a symbol sequence $\mathbf{a} = [a_1 \ldots a_l]$, the energy of $\mathbf{a}$ is defined as $\sum_{i=1}^{l} a_i^2$. ESS considers the sequences whose energies are less than or equal to a threshold $E_{\rm max}$ as codeword candidates

of the distribution matcher. Given an $E_{\max}$, ESS indexes the qualified sequences lexicographically, and an energy-bounded trellis is built to index the sequences.

Table I gives the normalized KL divergence of CCDM, MCDM, and ESS. CCDM delivers the largest normalized KL divergence, while ESS delivers the smallest normalized KL divergence. The MCDM with $\mathcal{C}_{\mathrm{HP}}$ delivers a comparable normalized KL divergence with ESS, and the MCDM with $\mathcal{C}_{\mathrm{TS}}$ is slightly larger than that of MCDM with $\mathcal{C}_{\mathrm{HP}}$.

We also compare the required memories for these four DMs. For the CCDM, it suffices to only store the type of codewords. For the ESS, the node values in the trellises are needed [28]. The MCDM needs to store all of the types of children CCDMs and the binary thresholds $\mathbf{b}$. As shown in Table I, CCDM only needs 24 bits for storing the codeword type. The MCDM with $\mathcal{C}_{\mathrm{HP}}$ requires a little bit less memory than ESS. The memory for the MCDM with $\mathcal{C}_{\mathrm{TS}}$ is an order of magnitude smaller than the memory for the MCDM with $\mathcal{C}_{\mathrm{HP}}$, because it uses fewer children CCDMs. In this example, $\mathcal{C}_{\mathrm{HP}}$ requires 2535 children CCDMs and $\mathcal{C}_{\mathrm{TS}}$ requires 327.

III. CRC-TCM-PAS System

This section presents the transmitter structure and the decoding algorithms for the proposed CRC-TCM-PAS transmission system.

A. CRC-TCM-PAS Transmission System Structure

Fig. 1 illustrates the diagram of the proposed CRC-TCM-PAS transmitter. The CRC-TCM-PAS system consists of three encoding procedures. First, a length-k binary source sequence $\mathbf{s} \in \mathbb{F}_2^k$ is encoded to a length-l symbol sequence $\mathbf{a} \in \mathcal{C}_{\mathrm{DM}}$ by a distribution matcher. Then, the binary representation $\mathbf{g}$ of $\mathbf{a}$ with k_0 bits per symbol, $\mathbf{g} \in \mathbb{F}_2^{k_0 l}$, is encoded by a systematic m-bit CRC with generator polynomial $p(x)$. The proposed system implicitly requires that k_0 divides m. Finally, the TCM module encodes the CRC output and maps the encoded bits to a length-n channel input sequence $\mathbf{x} \in \mathcal{X}^n$, where $\mathcal{X}$ denotes the AM constellation set and $n = l + \frac{m}{k_0}$. The TCM module includes a systematic, rate-$\frac{k_0}{k_0+1}$ TBCC, and a channel-signal mapping function which maps each k_0+1 encoded bits onto one of 2^{k_0+1} symbols in the AM constellation set $\mathcal{X}$.

The transmission rate of the CRC-TCM-PAS system is $\frac{k}{n}$ bits/real channel use. The remainder of this subsection introduces TBCC and the channel-signal mapping function for TCM.

1) Tail Biting Convolutional Code: A convolutional code with ν memory elements that takes a k_0-bit input symbol and generates a γ_0-bit output symbol in one stage is denoted by an (γ_0, k_0, ν) convolutional code. We refer to each input symbol as a *data frame*, and each output symbol as a *code frame*. This paper is focused on (k_0+1, k_0, ν) convolutional code. The convolutional code in Fig. 1 has $k_0 = 2$. Let $\mathcal{U} = \{0, 1, \ldots, 2^{k_0} - 1\}$ be the set of input symbols and $\mathcal{O} = \{0, 1, \ldots, 2^{\gamma_0} - 1\}$ be the set of output symbols. Denote the input symbol and output symbol in stage t by u_t and o_t, respectively. A convolutional code with n data frames can be described as an n-stage trellis. Denote the set of vertices (or states) at time instant t by $\mathcal{V}_t$. Let v_t be the state at time t. Denote an edge that starts with v_t, ends at v_{t+1} and has an output o_t by a 3-tuple (v_t, o_t, v_{t+1}). Let $\mathcal{E}_t$ be the set of edges in stage t. In this paper, we let $\mathcal{V}_t = \mathcal{V} = \{0, 1, \ldots, 2^\nu - 1\}$, and $\mathcal{E}_t = \mathcal{E}$. Let the sequence $(v_0, o_0, v_1, o_1, \ldots, o_{n-1}, v_n)$ be a valid path in the trellis, a tail-biting path requires $v_0 = v_n$. Denote the TBCC trellis by $\mathcal{T}$, and denote the TBCC sub-trellises whose starting and ending state are i, $i \in \mathcal{V}$, by $\mathcal{T}_i$.

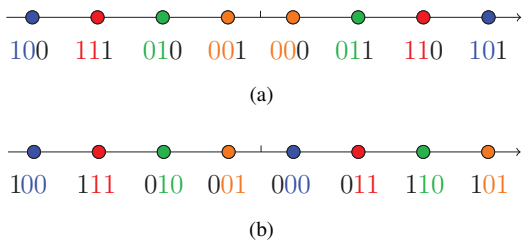


Fig. 2. Labeling of 8-AM channel signals from (a) magnitude perspective and (b) coset perspective. The least significant two bits identify the coset. The most significant two bits indicate the magnitude. The exclusive-or of all three bits indicates the sign.

2) Mapping Rule: In order to maximize free Euclidean distance (ED) of TCM, Ungerboeck in [24] proposed a mapping rule called "mapping by set partitioning". Ungerboeck's set partitioning mapping rule follows from the successive partitioning of a channel-signal set into subsets with increasing minimum distance between the signals in these subsets. With set partitioning, the coded bits serve as coset labels so that "uncoded errors" are guaranteed to have at least minimum distance between elements in the same coset.

Our design has an additional requirement that the systematic bits identify the magnitude of the symbol as produced by the distribution matcher. Fig. 2 gives binary labels for the equidistant 8-AM constellation set using a labeling that achieves both of these objectives. In this labeling, the sign is negative when the exclusive-or of all three bits is one. The two most significant bits are the systematic bits that identify the magnitude, and one may view the least significant bit as selecting the sign. The two least significant bits identify the coset, and one may view the most significant bit as selecting the sign.

B. Decoding Algorithms

The channel observation at the receiver over an AWGN channel is $\mathbf{y} = \mathbf{x} + \mathbf{z}$, where $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$ is the noise vector and σ^2 is the noise variance. This subsection introduces various decoding algorithms with varied complexity and error correction performance. We first give the definition of the codeword of a CRC-TCM-PAS system:

Definition 2. *$\mathbf{x} \in \mathcal{X}^n$ is a CRC-TCM-PAS codeword if it satisfies all of the following conditions:*

1) *$\mathbf{x}$ is a codeword of TCM.*
2) *The dataword of TCM that generates $\mathbf{x}$, $\mathbf{h}$, passes the CRC check.*
3) *The information bits $\mathbf{g}$ of the CRC codeword $\mathbf{h}$, are the binary representation of a codeword in $\mathcal{C}_{\mathrm{DM}}$.*

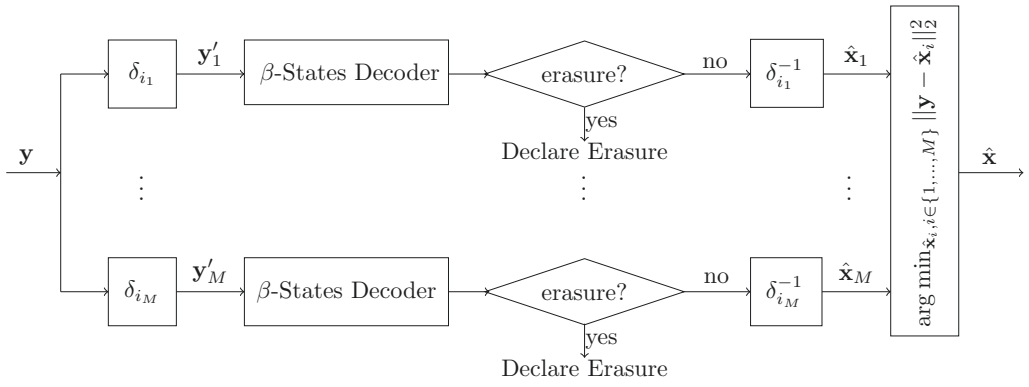


Fig. 3. The diagram of an AE decoder with M parallel β-States decoders, i.e., AED(M,β).

Denote the codebook of CRC-TCM-PAS by $\mathcal{C}_{\rm CTP}$, which has cardinality $|\mathcal{C}_{\rm CTP}| = 2^k$.

1) Maximum Likelihood (ML) Decoder: For AWGN, the ML decoder finds $\hat{\mathbf{x}} \in \mathcal{C}_{\rm CTP}$ that has smallest Euclidean distance with $\mathbf{y}$, i.e.:

$$\hat{\mathbf{x}} = \underset{\mathbf{x}\in\mathcal{C}_{\rm CTP}}{\arg\min} ||\mathbf{x}-\mathbf{y}||_2^2. \tag{5}$$

The ML decoder minimizes the FER, i.e., the probability of a codeword error, in AWGN. The decoding rule of (5) can be realized by serial list Viterbi decoding (SLVD) [29]. SLVD first finds the most likely path in tail-biting trellis $\mathcal{T}$. If the constellation point sequence corresponding to this path is not a codeword in $\mathcal{C}_{CTP}$, then SLVD is used again to find the next most likely path. If a path belongs to the sub-trellis $\mathcal{T}_i$, the trellis-tree algorithm (TTA) [30] for $\mathcal{T}_i$ is used for tracing back that path.

The ML decoding complexity can be decomposed into two parts. First, the initialization step calculates the metrics of local best paths in each of 2^ν sub-trellises. Second, if a path in $\mathcal{T}_i$ needs to be traced back, a data set of TTA for $\mathcal{T}_i$ needs to be constructed and maintained [30].

2) β-States Decoder: One solution to reduce the complexity of ML decoder is to consider only a subset of 2^ν states as the possible start/end states. We denote the subset by $\tilde{\mathcal{V}} \subseteq \mathcal{V}$ and the cardinality of $\tilde{\mathcal{V}}$ by $|\tilde{\mathcal{V}}|$. In this paper, we refer to a β-States decoder as a decoder that considers β states as start/end states, i.e., $|\tilde{\mathcal{V}}| = \beta$. Let $v(\mathbf{x})$ be the TBCC initial state of the codeword $\mathbf{x}$. The β-States decoder solves the following problem:

$$\hat{\mathbf{x}} = \underset{\substack{\mathbf{x}\in\mathcal{C}_{\rm CTP}\\ v(\mathbf{x})\in\tilde{\mathcal{V}}}}{\arg\min} ||\mathbf{x}-\mathbf{y}||_2^2. \tag{6}$$

The set $\tilde{\mathcal{V}}$ is identified using one iteration of the wrap-around Viterbi algorithm (WAVA) [31].

3) Automorphism Ensemble (AE) Decoder: Ensemble decoding algorithms [26] employ M parallel independent and identical sub-optimal decoders, with each proposing a codeword estimate. From among these M proposed codewords, the ensemble decoder selects the most likely candidate as the decoder output [26]. One category of ensemble decoding utilizes automorphism groups. An automorphism group is a set of permutations such that the permuted sequence of any codeword is still a codeword. When an automorphism group of the codes is known, identical constituent decoders decoding permuted versions of the channel output may be used, yielding the so-called Automorphism Ensemble (AE) decoding [26].

The cyclic shifts δ_i, $i = 0, ..., n-1$, are elements of an automorphism group of the TBCC, where δ_i indicates the cyclic shift of a sequence by i positions. Hence, as illustrated in Fig. 3, an AE decoder for the CRC-TCM-PAS system is constructed by employing M parallel β-States decoders for the channel observations that are cyclic-shifted by $\{\delta_{i_1}, \ldots, \delta_{i_M}\}$. The i^{th} β-States decoder either provides a shifted estimation candidate or declares an erasure. The final decoding result of the AE decoder is the candidate that has the smallest Euclidean distance from the channel observation. We denote an AE decoder with M parallel decoders with cyclic shifts $\{i_1, \ldots, i_M\}$, where each decoder utilizes β starting states obtained by WAVA as the decoder AED(M, β). In this paper, the cyclic shifts $\{i_1, \ldots, i_M\}$ are uniformly sampled from $\{0, \ldots, n-1\}$.

The M independent β-States decoders of AED(M, β) can be run in parallel, so the AED(M, β) has the same time complexity with a single β-States decoder but provides more potential codewords. However, the AED(M, β) requires more hardware resources than a single β-States decoder.

IV. Channel Input Distribution of CRC-TCM-PAS System

This section proves that the distribution of the channel input X of the CRC-TCM-PAS system is symmetric, i.e., $P_X(x) = P_X(-x)$ for $x \in \mathcal{X}$, where $\mathcal{X}$ is the PAM constellation set. We begin the proof with a theorem that shows the CRC check bits in the CRC-TCM-PAS system are asymptotically uniform, even though the input bits of the CRC encoder are not.

A. Uniformity of CRC bits

Denote the random variable that represents a DM output symbol by $\bar{A}$ with PMF $P(\bar{A})$. Because the cardinality of output symbol set is 2^{k_0}, $\bar{A}$ can be represented by k_0 bits, which are denoted by B_i, $i = 0, .., k_0 - 1$. Since $\bar{A}$ is not uniform, B_i, $i = 0, ..., k_0 - 1$, may have different

distributions. Let $a \in \mathcal{A}$ be a realization of $\bar{A}$, and let $\mathbf{b}(a) = [b_{k_0-1}(a), \ldots, b_1(a),\ b_0(a)] \in \mathbb{F}_2^{k_0}$ be the binary representation of a. The PMF of B_i is calculated by:

$$P_{B_i}(b) = \sum_{a=0}^{|\mathcal{A}|-1} P_{\bar{A}}(a)\mathbb{1}\left(b_i(a) = b\right), \tag{7}$$

$b = 0, 1,\ i = 0, 1, ..., k_0 - 1$. $\mathbb{1}(\cdot)$ is the indicator function. As shown in Fig. 1, the binary converter maps a length-l symbol sequence to a length-$k_0 l$ binary sequence. Let $G^{k_0 l} = [G_0, \ldots, G_{k_0 l-1}]$ be the random vector representing the binary sequence. Assume that the DM generates i.i.d. symbols, the G_i's that correspond to the same symbol bit position have the same distribution, i.e.:

$$P(G_i) = P(B_{i \pmod{k_0}}),\ i = 0, \ldots, k_0 l - 1. \tag{8}$$

Let $\mathbf{g} \in \mathbb{F}_2^{k_0 l}$ be a realization of $G^{k_0 l}$, and denote the polynomial form of $\mathbf{g}$ by $g(x) = \sum_{i=0}^{k_0 l-1} g_i x^i$. An m-bit CRC is specified by a degree-m binary polynomial $p(x) = \sum_{i=0}^{m} p_i x^i$. Let the polynomial form of the output of the CRC encoder be $h(x) = \sum_{i=0}^{k_0 l+m-1} h_i x^i$. $h(x)$ is calculated by $h(x) = x^m g(x) + x^m g(x) \pmod{p(x)}$. The following theorem proves that the CRC check bits, h_i, $i = 0, \ldots, m-1$, can be arbitrarily close to be equally likely, with a proper choice of l.

Theorem 1. *For a length-l random vector A^l whose elements A_i, $i = 0, \ldots, l-1$, are i.i.d. random variables with alphabet $|\mathcal{A}| = \{0, 1, 2, \ldots, 2^{k_0} - 1\}$ and distribution $P(A)$. Let $G^{k_0 l}$ be the binary representation of A^l and $H^{k_0 l+m}$ be the CRC output sequence by encoding $G^{k_0 l}$ with some degree-m CRC polynomial $p(x)$. For any $0 < \epsilon < 0.5$, there exists an l such that*

$$|P_{H_i}(0) - 0.5| < \epsilon,\ i = 0, 1, \ldots, m-1.$$

Please see the proof in [1]. Note that Theorem 1 can be generalized to any systematic linear block code, and it validates the uniform check bit assumption in [10].

B. Symmetry of Channel Input Distribution

Consider a length-n, rate-$\frac{k_0}{k_0+1}$, systematic, and recursive TBCC with ν memory elements. Denote the input symbol in stage t by $u_t \in \mathcal{U}$, $t = 0, ..., n-1$, and denote the state at time instant t by $v_t \in \mathcal{V}$, $t = 0, \ldots, n$. Let $\mathbf{u}_t \in \mathbb{F}_2^{k_0 \times 1}$ and $\mathbf{v}_t \in \mathbb{F}_2^{\nu \times 1}$ be the binary representation of u_t and v_t, respectively. Based on the state-space representation of convolutional code [32], [33], $\mathbf{v}_{t+1}$ is a function of $\mathbf{v_t}$ and $\mathbf{u_t}$, i.e., $\mathbf{v}_{t+1} = \mathbf{A}\mathbf{v}_t + \mathbf{B}\mathbf{u}_t$, where $\mathbf{A} \in \mathbb{F}_2^{\nu \times \nu}$ and $\mathbf{B} \in \mathbb{F}_2^{\nu \times k_0}$. The initial state $\mathbf{v}_0$ of a recursive TBCC codeword can be determined by the following equation:

$$\mathbf{v}_0 = (\mathbf{A}^n + \mathbf{I}_\nu)^{-1} \mathbf{v}_n^{[zs]}, \tag{9}$$

where $\mathbf{I}_\nu$ is a size ν identity matrix and $\mathbf{A}^n + \mathbf{I}_\nu$ is an invertible matrix [32]. The term $\mathbf{v}_N^{[zs]}$ is referred to as zero-state solution and is the final state by encoding the dataword with initial state 0. The encoding of tail-biting convolutional code has two steps:

1) Run encoding process first time by setting $v_0 = 0$ and record $v_n^{[zs]}$.
2) Run encoding process second time by setting v_0 using (9) and generate output symbols.

Therefore, in order to study the distribution of the output symbols of a recursive TBCC, we need to know the distribution of $v_n^{[zs]}$ by analyzing the first encoding process.

For the CRC-TCM-PAS system, the data frames, i.e., input symbols, of TBCC are the outputs of CRC encoder. Because the CRC encoder is systematic, the first $n - \frac{m}{k_0}$ input symbols of TBCC have DM output symbol distribution $P(\bar{A})$. Based on Theorem 1, the last $\frac{m}{k_0}$ input symbols have uniform distributions. This subsection uses state-space representation of convolution code in [32], [33] to analyze the PMF of the state in time instant t, V_t. The PMF of V_t, is calculated by:

$$P_{V_t}(v_t) = \sum_{v_{t-1} \in \mathcal{V}} P(v_{t-1}) \sum_{(v_{t-1}, o_t, v_t) \in \mathcal{E}} P(o_t, v_t | v_{t-1}). \tag{10}$$

Let $u_t = g^{-1}(v_{t-1}, o_t, v_t) \in \mathcal{U}$ be the input symbol that associates to the edge (v_{t-1}, o_t, v_t). Hence, $P(o_t, v_t | v_{t-1}) = P_{U_t}\left(g^{-1}(v_{t-1}, o_t, v_t)\right)$. If the convolution code is systematic, the input corresponded to (v_{t-1}, o_t, v_t) can be solely determined by
$ccoutputrealize_t$, we use $g^{-1}(o_t) = g^{-1}(v_{t-1}, o_t, v_t)$ as a simplification. Define the matrix $\mathbf{C}_{t-1} \in \mathbb{R}^{|\mathcal{V}| \times |\mathcal{V}|}$ as follows:

$$\mathbf{C}_{t-1}(v_t, v_{t-1}) = P(v_t | v_{t-1}) = \sum_{(v_{t-1}, o_t, v_t) \in \mathcal{E}} P(o_t, v_t | v_{t-1}). \tag{11}$$

Let $\mathbf{p_t} = [P_{V_t}(0) \ldots P_{V_t}(2^\nu - 1)]^T$, (10) can be rewritten as:

$$\mathbf{p}_t = \mathbf{C}_{t-1}\mathbf{p}_{t-1} = \left(\prod_{i=0}^{t-1} \mathbf{C}_i\right)\mathbf{p}_0,\ t = 1, 2, ..., n. \tag{12}$$

(11) implies that $\mathbf{C}_{t-1}$ is a left stochastic matrix, i.e., each column in $\mathbf{C}_{t-1}$ is a probability vector. Moreover, $\mathbf{C}_{t-1}$ is also right stochastic, meaning that each row has a sum of 1. To see this, for the trellis of a convolutional code, for each $v_t \in \mathcal{V}$, there are 2^{k_0} edges that connect v_t and each edge associates a distinct input in $\mathcal{U}$. As a result, $\mathbf{C}_{t-1}$ is a doubly stochastic matrix.

Theorem 2. *For an (γ_0, k_0, ν) convolutional code with any initial state distribution $P(V_0)$, if the data frames are i.i.d. random variables with PMF $P(U)$ and $P_U(u) > 0$ for any $u \in \mathcal{U}$. Let V_t be the state at time instant t, then the random sequence $V_0, V_1, \ldots$ converges in distribution to a uniform random variable V_{uni}, i.e., $V_t \xrightarrow{d} V_{\text{uni}}$.*

Proof. Because all the data frames have the same distribution, it has $\mathbf{C}_t = \mathbf{C}$. Hence, (12) can be rewritten as $\mathbf{p}_t = \mathbf{C}^t \mathbf{p}_0$. $\mathbf{C}$ is not only a doubly stochastic matrix but also a regular matrix. For a convolutional code, any state $v_i \in \mathcal{V}$ can always reach any state $v_j \in \mathcal{V}$ with a finite-length path. $\mathbf{C}$ retains this property, because $P_U(u) > 0$, for any $u \in \mathcal{U}$. As a result, $\mathbf{C}$ is regular. Based on Perron-Frobenius theorem [34], the non-negative and regular matrix $\mathbf{C}$ has the following properties:

1) $\mathbf{C}$ has $\lambda_1 = 1$ as an eigenvalue of multiplicity 1, and the normalized right eigenvector corresponded to eigenvalue 1 is $\mathbf{q}^* = \left[\frac{1}{\sqrt{2^\nu}} \ \frac{1}{\sqrt{2^\nu}} \dots \frac{1}{\sqrt{2^\nu}}\right]^T$.
2) For all other eigenvalues λ_j, $j = 2, ..., q$, it has $|\lambda_j|$ is *strictly* smaller than 1, i.e., $|\lambda_j| < 1$.

Let $\mathbf{J} = \mathbf{Q}^{-1}\mathbf{C}\mathbf{Q}$ be the Jordan canonical form of $\mathbf{C}$. Based on Perron-Frobenius theorem, $\mathbf{J} = \text{diag}(1, \mathbf{J}_2, \dots, \mathbf{J}_q)$, where $\mathbf{J}_2, \dots, \mathbf{J}_q$ are Jordan block matrices that correspond to eigenvalues $\lambda_2, \dots, \lambda_q$, respectively. Let $\mathbf{Q} = [\mathbf{q}_1 \dots \mathbf{q}_{2^\nu}]$ and, $\mathbf{q}_1$ is the eigenvector associated to eigenvalue 1, $\mathbf{q}_1 = \alpha\mathbf{q}_1^*$, $\alpha \in \mathbb{R}$. Let $\mathbf{p}_0 = \sum_{i=1}^{2^\nu} c_i\mathbf{q}_i = \mathbf{Q}\mathbf{c}$, it has $\mathbf{p}_t = \mathbf{C}^t\mathbf{p}_0 = \mathbf{Q}\mathbf{J}^t\mathbf{c}$. Because $\lim_{t\to\infty} \mathbf{J}_i = \mathbf{0}$ for $j = 2, \dots, 2^\nu$, it has $\lim_{t\to\infty} \mathbf{p}_t = c_1\alpha\mathbf{q}_1^* = \left[\frac{1}{2^\nu} \dots \frac{1}{2^\nu}\right]^T$. □

The following example illustrates that a moderate t is sufficient to let V_t be uniform.

Example 1. *Consider the (3,2,3) convolution code shown in Fig. 1. Let the initial state be 0 and* $P(U) = (0.5742, 0.3188, 0.01642, 0.09048)$. *When* $t = 12$, $|P_{V_{12}}(v) - \frac{1}{8}| < 10^{-4}$, $v = 0, \dots, 7$.

Besides, if the state distribution at time t is uniform, the state distribution at time $t+1$ is also uniform, no matter what $P(U_t)$ is. Hence, the zero-state solution, as well as the initial state of TBCC, have a uniform distribution. As a result, the states at all $n+1$ time instants in second encoding process have uniform distribution.

Now, we show that if the state at time instant t is uniform, then the (k_0+1, k_0, ν) systematic recursive TBCC generates an equally likely parity check bit in stage t. First of all, the following theorem gives that distribution of output symbol in stage t.

Theorem 3. *Consider a* (k_0+1, k_0, ν) *systematic recursive convolutional code that is defined by state set* $\mathcal{V}$, *edge set* $\mathcal{E}$, *input set* $\mathcal{U}$, *and output set* $\mathcal{O}$. *If the state distribution at time instant* t *is uniform, i.e.,* $\mathbf{p}_t = \left[\frac{1}{2^\nu} \frac{1}{2^\nu} \dots \frac{1}{2^\nu}\right]^T$, *then the output symbol distribution in stage* t, $P_{O_t}(o_t) = \frac{1}{2}P_{U_t}\left(g^{-1}(o_t)\right)$, $\forall o_t \in \mathcal{O}$.

Proof. Define matrix $\mathbf{D}_t \in \mathbb{R}^{|\mathcal{O}|\times|\mathcal{V}|}$ with $\mathbf{D}_t(o_t, v_{t-1}) = P(o_t|v_{t-1})$, where $o_t \in \mathcal{O}$ and $v_{t-1} \in \mathcal{V}$. Define $\mathbf{q}_t = [P_{O_t}(0) \dots P_{O_t}(|\mathcal{O}|-1)]^T$. $\mathbf{q}_t$ can be calculated by $\mathbf{q}_t = \mathbf{D}_{t-1}\mathbf{p}_t$.

Because the TBCC is systematic, $\mathbf{D}_t(o_t, v_{t-1}) = P_{U_t}(g^{-1}(o_t))$. Hence, one property of $\mathbf{D}_t$ is that the non-zero elements in each row have the same value.

The other property is that $\mathbf{D}_t$ contains $2^{\nu-1}$ non-zero elements for each row, i.e., given any output $o_t \in \mathcal{O}$, there are only $2^{\nu-1}$ possible states from which o_t can be generated. This is because for a rate-$\frac{k_0}{k_0+1}$, systematic, recursive convolution code, the register adjacent to the output is determined by o_t, hence the freedom of v_{t-1} is reduced by 1. Based on the two properties of $\mathbf{D}$, for any $o_t \in \mathcal{O}$, it has: $P_{O_t}(o_t) = \sum_{i=1}^{2^\nu} \mathbf{D}(l, i)P_{V_t}(i) = \frac{1}{2}P_{U_t}(g^{-1}(o_t))$. □

Theorem 3 implies that, if the state distribution at time t is uniform, then the parity bit generated by the convolutional code at stage t is uniform. Because the sign value of the channel input symbol at stage t, X_t, is determined by parity bit, it has $P_{X_t}(x) = P_{X_t}(-x)$, for $x \in \mathcal{X}$.

Because the states of each time instant of TBCC have uniform distribution, the channel inputs in each stage have symmetric distributions. Besides, the magnitude distributions of first $n - \frac{m}{k_0}$ and last $\frac{m}{k_0}$ channel inputs follow $P(\bar{A})$ and uniform distribution, respectively.

V. FER Upper Bound for CRC-TCM-PAS System

In this section, we derive the FER upper bound for the CRC-TCM-PAS system with the specified CC, CRC, and an ideal distribution matcher that generates length-l symbol sequences with the desired distribution $P(\hat{A}^l)$. The upper bound is computed using the generating function of an equivalent convolutional code whose error events correspond exactly to the undetectable error events of the concatenation of the original CRC and CC.

A. Equivalent Code for CRC-Aided Convolutional Code

As shown in Fig. 1, the binary representation of the symbol sequence generated by a distribution matcher is encoded by a CRC and a TBCC serially. We begin our analysis by replacing the CRC and convolutional encoder with a single convolutional encoder whose input is the quotient of dividing the CRC codeword by the CRC polynomial.

Let $\mathbf{h}$ be a length-$(\tilde{l}+m)$ CRC codeword with polynomial form $h(x) = \sum_{t=0}^{\tilde{l}+m+1} h_t x^t$. Based on the notation in Fig. 1, $\tilde{l} = k_0 l$. For a rate-$\frac{k_0}{k_0+1}$ convolutional code, there are k_0 input branches. Let the input of the i^{th} branch be $\mathbf{h}^{(i)}$, and let the corresponding polynomial be $h^{(i)}(x)$. $\mathbf{h}^{(i)} = [h_i \ h_{k_0 i} \dots h_{\tilde{l}+m-k_0+i}]$ is obtained by sampling $\mathbf{h}$ every k_0 positions starting from i^{th} position, and $h^{(i)}(x) = \sum_{t=0}^{(\tilde{l}+m)/k_0-1} h_{k_0 t+i}x^t$, $i = 0, \dots, k_0-1$.

Let $\mathbf{q}$ be the quotient of dividing the CRC output by the CRC polynomial. The polynomial form of $\mathbf{q}$, $q(x)$, is calculated by $q(x) := h(x)/p(x)$.

Analogously to $\mathbf{h}^{(i)}$, let $\mathbf{q}^{(i)}$ denote the sequence by sampling $\mathbf{q}$ every k_0 positions starting from i^{th} position. We refer to the polynomial vector $\mathbf{h}_{k_0}(x) = [h^{(0)}(x) \dots h^{(k_0-1)}(x)]$ and $\mathbf{q}_{k_0}(x) = [q^{(0)}(x) \dots q^{(k_0-1)}(x)]$ as k_0-*split* polynomial vector of $h(x)$ and $q(x)$, respectively.

Theorem 4. *Consider an* m*-bit CRC encoder which is specified by an* m*-degree polynomial* $p(x)$. *Let the number of input bits be* $\tilde{l}$. *Let* k_0 *be an integer that divides* $m + \tilde{l}$. *Then for any codeword polynomial* $h(x)$, *its* k_0*-split polynomial vector,* $\mathbf{h}_{k_0}(x)$ *can be calculated by* $\mathbf{h}_{k_0}(x) = \mathbf{q}_{k_0}(x)\mathbf{P}_{\text{eq}}(x)$. *where* $\mathbf{q}_{k_0}(x)$ *is the* k_0*-split polynomial vector of* $q(x) = h(x)/p(x)$ *and* $\mathbf{P}_{\text{eq}}(x) \in \mathbb{F}_2[x]^{k_0\times k_0}$ *is a* $k_0 \times k_0$ *square binary polynomial matrix.*

Proof. Based on the relationship $h(x) = p(x)q(x)$, the t^{th} bit of $\mathbf{h}^j$, $h_t^{(j)}$ is calculated by:

$$h_t^{(j)} = h_{k_0 t+j} = \sum_{s=0}^{m} q_{k_0 t+j-s} p_s \tag{13}$$

$$= \sum_{\ell=0}^{m/k_0-1} \sum_{i=0}^{j} q_{k_0(t-\ell)+i} p_{k_0\ell+j-i} + \sum_{\ell=1}^{m/k_0} \sum_{i=j+1}^{k_0-1} q_{k_0(t-\ell)+i} p_{k_0\ell+j-i} + q_{k_0 t+j-m} p_m \tag{14}$$

Let $p_t^{(i)} = p_{kt+i}$, $h_t^{(j)}$ can be rewritten as:

$$h_t^{(j)} = \sum_{i=0}^{j} \sum_{\ell=0}^{m/k_0-\mathbb{1}(i\neq j)} q_{t-\ell}^{(i)} p_\ell^{(j-i)} + \sum_{i=j+1}^{k_0-1} \sum_{\ell=0}^{m/k_0-1} q_{t-\ell-1}^{(i)} p_{\ell+1}^{(j-i+k_0)}. \tag{15}$$

Define $p^{(i)}(x) = \sum_{t=0}^{m/k_0-\mathbb{1}(i=0)} p_{k_0 t+i} x^t$. The $h^{(j)}(x)$ can be calculated by:

$$h^{(j)}(x) = \sum_{i=0}^{j} q^{(i)}(x) p^{(j-i)}(x) + \sum_{i=j+1}^{k_0-1} x q^{(i)}(x) p^{(j-i+k_0)}(x). \tag{16}$$

(16) implies that, by choosing the polynomial of i^{th} row and j^{th} column of $\mathbf{P}_{\text{eq}}(x)$ as:

$$\mathbf{P}_{\text{eq}}(x)_{i,j} = p^{(j-i)}(x)\mathbb{1}(i \leq j) + x p^{(j-i+k_0)}(x)\mathbb{1}(i > j), \tag{17}$$

it has $\mathbf{h}_{\text{split}}(x) = \mathbf{q}_{\text{split}}(x)\mathbf{P}_{\text{eq}}(x)$. □

As a result, the concatenation of a CRC with generator polynomial $p(x)$ and a rate-$\frac{k_0}{k_0+1}$ convolutional code with generator matrix $\mathbf{G}(x)$ is equivalent to a convolutional code with generator matrix $\mathbf{G}_{\text{eq}}(x)$, which is defined as follows:

$$\mathbf{G}_{\text{eq}}(x) = \mathbf{P}_{\text{eq}}(x)\mathbf{G}(x). \tag{18}$$

The error events of the equivalent convolutional code correspond exactly to the error events of the original concatenation of CRC and convolutional code. Because the concatenation of a CRC expurgates the original TBCC by removing the codewords whose corresponding messages do not pass the CRC, the remaining codewords all meet the tail-biting condition so that the equivalent convolutional code is still tail-biting.

B. FER Upper Bound

This subsection bounds the FER for the CRC-TCM-PAS system. Based on the analysis in the previous subsection, the CRC-aided TBCC can be replaced by an equivalent TBCC with the generator matrix given in (18). The final computation of FER requires the output symbol distributions. For the purposes of this analysis, we assume a distribution matcher that generates l i.i.d. symbols with the target symbol distribution $P(A)$. After the distribution matcher, $n-l$ CRC symbols are appended to the sequence. Based on Theorem 1, these CRC symbols should be approximated as having a uniform distribution rather than $P(A)$. The output symbol distributions for the analyzed system of the equivalent TBCC with the generator matrix given in (18) with our idealized distribution matcher are thus l output symbols distributed according to $P(A)$ and $n-l$ output symbols distributed according to a uniform distribution.

Let $\mathcal{C}_{\text{T}} \subset \mathcal{X}^n$ be the codebook of TCM. Let $\mathbf{x}_c \in \mathcal{C}_{\text{T}}$ be the transmitted codeword, and let $\mathbf{y}$ be the channel observation over AWGN channel. Let $\varepsilon_{\mathbf{x}_c}$ denote the event that, given observation $\mathbf{y}$, an ML decoder selects $\hat{\mathbf{x}} \neq \mathbf{x}_c$. Let $e_{\mathbf{x}_c,\mathbf{x}_e}$ denote the event that, given $\mathbf{y}$, codeword $\mathbf{x}_e$ is more likely than codeword $\mathbf{x}_c$. The FER of CRC-TCM-PAS transmission system P_e is upper bounded by the union bound: $P_e \leq \sum_{\mathbf{x}_c\in\mathcal{C}_{\text{T}}} P(X^n = \mathbf{x}_c) \sum_{\substack{\mathbf{x}_e\in\mathcal{C}_{\text{T}} \\ \mathbf{x}_e\neq\mathbf{x}_c}} P\left(e_{\mathbf{x}_c,\mathbf{x}_e}\right)$. The probability $P\left(e_{\mathbf{x}_c,\mathbf{x}_e}\right)$ is referred as the pairwise error probability (PEP).

Because $P(X^n)$ is non-uniform[1], choosing the codeword that has the smallest Euclidean distance with the channel observation is no longer optimal. Let $\mathbf{u}_c, \mathbf{u}_e$ denote the convolutional inputs corresponding to outputs $\mathbf{x}_c, \mathbf{x}_e$, $e_{\mathbf{x}_c,\mathbf{x}_e}$ happens if $P_{X^n|Y^n}(\mathbf{x}_e|\mathbf{y}) > P_{X^n|Y^n}(\mathbf{x}_c|\mathbf{y})$, this condition is equivalent to:

$$2\langle \mathbf{y}-\mathbf{x}_c, \mathbf{x}_e-\mathbf{x}_c\rangle - ||\mathbf{x}_c-\mathbf{x}_e||_2^2 > 2\sigma^2 \log\left(\frac{P_{X^n}(\mathbf{x}_c)}{P_{X^n}(\mathbf{x}_e)}\right). \tag{19}$$

$\langle\cdot,\cdot\rangle$ represents the inner product and $||\cdot||_2$ represents l^2-norm. Define $z' = \frac{\langle \mathbf{y}-\mathbf{x}_c, \mathbf{x}_e-\mathbf{x}_c\rangle}{||\mathbf{x}_c-\mathbf{x}_e||_2}$, it can be proved that $z' \sim \mathcal{N}(0,\sigma^2)$. Manipulating (19) reveals that $e_{\mathbf{x}_c,\mathbf{x}_e}$ occurs if the following inequality is satisfied:

$$z' > \frac{1}{2}||\mathbf{x}_c-\mathbf{x}_e||_2 + \frac{\sigma^2}{||\mathbf{x}_c-\mathbf{x}_e||_2}\log\left(\frac{P_{X^n}(\mathbf{x}_c)}{P_{X^n}(\mathbf{x}_e)}\right) \tag{20}$$

$$\triangleq \frac{1}{2}d(\mathbf{x}_c,\mathbf{x}_e). \tag{21}$$

Note that d is not a metric as $d(\mathbf{x}_c,\mathbf{x}_e) \neq d(\mathbf{x}_e,\mathbf{x}_c)$.

Applying (20) yields $P\left(e_{\mathbf{x}_c,\mathbf{x}_e}\right) = Q\left(\frac{\sqrt{d^2(\mathbf{x}_c,\mathbf{x}_e)}}{2\sigma}\right)$, where $d^2(\mathbf{x}_c,\mathbf{x}_e)$ is calculated by:

$$d^2(\mathbf{x}_c,\mathbf{x}_e) = ||\mathbf{x}_c-\mathbf{x}_e||_2^2 + 4\sigma^2\log\left(\frac{P_{X^n}(\mathbf{x}_c)}{P_{X^n}(\mathbf{x}_e)}\right) + \left(\frac{2\sigma^2}{||\mathbf{x}_c-\mathbf{x}_e||_2}\log\left(\frac{P_{X^n}(\mathbf{x}_c)}{P_{X^n}(\mathbf{x}_e)}\right)\right)^2. \tag{22}$$

Define $d_{\text{prox}}^2(\mathbf{x}_c,\mathbf{x}_e)$ by neglecting the last squared term in (22), i.e.:

$$d_{\text{prox}}^2(\mathbf{x}_c,\mathbf{x}_e) = ||\mathbf{x}_c-\mathbf{x}_e||_2^2 + 4\sigma^2\log\left(\frac{P_{X^n}(\mathbf{x}_c)}{P_{X^n}(\mathbf{x}_e)}\right). \tag{23}$$

[1]In a practical CRC-TCM-PAS system, the codewords are uniform, specifically, $P_{X^n}(\mathbf{x}) = \frac{1}{2^k}\mathbb{1}(\mathbf{x}\in\mathcal{X}_{\text{CTP}})$.

Because $d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e) \leq d^2(\mathbf{x}_c, \mathbf{x}_e)$, the PEP $P(e_{\mathbf{x}_c,\mathbf{x}_e})$ is upper bounded by:

$$P(e_{\mathbf{x}_c,\mathbf{x}_e}) = Q\left(\frac{\sqrt{d^2(\mathbf{x}_c, \mathbf{x}_e)}}{2\sigma}\right) \leq Q\left(\frac{\sqrt{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)}}{2\sigma}\right). \tag{24}$$

Hence, P_e is further bounded by:

$$P_e \leq \sum_{\mathbf{x}_c \in \mathcal{C}_{\text{T}}} P(X^n = \mathbf{x}_c) \sum_{\substack{\mathbf{x}_e \in \mathcal{C}_{\text{T}} \\ \mathbf{x}_e \neq \mathbf{x}_c}} Q\left(\frac{\sqrt{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)}}{2\sigma}\right). \tag{25}$$

Based on the ideal DM assumption and our analysis of CRC and TBCC encoding, the output symbols of the CRC-TCM-PAS system are independent of each other. Hence, $d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e) = \sum_{i=1}^{n} d^2_{\text{prox}}(x_{c,i}, x_{e,i})$, where $x_{c,i}$ and $x_{e,i}$ are the i^{th} element in $\mathbf{x}_c$ and $\mathbf{x}_e$, respectively, and $d^2_{\text{prox}}(x_{c,i}, x_{e,i}) = (x_{c,i} - x_{e,i})^2 + 4\sigma^2 \log \frac{P_{X_i}(x_{c,i})}{P_{X_i}(x_{e,i})}$.

C. Generating Function with State-Reduction Method

This subsection derives the generating function of non-uniform-input TCM using Biglieri's product state method [35], with state-reduction method as described in [36]. The product state diagram [35] is built by replacing each state in the error state diagram with a complete encoder state diagram. Hence, for a convolutional code that has ν memory elements, there are totally $2^{2\nu}$ states in the product state diagram. Wesel in [36] reduces the total number of states by proposing an "equivalence-class encoder" with ν_x memory elements. Because $\nu_x < \nu$, the state-reduction method requires fewer states than the product state diagram.

For an equivalence-class encoder, denote the set of output by $\mathcal{O}_{\text{eq}}$. Let $q \in \mathcal{O}_{\text{eq}}$ be an output of the equivalent-class encoder. Let $e_o \in \mathcal{O}$ be a symbol error. As a reminder, $\mathcal{O}$ is the set of TBCC output symbols. Let x_q, x_{qe_o} be any constellation point that belongs to equivalent class q and the constellation point that x_q moves to because of e_o. We define $d^2_{\text{prox}}(q, e_o)$ as follows:

$$d^2_{\text{prox}}(q, e_o) = (x_q - x_{qe_o})^2 + 4\sigma^2 \log \frac{P_X(x_q)}{P_X(x_{qe_o})}. \tag{26}$$

We follow the notations in [36] to describe the state-reduced product state diagram. Denote the set of equivalence-class encoder states and the set of error states by $\mathcal{S}_q$ and $\mathcal{S}_e$, respectively. The pair $(s_q, s_e) \in \mathcal{S}^* = \mathcal{S}_q \times \mathcal{S}_e$ describes where the states "should be" if there is no error occurs, and where the state is "drifted to" because of some error event. The notation "$\times$" means Cartesian product. Let $(s_q, s_e), (s'_q, s'_e) \in \mathcal{S}^*$, we label the state transition $(s_q, s_e) \rightarrow (s'_q, s'_e)$ with $P\left(s_q \rightarrow s'_q\right) \sum_{e_o} \sum_{\tilde{q}} P\left(\tilde{q} | s_q \rightarrow s'_q\right) W^{d^2_{\text{prox}}(\tilde{q}, e_o)}$, where $s_q \rightarrow s'_q$ is the event that the state of the equivalent class encoder transits from s_q to s'_q. The first summation is over all possible symbol error e_0 due to error state diagram transition $s_e \rightarrow s'_e$, and the second summation is over all possible equivalent class q' due to equivalent-class encoder state diagram transition $s_q \rightarrow s'_q$.

Based on the channel-signal mapping rule, the constellation of TCM output is symmetric with respect to 0 and the equivalence class is determined by the systematic bits. Thus, one generator polynomial matrix of the minimal equivalent-class encoder for the rate-$\frac{k_0}{k_0+1}$, systematic TBCC in TCM is simply a size-k_0 identity matrix. Thus, by Theorem 1 in [36], it is sufficient to use the error state diagram to compute the transfer function, and the label of transition $s_e \rightarrow s'_e$ is $\sum_{e_o} \sum_{q \in \mathcal{O}_{\text{eq}}} P(q)\, W^{d^2_{\text{prox}}(q, e_o)}$. The equivalent class q of the constellation of TCM output is associated with the magnitude of the constellation point, which has either capacity-approaching distribution $P(A)$ for the first $n - l$ output symbols or uniform distribution for the last l output symbols. Define $|\mathcal{S}_e| \times |\mathcal{S}_e|$ matrices $\mathbf{G}_A(W)$ and $\mathbf{G}_{\text{uni}}(W)$ that enumerate all possible state transitions with equivalent-class PMFs of $P(A)$ and uniform distribution as follows:

$$\mathbf{G}_A(W)_{s_e, s'_e} = \sum_{e_o} \sum_{q} P_A(q) W^{d^2_{\text{prox}}(q, e_o)}, \tag{27}$$

$$\mathbf{G}_{\text{uni}}(W)_{s_e, s'_e} = \sum_{e_o} \sum_{q} \frac{1}{|\mathcal{A}|} W^{d^2_{\text{prox}}(q, e_o)}. \tag{28}$$

We define the generating function as $T_{\text{TBCC}}(W) = -1 + \sum_{i=0}^{\mathcal{S}_e} \mathbf{e}_i \mathbf{G}^l_A(W) \mathbf{G}^{n-l}_{\text{uni}}(W) \mathbf{e}_i^{\text{T}}$, where $\mathbf{e}_i$ is a length $|\mathcal{S}_e|$ indicator vector where $e_{i,j} = \mathbb{1}(j = i)$. For the TBCC, the error events must be tail-biting paths, $\mathbf{v}_i$ selects the starting/ending state of the error events.

Define the free distance, $d_{\text{free}} = \min_{\mathbf{x}_c, \mathbf{x}_e \in \mathcal{C}_{\text{T}}} d_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)$. With the inequality:

$$\begin{aligned} &Q\left(\frac{\sqrt{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)}}{2\sigma}\right) \leq \\ &Q\left(\frac{\sqrt{d^2_{\text{free}}}}{2\sigma}\right) \exp\left(\frac{d^2_{\text{free}} - d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)}{8\sigma^2}\right), \end{aligned} \tag{29}$$

P_e in (25) is further bounded by:

$$P_e \leq Q\left(\frac{\sqrt{d^2_{\text{free}}}}{2\sigma}\right) \exp\left(\frac{d^2_{\text{free}}}{8\sigma^2}\right) \times \sum_{\mathbf{x}_c \in \mathcal{C}_{\text{T}}} \sum_{\substack{\mathbf{x}_e \in \mathcal{C}_{\text{T}} \\ \mathbf{x}_e \neq \mathbf{x}_c}} \prod_{i=1}^{n} \left[\exp\left(-\frac{d^2_{\text{prox}}(x_{c,i}, x_{e,i})}{8\sigma^2}\right) P_{X_i}(x_{c,i})\right]. \tag{30}$$

Note the (29) can be proved by $Q(\sqrt{x+y}) \leq Q(\sqrt{x}) e^{-\frac{y}{2}}$, for $x, y \geq 0$. The double summation term in (30) can be rewritten as follows:

$$\sum_{\mathbf{x}_c \in \mathcal{C}_{\text{T}}} \sum_{\substack{\mathbf{x}_e \in \mathcal{C}_{\text{T}} \\ \mathbf{x}_e \neq \mathbf{x}_c}} \left[\exp\left(-\frac{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)}{8\sigma^2}\right) P_{X^n}(\mathbf{x}_c)\right], \tag{31}$$

$$= \sum_{\mathbf{x}_c \in \mathcal{C}_{\text{T}}} \sum_{\substack{\mathbf{x}_e \in \mathcal{C}_{\text{T}} \\ \mathbf{x}_e \neq \mathbf{x}_c}} \left[W^{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)} P_{X^n}(\mathbf{x}_c)\right]\Big|_{W = e^{-\frac{1}{8\sigma^2}}}, \tag{32}$$

$$= \sum_{\mathbf{x}_c, \mathbf{x}_e \in \mathcal{C}_T} \left[W^{d^2_{\text{prox}}(\mathbf{x}_c, \mathbf{x}_e)} P_{X^n}(\mathbf{x}_c)\right]\Big|_{W = e^{-\frac{1}{8\sigma^2}}} - 1, \tag{33}$$

TABLE II
OPTIMIZED CONVOLUTIONAL CODE AND CRC PAIRS. ALL THE PARAMETERS ARE OPTIMIZED WHILE SNR EQUALS 11 DB.

		$H^0(D)$	$H^1(D)$	$H^2(D)$	$p(x)$	FER bound
$\nu = 3$	Ung.	13	04	00	7	6.65e-4
$m = 2$	Opt.	13	06	00	5	5.80e-4
$\nu = 5$	Ung.	45	10	00	5	8.20e-5
$m = 2$	Opt.	43	26	00	5	6.58e-5
$\nu = 7$	Ung.	235	126	000	5	1.15e-5
$m = 2$	Opt.	211	142	000	5	8.96e-6

$$= \sum_{\substack{\mathbf{q}\in\mathcal{O}_{\text{eq}}^n \\ \mathbf{e}\in\mathcal{C}_{\text{T}}^n}} \prod_{i=1}^{n} \left[W^{d^2_{\text{prox}}(q_i,e_i)} P(q_i) \right] \Big|_{W=e^{-\frac{1}{8\sigma^2}}} - 1, \tag{34}$$

$$= \sum_{i=0}^{|\mathcal{S}_e|} \mathbf{e}_i \mathbf{G}_A^l(W) \mathbf{G}_{\text{uni}}^{n-l}(W) \mathbf{e}_i^{\text{T}} \Big|_{W=e^{-\frac{1}{8\sigma^2}}} - 1. \tag{35}$$

As a result, the FER upper bound can be calculated using the generating function by

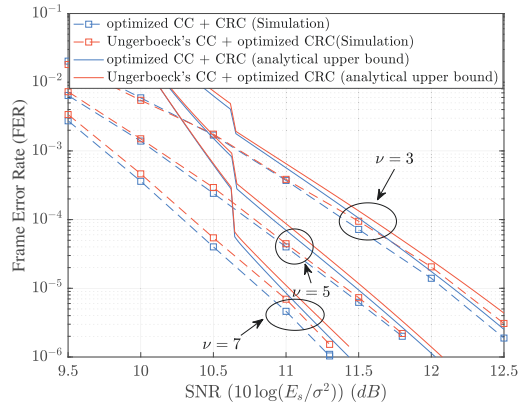
$$P_e \le Q\left(\frac{\sqrt{d^2_{\text{free}}}}{2\sigma}\right) \exp\left(\frac{d^2_{\text{free}}}{8\sigma^2}\right) T_{\text{TBCC}}\left(W = e^{-\frac{1}{8\sigma^2}}\right). \tag{36}$$

VI. SIMULATION RESULTS

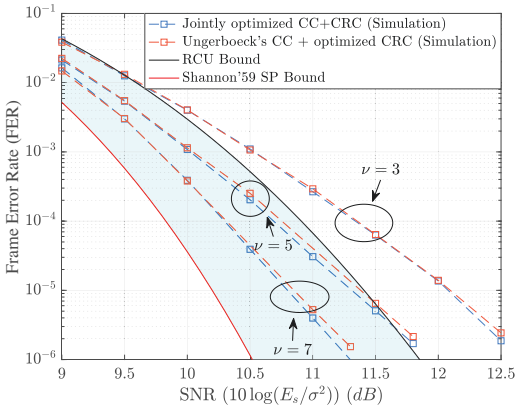
This section evaluates the performance of the CRC-TCM-PAS system over AWGN channel with different DMs and decoding methods. The CRC-TCM-PAS systems use degree-2 CRCs and rate-2/3 TBCCs. The channel inputs are equidistant 8-PAM symbols. We use the magnitudes (0.449, 1.348, 2.247, 3.146) with the PMF (0.5877, 0.3120, 0.0144, 0.0859) that is optimized for an SNR of 8 dB using a version of DAB that constrains the points to be equally spaced [9].

Fig. 4 considers a CRC-TCM-PAS system with $k = 87$ input bits and $n = 65$ output symbols. We use the FER upper bound derived in Section V as an objective function to jointly optimize the CRC and TBCC. As a baseline, we adopt the convolutional codes optimized in Ungerboeck's paper [24], and the CRC is optimized by fixing the convolutional code. We consider the number of memory elements of the convolutional code $\nu = 3$, 5, and 7. Table II lists the optimized TBCCs and CRCs in octal form. All the parameters are optimized for an SNR of 11 dB. Table II also provides the FER upper bounds at 11 dB. For the joint optimization, the optimized CRC polynomial is $p(x)$ and the optimized TBCC generator matrix is $\left[\begin{array}{cc|c} 1 & 0 & H^2(D)/H^0(D) \\ 0 & 1 & H^1(D)/H^0(D) \end{array}\right]$.

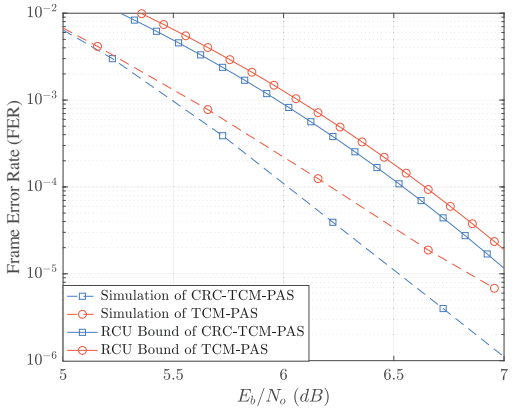
Fig. 4a presents analytical upper bounds and simuulation results that compare FERs for the optimized convolutional codes to Ungerboeck's convolutional codes for a CRC-TCM-PAS system that assumes an ideal DM. Hence, the system input "messages" are length-64 i.i.d. magnitude symbol sequences according to the PMF $P(\hat{A})$. The magnitude sequences are encoded and modulated by CRC-aided TCM to length-65 8-AM symbol sequences. Simulation results show that maximizing the FER upper bound finds slightly better convolutional codes than those in Ungerboeck's paper. Note that in both cases the FER upper bound was used to optimize the CRC polynomial.



(a)



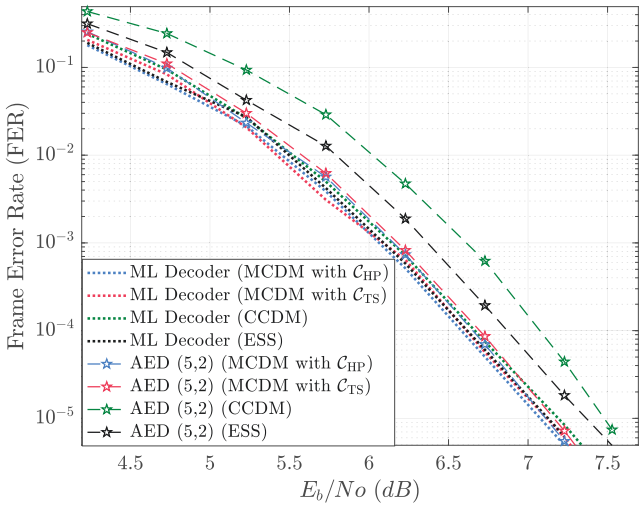
(b)



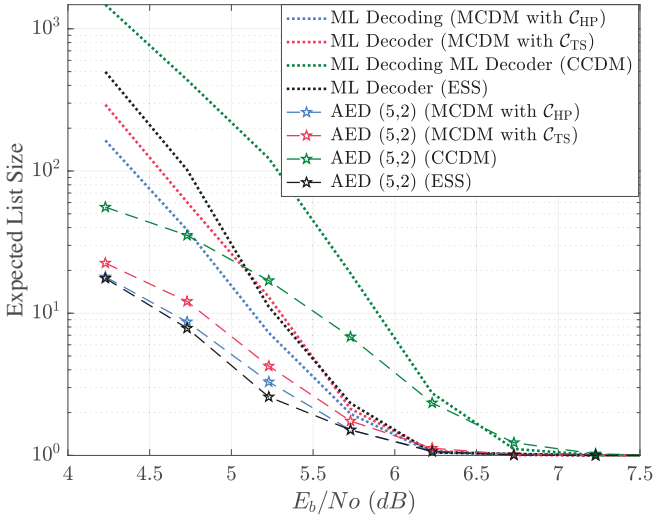
(c)

Fig. 4. (a): The upper bounds and FER simulations of the simplified CRC-TCM-PAS system with a degree-2 CRC. The simplified system takes length-64 i.i.d. 4-ary amplitude symbol sequences and generates length-65 8-AM symbol sequences. (b): The FER curves of the practical CRC-TCM-PAS transmission system that uses MCDM with $\mathcal{C}_{\text{HP}}$. This system takes 87 input bits and generates 65 8-AM symbols. (c): The FER curves and RCU bounds of the CRC-TCM-PAS system and TCM-PAS system. The gap between the two curves indicates the contribution of the 2-bit CRC.

The system uses TBCCs and CRCs from Table II. The receiver uses an ML decoder. Shannon's 1959 sphere packing (SP) bound [37] and Polyanskiy's random coding union (RCU) bound [22] are also shown. Note that the last channel input of the CRC-TCM-PAS system is uniform [1]. When calculating

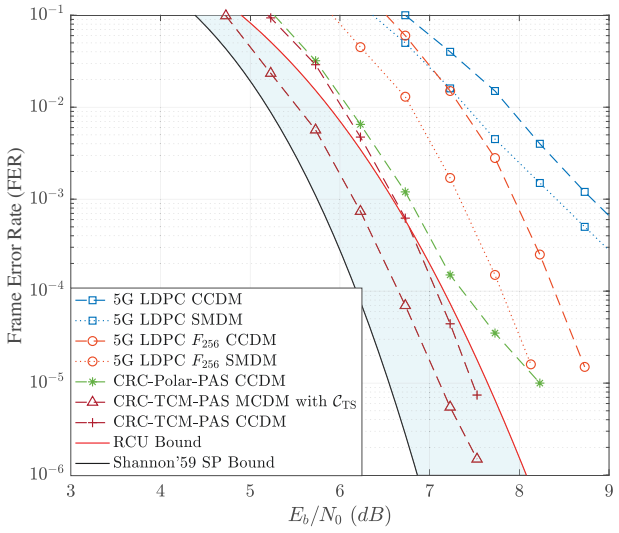


(a)

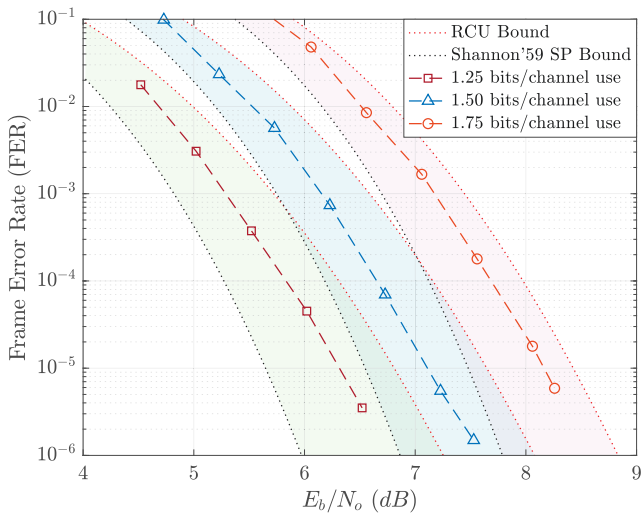


(b)

Fig. 5. The performance of a CRC-TCM-PAS transmission system with various DMs and decoders. The system takes 96 input bits and generates 64 output symbols. Fig. (a) and (b) give the FER and expected list size, respectively.



(a)



(b)

Fig. 6. (a): The CRC-TCM-PAS system utilizes CCDM and MCDM with $\mathcal{C}_{\text{TS}}$ as the DM. The decoder of the CRC-TCM-PAS system is AED(5,2) with a maximum list size of 100. (b): The FER curves of CRC-TCM-PAS systems with various rates. The CRC-TCM-PAS systems generate 64 8-AM symbols, with transmission rates of 1.25, 1.5, and 1.75 bit/real channel use, respectively.

the RCU bound, we assume all channel inputs have the DM output distribution. Fig. 4b shows that, when a practical DM is considered, the optimized convolutional codes deliver a slightly better performance than Ungerboeck's convolutional codes. When $\nu = 7$, the FER performance of the CRC-TCM-PAS system with optimized CRC and TBCC is better than RCU bound by 0.55 dB at the FER of 10^{-6}. Note that the FER curves from the simulation with the ideal DM in Fig. 4a are similar to those with the real DM in Fig. 4b.

Fig. 4c evaluates the contribution of the 2-bit CRC of the CRC-TCM-PAS system with $\nu = 7$ TBCC in Fig. 4b. We refer to the system without CRC as the TCM-PAS system. Hence, the TCM-PAS system takes 87 input bits and generates 64 8-AM symbols. The FER curve and the RCU bound for the two systems are given in Fig. 4c. It can be seen that the CRC-TCM-PAS system outperforms the TCM-PAS system by about 0.3 dB at the FER of 10^{-5}, which implies the importance of the 2-bit CRC.

Fig. 5 investigates the CRC-TCM-PAS system that uses various DMs and two decoders, ML decoding and a sub-optimal but less complex AED(5,2) decoder. The system in Fig. 5 has $k = 96$ input bits and $n = 64$ output symbols, and the transmission rate is 1.5 bits/real channel use. The CRC-aided TCM uses the jointly optimized $\nu = 7$, rate-2/3 TBCC, and the 2-bit CRC in Table II. Fig. 5a and 5b give the FER performances and expected list sizes, respectively.

We first investigate the performances of the CRC-TCM-PAS systems with various DMs and the ML decoder. The simulation results show that the four considered distribution matchers, i.e., ESS, CCDM, MCDM with $\mathcal{C}_{\text{HP}}$ and $\mathcal{C}_{\text{TS}}$ deliver similar FER performances under ML decoding. However, the

CCDM requires more list size than the other three DMs. Fig. 5 also presents the FER performance when the AED(5,2) is used. The maximum list size of all 2-States decoders in AED(5,2) is 100. As shown in Fig. 5, when AED(5,2) is used as the decoder, the CRC-TCM-PAS system with CCDM delivers the worst FER and largest expected list size. On the other hand, the CRC-TCM-PAS systems that use the MCDM with $\mathcal{C}_{\mathrm{HP}}$ and $\mathcal{C}_{\mathrm{TS}}$ deliver the near-optimal FER performance and outperform the system that uses ESS.

Fig. 6a compares the decoding performance of CRC-TCM-PAS system with other PAS systems that use various FEC codes in [2, Fig.14]. All systems have 96 input bits, and the transmission rate is 1.5 bits/real channel use. For the CRC-TCM-PAS, two distribution matchers are considered, i.e., MCDM with $\mathcal{C}_{\mathrm{TS}}$ and CCDM. The decoder uses AED(5,2) with a maximum list size of 100. The details of other PAS systems are described in [2]. The simulation results show that the CRC-TCM-PAS system with MCDM delivers the best performance and outperforms the CRC-Polar-PAS system by nearly 1dB. Since the CRC-Polar-PAS system uses CCDM as the distribution matcher, the gain of CRC-TCM-PAS over CRC-Polar-PAS can come from two factors: the choice of DM or the coded modulation scheme. As shown in Fig. 6a, with CCDM as the distribution matcher, the CRC-TCM-PAS system still outperforms the CRC-Polar-PAS system but does not perform as well as CRC-TCM-PAS with MCDM. Notably, the CRC-TCM-PAS system doesn't display the error floor of the CRC-Polar-PAS system, which shows an error floor at FER of 10^{-5}. Hence, the gap between the FER curves of the CRC-TCM-PAS with CCDM and the CRC-Polar-PAS with CCDM can be treated as the gain of CRC-TCM code over CRC-Polar code, and the gap between the FER curves of the CRC-TCM-PAS with CCDM and the MCDM can be treated as the gain of MCDM over CCDM.

The error floor seen in the CRC-Polar-PAS with CCDM could be due to a variety of factors. One factor is the sub-optimality in the decoder. Serial list Viterbi decoding of CRC-TBCC either chooses the ML codeword or reports an erasure with each growing list size. In contrast, successive cancellation list (SCL) decoding of CRC-polar codes sometimes selects non-ML codewords with a fixed list size of 32. The error floor could also be due to a CRC that is too short, not optimized for high SNR, or otherwise sub-optimal.

Fig. 6b evaluates the CRC-TCM-PAS system with various transmission rates. We design three CRC-TCM-PAS systems that take 80, 96, and 112 information bits, respectively, and generate 64 8-AM symbols. The resultant transmission rates are 1.25, 1.50, and 1.75 bits/real channel use, respectively. We design the MCDM with $\mathcal{C}_{\mathrm{HP}}$ for all three transmission rates as distribution matcher. All three transmission rates employ the $\nu = 7$ CC and the 2-bit CRC in Table II. AED(5,2) with a maximum list size of 100 is used as the decoder. Fig. 6b gives the FER curves, as well as the RCU bound and Shannon's 59 SP bound, of all three transmission rates. The simulation result shows that the FER curves for all three rates lie between the RCU and the SP bound, which indicates excellent decoding performance.

VII. Conclusion

Shannon's proof of the channel coding theorem [38] generates a random codebook that has an optimal distribution and then performs an expurgation to improve the codebook. The CRC-TCM-PAS system described in this paper follows that paradigm. The DM plays the role of random codebook generation and the selection of that TCM and CRC polynomials expurgates that code to make it stronger. While there are many recent PAS systems, CRC-TCM-PAS allows the use of the tight FER upper bound derived in this paper for a precise expurgation of the codebook produced by the DM. The TCM and CRC can be jointly selected to optimize FER performance. This also paper proposes a new multi-composition DM (MCDM), which allows codewords with different compositions. The new MCDM provides a significant benefit when decoding complexity is limited. Simulation results show that the optimized CRC-TCM-PAS system with MCDM exceeds the RCU bound for a variety of rates and outperforms the PAS systems with various FEC codes studied in [2].

References

[1] L. Wang, D. Song, F. Areces, and R. D. Wesel, "Achieving short-blocklength RCU bound via CRC list decoding of TCM with probabilistic shaping," in *2022 International Conference on Communications (ICC)*, 2022.

[2] M. C. Coşkun, G. Durisi, T. Jerkovits, G. Liva, W. Ryan, B. Stein, and F. Steiner, "Efficient error-correcting codes in the short blocklength regime," *Physical Communication*, vol. 34, pp. 66–79, 2019.

[3] R. G. Gallager, *Information theory and reliable communication*. Springer, 1968, vol. 588.

[4] G. Forney, R. Gallager, G. Lang, F. Longstaff, and S. Qureshi, "Efficient modulation for band-limited channels," *IEEE Journal on Selected Areas in Communications*, vol. 2, no. 5, pp. 632–647, 1984.

[5] G. D. Forney, "Trellis shaping," *IEEE Trans. on Info. Theory*, vol. 38, no. 2, pp. 281–300, 1992.

[6] F. Kschischang and S. Pasupathy, "Optimal nonuniform signaling for gaussian channels," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 913–929, 1993.

[7] R. Laroia, N. Farvardin, and S. A. Tretter, "On optimal shaping of multidimensional constellations," *IEEE Trans. on Info. Theory*, vol. 40, no. 4, pp. 1044–1056, 1994.

[8] C. Fragouli, R. Wesel, D. Sommer, and G. Fettweis, "Turbo codes with non-uniform constellations," in *ICC 2001. IEEE Inter. Conf. on Comm.. Conference Record (Cat. No.01CH37240)*, vol. 1, 2001, pp. 70–73 vol.1.

[9] D. Xiao, L. Wang, D. Song, and R. D. Wesel, "Finite-support capacity-approaching distributions for awgn channels," in *2020 IEEE Information Theory Workshop (ITW)*. IEEE, 2021, pp. 1–5.

[10] G. Böcherer, F. Steiner, and P. Schulte, "Bandwidth efficient and rate-matched low-density parity-check coded modulation," *IEEE Trans. on comm.*, vol. 63, no. 12, pp. 4651–4665, 2015.

[11] G. Böcherer, P. Schulte, and F. Steiner, "Probabilistic shaping and forward error correction for fiber-optic communication systems," *Journal of Lightwave Technology*, vol. 37, no. 2, pp. 230–244, 2019.

[12] P. Schulte and G. Böcherer, "Constant composition distribution matching," *IEEE Trans. on Info. Theory*, vol. 62, no. 1, pp. 430–434, 2015.

[13] R. A. Amjad and I. G. Böcherer, "Algorithms for simulation of discrete memoryless sources," Master's thesis, Technische Universität München, 2013.

[14] P. Schulte and F. Steiner, "Divergence-optimal fixed-to-fixed length distribution matching with shell mapping," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 620–623, 2019.

[15] P. Schulte, "Algorithms for distribution matching," Ph.D. dissertation, Technische Universität München, May 2020.

[16] M. Pikus and W. Xu, "Arithmetic coding based multi-composition codes for bit-level distribution matching," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[17] T. Fehenberger, D. S. Millar, T. Koike-Akino, K. Kojima, and K. Parsons, "Multiset-partition distribution matching," *IEEE Trans. on Comm.*, vol. 67, no. 3, pp. 1885–1893, 2018.

[18] E. Liang, H. Yang, D. Divsalar, and R. D. Wesel, "List-decoded tail-biting convolutional codes with distance-spectrum optimal CRCs for 5g," in *2019 IEEE Glob. Comm. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[19] H. Yang, S. V. Ranganathan, and R. D. Wesel, "Serial list viterbi decoding with CRC: Managing errors, erasures, and complexity," in *2018 IEEE Glob. Comm. Conf. (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[20] H. Yang, E. Liang, H. Yao, A. Vardy, D. Divsalar, and R. D. Wesel, "A list-decoding approach to low-complexity soft maximum-likelihood decoding of cyclic codes," in *2019 IEEE Glob. Comm. Conf. (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[21] H. Yang, E. Liang, M. Pan, and R. D. Wesel, "Crc-aided list decoding of convolutional codes in the short blocklength regime," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3744–3766, 2022.

[22] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. on Info. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[23] J. King, A. Kwon, H. Yang, W. Ryan, and R. D. Wesel, "Crc-aided list decoding of convolutional and polar codes for short messages in 5g," *arXiv preprint arXiv:2201.07843*, 2022.

[24] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. on Info. Theory*, vol. 28, no. 1, pp. 55–67, 1982.

[25] M. Pikus and W. Xu, "Arithmetic coding based multi-composition codes for bit-level distribution matching," in *2019 IEEE Wireless Comm. and Networking Conf. (WCNC)*, 2019, pp. 1–6.

[26] M. Geiselhart, M. Ebada, A. Elkelesh, J. Clausius, and S. t. Brink, "Automorphism ensemble decoding of quasi-cyclic ldpc codes by breaking graph symmetries," *arXiv preprint arXiv:2202.00287*, 2022.

[27] M. Thomas and A. T. Joy, *Elements of information theory*. Wiley-Interscience, 2006.

[28] A. Amari, S. Goossens, Y. C. Gültekin, O. Vassilieva, I. Kim, T. Ikeuchi, C. M. Okonkwo, F. M. Willems, and A. Alvarado, "Introducing enumerative sphere shaping for optical communication systems with short blocklengths," *Journal of Lightwave Technology*, vol. 37, no. 23, pp. 5926–5936, 2019.

[29] N. Seshadri and C. Sundberg, "List viterbi decoding algorithms with applications," *IEEE trans. on comm.*, vol. 42, no. 234, pp. 313–323, 1994.

[30] F. K. Soong and E.-F. Huang, "A fast tree-trellis search for finding the n-best sentence hypotheses in continuous speech recognition," *The Journal of the Acoustical Society of America*, vol. 87, no. S1, pp. S105–S106, 1990.

[31] R. Shao, S. Lin, and M. Fossorier, "Two decoding algorithms for tailbiting codes," *IEEE Trans. on Comm.*, vol. 51, no. 10, pp. 1658–1665, 2003.

[32] C. Weiß, C. Bettstetter, and S. Riedel, "Code construction and decoding of parallel concatenated tail-biting codes," *IEEE Trans. on Info. Theory*, vol. 47, no. 1, pp. 366–386, 2001.

[33] C. Fragouli and R. D. Wesel, "Convolutional codes and matrix control theory," in *Proceedings of the 7th Inte. Conf. on Advances in Comm. and Cont., Athens, Greece*. Citeseer, 1999.

[34] F. R. Gantmakher, *The Theory of Matrices, Volume 2*. American Mathematical Soc., 2000, vol. 133.

[35] E. Biglieri, "High-level modulation and coding for nonlinear satellite channels," *IEEE Trans. on Comm.*, vol. 32, no. 5, pp. 616–626, 1984.

[36] R. Wesel, "Reduced-state representations for trellis codes using constellation symmetry," *IEEE Trans. on Comm.*, vol. 52, no. 8, pp. 1302–1310, 2004.

[37] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell System Tech. Jour.*, vol. 38, no. 3, pp. 611–656, 1959.

[38] C. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.