Analysis on Tailed Distributed Arithmetic Codes for Uniform Binary Sources

Yong Fang, *Member, IEEE*, Vladimir Stankovic, *Senior Member, IEEE*, Samuel Cheng, *Senior Member, IEEE*, and En-hui Yang, *Fellow, IEEE*

Abstract

Distributed Arithmetic Coding (DAC) is a variant of Arithmetic Coding (AC) that can realize Slepian-Wolf Coding (SWC) in a nonlinear way. In the previous work, we defined Codebook Cardinality Spectrum (CCS) and Hamming Distance Spectrum (HDS) for DAC. In this paper, we make use of CCS and HDS to analyze tailed DAC, a form of DAC mapping the last few symbols of each source block onto non-overlapped intervals as traditional AC. We first derive the exact HDS formula for tailless DAC, a form of DAC mapping all symbols of each source block onto overlapped intervals, and show that the HDS formula previously given is actually an approximate version. Then the HDS formula is extended to tailed DAC. We also deduce the average codebook cardinality, which is closely related to decoding complexity, and rate loss of tailed DAC with the help of CCS. The effects of tail length are extensively analyzed. It is revealed that by increasing tail length to a value not close to the bitstream length, closely-spaced codewords within the same codebook can be removed at the cost of a higher decoding complexity and a larger rate loss. Finally, theoretical analyses are verified by experiments.

Index Terms

Distributed source coding, Slepian-Wolf coding, distributed arithmetic coding, Hamming distance spectrum, codebook cardinality spectrum.

Y. Fang is with the College of Information Engineering, Northwest A&F University, Yangling, Shaanxi 712100, China (email: yfang79@gmail.com). V. Stankovic is with the Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, UK (email: vladimir.stankovic@strath.ac.uk). S. Cheng is with the School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK (email: samuel.cheng@ou.edu). E.-H. Yang is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (email: ehyang@uwaterloo.ca). The corresponding author is Y. Fang.

I. INTRODUCTION

As a variant of *arithmetic coding* (AC) [1], [2], *distributed arithmetic coding* (DAC) [3], [4] is a nonlinear practical realization of *Slepian-Wolf coding* (SWC) [5], i.e., the lossless version of *distributed source coding* (DSC), which is traditionally solved by channel codes, e.g., turbo codes [6] and *low-density parity-check* (LDPC) codes [7]. Compared with the linear approach based on channel codes [6], [7], DAC has advantages including better adaptability to nonstationary source statistics and better performance for data blocks of short-to-medium length [3], [4]. As such, DAC may be a preferred solution, whenever data block lengths are relatively short. For example, a potential application of DAC is biometric data encryption in biometric authentication systems, because the typical length of biometric data blocks is $O(10^2)$ to $O(10^3)$, which makes DAC a better candidate for biometric data encryption than channel codes [8]. For recent advances on DAC, the reader may refer to [9], [10], [11], [12], [13], [14], [15], [16], [17].

In essence, each *distributed arithmetic* (DA) code partitions *source space*, the set of all possible *codewords*, i.e., blocks of source symbols, into a number of *codebooks*. DAC's performance is subject to two factors: (1) the distribution of *codebook cardinality*, (2) the distribution of *inner-codebook Hamming distance*. To study the distribution of DAC codebook cardinality, the concept of *codebook cardinality spectrum* (CCS) was proposed in [18], where the mathematical expression of CCS was derived to facilitate theoretical analysis and a numerical method was proposed for the practical calculation. Based on CCS, two methods were proposed to improve DAC's performance in [19]. To study the distribution of inner-codebook Hamming distance, the concept of *Hamming distance spectrum* (HDS) was proposed for DAC in [20], where a calculation method was also developed.

This paper is motivated mainly by two phenomena of DAC that are experimentally observed [3], [4]. First, different symbol mapping schemes may result in different coding efficiency. More concretely, if one maps the last few symbols of each source block onto non-overlapped intervals as traditional AC, rather than mapping all symbols onto overlapped intervals, DAC's coding efficiency will be improved to a great degree [3], [4]. We refer to the former mapping scheme as *tailed DAC*, while the latter is called *tailless DAC*. For tailed DAC, the last few symbols of each source block that are mapped onto non-overlapped intervals make up the so-called *tail*, while the preceding symbols that are mapped onto overlapped intervals make up the so-called *body*.

With breath-first decoding, the results in [3], [4] indicate the performance superiority of tailed DAC over tailless DAC. The second phenomenon is that as tail length increases, the decoding complexity of tailed DAC will go up very fast (hyper-exponentially). The two phenomena imply that tail length is an important parameter of tailed DAC that should be selected carefully to strike a balance between coding efficiency and decoding complexity.

Another motivation for this paper comes from another recent finding, namely, though the HDS calculated by equation (46) in [20] usually coincides with experimental results very well, there is a large gap in the special case of $d = n$, where d is the Hamming distance and n is the code length. More concretely, for $d = n$, the value calculated by equation (46) in [20] is roughly half of the value obtained by experiments. It is important to explain this gap analytically.

The main purpose of this paper is to provide analytic explanations for the above phenomena. First, we derive the exact HDS formula for tailless DAC and show that equation (46) in [20] is in fact an approximate version of the exact HDS formula. Further, the HDS behavior in the special case of $d = n$ is explained. Next, we extend the work on HDS from tailless DAC to tailed DAC and show that closely-spaced fellow codewords can be removed by increasing tail length to a value not very close to the bitstream length, where *fellow codewords* refer to the codewords belonging to the same codebook, which explains why decoding errors of DAC can be reduced by introducing tails. Third, we derive the *average codebook cardinality* (ACC), which is closely related to decoding complexity of tailed DAC and show that on average, each DAC codebook will consist of more codewords as tail length increases to a value not very close to the bitstream length, which logically explains why a longer tail usually leads to higher decoding complexity. In addition, we also derive the *rate loss* of tailed DAC and show that a longer tail usually causes larger rate loss.

The rest of this paper is arranged as follows. The exact HDS formula of tailless DAC is derived in Sect. II. A conjecture about the ceiling errors of geometric series is proposed in Sect. III, which lays a foundation for deriving the approximate HDS formula in Sect. IV. Then, both exact and approximate HDS formulas are extended to tailed DAC in Sect. V. The related work on CCS is briefly reviewed in Sect. VI. We then make use of CCS as a tool to analyze the ACC and rate loss of tailed DAC in Sect. VII. A numerical algorithm is given in Sect. VIII for calculating the ACC and rate loss of tailed DAC. Experimental results are reported in Sect. IX, and finally Sect. X concludes this paper.

II. Exact HDS of Tailless DAC

A. Notation Definition

Let X be a random variable, $\mathcal{X}$ the alphabet of X, and $x \in \mathcal{X}$ a realization of X. Let $f(X)$ be a function of X and $f(x)$ a realization of $f(X)$. Let $X_i^j := (X_i, \cdots, X_{j-1})$, where $i \leq j$. If $i = j$, X_i^j is empty; if $i = 0$, the subscript of X_i^j can be dropped, i.e., $X^j = X_0^j$. The realization of X_i^j is denoted by $x_i^j := (x_i, \cdots, x_{j-1})$. Let $[i:j] := \{i, \cdots, j\}$ and $(i:j) := \{(i+1), \cdots, (j-1)\}$, while the meanings of $[i:j)$ and $(i:j]$ are similar. Let $a^{\pm[i:j]b} := (a^{\pm ib}, \cdots, a^{\pm jb})$ and the meanings of $a^{\pm(i:j)b}$, $a^{\pm[i:j)b}$, and $a^{\pm(i:j]b}$ are similar.

The τ-shifting operation of continuous interval $[l, h)$ is defined as $\{[l, h) \pm \tau\} := [l \pm \tau, h \pm \tau)$. In addition, we define $\{\tau + [l, h)\} = \{[l, h) + \tau\}$ and $\{\tau - [l, h)\} := (\tau - h, \tau - l]$. The k-shifting operation of discrete interval $[i:j)$ is defined as $\{[i:j) \pm k\} := [(i \pm k) : (j \pm k))$. In addition, we define $\{k + [i:j)\} = \{[i:j) + k\}$ and $\{k - [i:j)\} := ((k-j) : (k-i)]$. As for other forms of continuous/discrete intervals, the definitions of shifting operations are similar.

Depending on the operand, $|\cdot|$ may denote the cardinality of a set, the length of an interval, the absolute value of a scalar, or the number of supports, i.e., nonzero elements, in a vector. As in [20], we define $(\cdot)^+ := \max(\cdot, 0)$. The round operation is denoted by $\mathrm{rnd}(\cdot)$. There are two forms of indicator functions: $\mathbf{1}_{\mathcal{I}}(x)$ takes values 1 or 0 depending on whether $x \in \mathcal{I}$ or not; $\mathbf{1}_s$ takes values 1 or 0 depending on whether the statement s is true or false.

B. Review of Tailless DAC Encoding

The (n, R) DA code, which stands for a tailless DA code with length n and rate $R \in (0, 1)$, partitions source space $\mathbb{B}^n$ into 2^{nR} codebooks, where $nR \in \mathbb{Z}$ [20]. The DA encoder replaces each binary block $x^n \in \mathbb{B}^n$ with a codebook index $m \in [0 : 2^{nR})$, which is realized via iteratively mapping source symbols onto partially-overlapped intervals. The mapping rule is $0 \to [0, 2^{-R})$ and $1 \to [(1 - 2^{-R}), 1)$ for uniform binary sources [3], [4]. As shown in [19], the final interval after coding x^n is given by $[l(x^n), l(x^n) + 2^{-nR})$, where

$$l(x^n) = (1 - 2^{-R}) \sum_{i=0}^{n-1} x_i 2^{-iR}. \tag{1}$$

Further, we define $s(x^n) := 2^{nR} l(x^n)$. It is easy to show that

$$s(x^n) = (1 - 2^{-R}) \sum_{i=0}^{n-1} x_i 2^{(n-i)R}. \tag{2}$$

The final interval $[l(x^n), l(x^n) + 2^{-nR})$ is now mapped onto $[s(x^n), s(x^n) + 1)$ [20]. It is easy to see $s(x^n) \in [s(0^n), s(1^n)] = [0, (2^{nR} - 1)]$. Let us define $m(x^n) := \lceil s(x^n) \rceil$. It is obvious that $m(x^n) \in [0 : 2^{nR})$, so $m(x^n)$ is the index of the DAC codebook containing x^n. Now it is clear that the coexistence of x^n and $(x^n \oplus z^n)$, where $z^n \in \mathbb{B}^n$, in the same DAC codebook, is equivalent to $m(x^n \oplus z^n) = m(x^n)$. Note that $m(x^n) = 0$ only if $x^n = 0^n$, so there is only one codeword 0^n in $\mathcal{C}_0$, where $\mathcal{C}_m := \{x^n : \lceil s(x^n) \rceil = m\}$ denotes the m-th DAC codebook.

C. Definition of DAC HDS

Let $k_d(x^n)$ be the number of d-away *fellow codewords* of x^n [20], i.e.,

$$k_d(x^n) := \left|\{z^n : |z^n| = d \text{ and } m(x^n \oplus z^n) = m(x^n)\}\right|, \tag{3}$$

where $|z^n|$ denotes the number of supports in z^n. Obviously, $k_0(x^n) \equiv 1$. Let X^n be the tuple of random variables associated with x^n. We define $\psi_{n,R}(d)$ as

$$\psi_{n,R}(d) := E[k_d(X^n)] = \sum_{x^n \in \mathbb{B}^n} \Pr(X^n = x^n) k_d(x^n) \overset{(a)}{=} 2^{-n} \sum_{x^n \in \mathbb{B}^n} k_d(x^n), \tag{4}$$

where (a) comes from the assumption that X is a uniform binary source. It is easy to see that $\psi_{n,R}(d)$ is the average number of d-away fellow codewords for each codeword $x^n \in \mathbb{B}^n$. We refer to $\psi_{n,R}(d)$ as the HDS of the (n, R) DA code [20], which is a function *with respect to* (w.r.t.) Hamming distance d that is parameterized by code length n and code rate R.

According to (3), it is easy to show that $\frac{1}{2}\sum_{x^n \in \mathcal{C}_m} k_d(x^n)$ is equal to the number of d-away codeword-pairs in $\mathcal{C}_m$ and $\sum_{d=0}^{n} k_d(x^n) = |\mathcal{C}_m|$ for all $x^n \in \mathcal{C}_m$. Further, from (4), we can obtain

$$\sum_{d=0}^{n} \psi_{n,R}(d) = 2^{-n} \sum_{m=0}^{2^{nR}-1} |\mathcal{C}_m|^2. \tag{5}$$

Obviously, the right-hand side of (5) is in fact the ACC of the (n, R) DA code.

D. Definition of Coexisting Interval

Definition 1 [**Coexisting Interval**] The coexisting interval of $x^n \in \mathbb{B}^n \setminus 0^n$ is

$$\mathcal{I}(x^n) := ((m(x^n) - 1), m(x^n)]. \tag{6}$$

Apparently, $s(x^n) \in \mathcal{I}(x^n)$ holds always. If $s(x^n \oplus z^n) \in \mathcal{I}(x^n)$, x^n and $(x^n \oplus z^n)$ will coexist in the same codebook. Conversely, if $m(x^n) = m(x^n \oplus z^n)$, we have $s(x^n \oplus z^n) \in \mathcal{I}(x^n \oplus z^n) =$

$\mathcal{I}(x^n)$. It is easy to see that for any $x^n \neq 0^n$, $|\mathcal{I}(x^n)| \equiv 1$, i.e., the length of $\mathcal{I}(x^n)$ is always 1. Since 0^n is the unique codeword in $\mathcal{C}_0$, we define $\mathcal{I}(0^n) := \{0\}$. For conciseness, the case of $x^n = 0^n$ will be ignored below without explicit declaration.

It can be obtained from (2) that

$$s(x^n \oplus z^n) = s(x^n) + \tau_{n,R}(x^n, z^n), \tag{7}$$

where $\tau_{n,R}(x^n, z^n)$ is a function w.r.t. x^n and z^n that is parameterized by n and R, i.e.,

$$\tau_{n,R}(x^n, z^n) := (1 - 2^{-R}) \sum_{i=0}^{n-1} z_i(1 - 2x_i)2^{(n-i)R}. \tag{8}$$

It is easy to show that

$$\tau_{n,R}((x^n \oplus z^n), z^n) = \tau_{n,R}((x^n \oplus 1^n), z^n) = -\tau_{n,R}(x^n, z^n) \tag{9}$$

and $|\tau_{n,R}(x^n, z^n)| \leq s(1^n) = (2^{nR} - 1)$. If $m(x^n) = m(x^n \oplus z^n)$, i.e., x^n and $(x^n \oplus z^n)$ coexist in the same codebook, $s(x^n \oplus z^n) \in \mathcal{I}(x^n)$ must hold and thus according to (7), $s(x^n) \in \{\mathcal{I}(x^n) - \tau_{n,R}(x^n, z^n)\}$. Next we give the concept of z^n-coexisting interval.

Definition 2 [z^n**-Coexisting Interval**] The z^n-coexisting interval of $x^n \in \mathbb{B}^n \setminus 0^n$ is

$$\mathcal{I}(x^n, z^n) := \{\mathcal{I}(x^n) - \tau_{n,R}(x^n, z^n)\} \cap \mathcal{I}(x^n). \tag{10}$$

Obviously, $\mathcal{I}(x^n, z^n) \subseteq \mathcal{I}(x^n)$. It is easy to see that $s(x^n) \in \mathcal{I}(x^n, z^n)$ is the necessary and sufficient condition for the coexistence of x^n and $(x^n \oplus z^n)$ in the same codebook. On the other hand, if $m(x^n) = m(x^n \oplus z^n)$, we have $\mathcal{I}(x^n) = \mathcal{I}(x^n \oplus z^n)$ and

$$s(x^n \oplus z^n) \in \mathcal{I}((x^n \oplus z^n), z^n) \subseteq \mathcal{I}(x^n \oplus z^n). \tag{11}$$

It can be obtained from (10) that given $m(x^n) = m(x^n \oplus z^n)$,

$$\begin{aligned} \mathcal{I}((x^n \oplus z^n), z^n) &= \{\mathcal{I}(x^n \oplus z^n) - \tau_{n,R}((x^n \oplus z^n), z^n)\} \cap \mathcal{I}(x^n \oplus z^n) \\ &\overset{(a)}{=} \{\mathcal{I}(x^n) + \tau_{n,R}(x^n, z^n)\} \cap \mathcal{I}(x^n), \end{aligned} \tag{12}$$

where (a) comes from $\tau_{n,R}((x^n \oplus z^n), z^n) = -\tau_{n,R}(x^n, z^n)$ and $\mathcal{I}(x^n \oplus z^n) = \mathcal{I}(x^n)$ in the case of $m(x^n) = m(x^n \oplus z^n)$. It is obvious that $|\mathcal{I}(x^n, z^n)| = |\mathcal{I}((x^n \oplus z^n), z^n)|$ and

$$\begin{aligned} |\mathcal{I}(x^n, z^n)| &= (|\mathcal{I}(x^n)| - |\tau_{n,R}(x^n, z^n)|)^+ \\ &= (1 - |\tau_{n,R}(x^n, z^n)|)^+ \leq 1. \end{aligned} \tag{13}$$

Obviously, $\mathcal{I}(x^n, z^n) = \emptyset$ if $|\tau_{n,R}(x^n, z^n)| \geq 1$. However, note that $\mathcal{I}(x^n, z^n) \neq \emptyset$ is only the necessary condition for $m(x^n) = m(x^n \oplus z^n)$, not the sufficient condition.

E. Calculation of Exact HDS

With z^n-coexisting interval, we can easily obtain

$$k_d(x^n) = |\{z^n : |z^n| = d \text{ and } s(x^n) \in \mathcal{I}(x^n, z^n)\}|. \tag{14}$$

The exact HDS of the (n, R) DA code is then

$$\psi_{n,R}(d) = 2^{-n} \sum_{x^n \in \mathbb{B}^n} \left(\sum_{z^n : |z^n| = d} \mathbf{1}_{\mathcal{I}(x^n, z^n)}(s(x^n)) \right). \tag{15}$$

Given $|z^n| = d$, there are $\binom{n}{d}$ different z^n's, so the complexity of computing $\psi_{n,R}(d)$ via (15) is $O(\binom{n}{d}2^n)$. Further, since $\sum_{d=0}^{n} \binom{n}{d} = 2^n$, the total complexity of computing all $\psi_{n,R}(d)$'s for $d \in [0 : n]$ via (15) is $O(4^n)$. As for calculating each term $\mathbf{1}_{\mathcal{I}(x^n, z^n)}(s(x^n))$, it can be found from (2), (8), and (10) that the complexity is $O(n)$.

III. Ceiling Errors of Geometric Series

Though we obtain the exact HDS expression (15) for tailless DAC in Sect. II, its computational complexity is too large for practical use. Therefore, it is necessary to simplify (15). Before doing so, let us give the following conjecture.

Conjecture 1 **[Ceiling Errors of Geometric Series]** Let $(a, ar, ar^2, \cdots)$ be a *geometric series* (GS) with initial term a and common ratio r. Let $e_i := (\lceil ar^i \rceil - ar^i)$. If $r > 1$ and $r \notin \mathbb{Z}$, e_i's can be taken as the samples of *independent and identically-distributed* (i.i.d.) random variables that are uniformly distributed over $[0, 1)$.

The principle of Conject. 1 is very similar to that of the well-known *linear congruential* (LC) method, which is widely used in generating uniformly-distributed pseudo-random numbers. Let us recall how the LC method works. If $(x_0, x_1, \cdots)$ is a sequence generated by the LC method, we have $x_n = ((rx_{n-1} + c) \mod m)$, where r, c, and m are all integers. In the special case of $c = 0$, we have $x_n = (rx_{n-1} \mod m)$. It is easy to see that $(rx_{n-1} - x_n) = km$, where $k \in \mathbb{Z}$. Thus we can obtain $x_{n+1} = (rx_n \mod m) = ((r^2 x_{n-1} - rkm) \mod m) = (r^2 x_{n-1}$

$\mod m$). In general, we have $x_n = (r^n x_0 \mod m)$, showing that the numbers generated by the LC method are in fact the modulus errors of a GS with integer common ratio.

Though we are not able to prove Conject. 1, its correctness can be verified by simulations. Some examples are given in Fig. 1 to confirm Conject. 1 from different aspects. First, Fig. 1(a) shows that the samples of GS ceiling errors look very like the samples generated by the LC method. Second, Fig. 1(b) gives an approximate *probability density function* (PDF) of GS ceiling errors to show that GS ceiling errors are uniformly distributed over $[0, 1)$. In addition, it can also be found from the caption of Fig. 1 that the mean and variance of GS ceiling errors are very close to those of $\mathcal{U}(0, 1)$, where $\mathcal{U}(a, b)$ stands for the uniform distribution over $[a, b)$, especially when there are a large number of samples.

Third, Figs. 1(c) and 1(d) give the *total variation distance* (TVD) and *Kullback-Leibler divergence* (KLD) of GS ceiling errors to show that GS ceiling errors can be taken as the samples of independent random variables. The TVD between probability distributions P and Q is defined as $\delta(P, Q) := \sup |p(x) - q(x)|$, where p and q denote the densities of P and Q. The KLD of Q from P is defined as

$$D_{\text{KL}}(P\|Q) := \int_{-\infty}^{\infty} p(x) \log_2 \frac{p(x)}{q(x)} dx. \tag{16}$$

To make the results more convincing, we study the TVD and KLD of GS ceiling errors from multiple dimensions. Let $(e_0, e_1, \cdots)$ be a series of GS ceiling errors and $q(x^k)$ the "joint PDF" of $(e_i, \cdots, e_{i+k-1})$. If $e_0, e_1, \cdots$ are *independent and uniformly-distributed* (i.u.d.) over $[0, 1)$, we have $q(x^k) = 1$ for all $x^k \in [0, 1)^k$. To verify this point, we let $p(x^k) = 1$ for all $x^k \in [0, 1)^k$. Then the k-D TVD between P and Q becomes $\delta(P, Q) = \sup_{x^k \in [0,1)^k} |q(x^k) - 1|$ and the k-D KLD of Q from P becomes

$$D_{\text{KL}}(P\|Q) := -\int_0^1 \cdots \int_0^1 \log_2 q(x^k) dx_0 \cdots dx_{k-1}. \tag{17}$$

To estimate $q(x^k)$, we discretize space $[0, 1)^k$ into m^k equal-size cells and count the number of GS ceiling errors falling within each cell. Then $D_{\text{KL}}(P\|Q)$ can be approximated by

$$D_{\text{KL}}(P\|Q) \approx -(1/m^k) \sum_{i^k \in [0:m)^k} \log_2 q(i^k/m). \tag{18}$$

Considering the complexity, only 3 dimensions of TVD and KLD are given in Figs. 1(c) and 1(d). It can be seen that as the number of samples n increases, both TVD and KLD will go

down, showing that $q(x^k)$ tends to be uniform over $[0,1)^k$. Hence, GS ceiling errors can be taken as the samples of i.u.d. random variables.

Similar results are also obtained for other settings. According to the above observations, we assume that Conject. 1 is correct and use it in the following deduction. In addition, because flooring and rounding errors can be taken as the shifted versions of ceiling errors, for a GS with non-integer common ratio $r > 1$, flooring and rounding errors can be taken as the samples of i.i.d. random variables that are uniformly distributed over $(-1, 0]$ and $(-0.5, 0.5]$, respectively.

Assuming that Conject. 1 is true, then it is easy to prove the following conjecture.

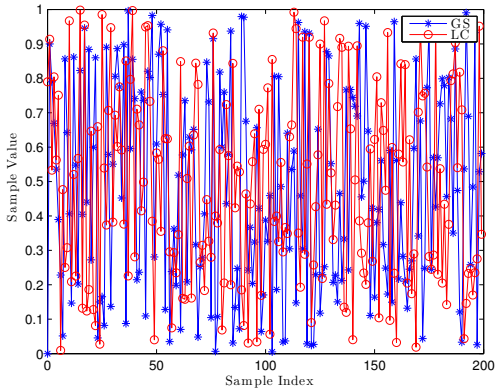
Conjecture 2 [Ceiling Errors of Weighted Sum of Geometric Series] Let $(a, ar, ar^2, \cdots)$ be a GS with initial term a and non-integer common ratio $r > 1$. Let X^n be a tuple of i.i.d. binary random variables and $S = \sum_{i=0}^{n-1} ar^i X_i$. Let $U = (\lceil S \rceil - S)$. Then for n sufficiently large, $U \sim \mathcal{U}(0,1)$ and U is weakly correlated with X^n.

IV. Approximate HDS of Tailless DAC

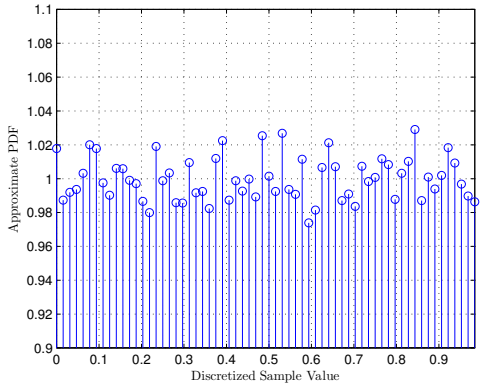
With the help of Conject. 1, this section will derive a fast method to compute the approximate value of $\psi_{n,R}(d)$. We define a ternary variable $w_i := z_i(1 - 2x_i) \in \mathbb{T} := \{-1, 0, 1\}$. Clearly, $w_i = 0$ if $z_i = 0$ and $w_i = \pm 1$ if $z_i = 1$. Conversely, if $w_i = \pm 1$, we have $z_i = 1$ and $x_i = (1 - w_i)/2$; otherwise, i.e., $w_i = 0$, we can get $z_i = 0$, but x_i is unknownable. Thus, given w^n, z^n is fully determined, but x^n is partially determined. Concretely speaking, each w^n leads $2^{n-|w^n|}$ different x^n's. Further, we let $\mathcal{Z} \subseteq [0:n)$ be the set of support indices of z^n and $\mathcal{Z}^c := [0:n) \setminus \mathcal{Z}$, i.e., $z_i = 1$ if $i \in \mathcal{Z}$ and $z_i = 0$ if $i \in \mathcal{Z}^c$. Thus $|\mathcal{Z}| = |z^n|$ and $|\mathcal{Z}^c| = n - |z^n|$. From x^n, we draw all elements indexed by $\mathcal{Z}$ to form a sub-vector $x_{\mathcal{Z}} \in \mathbb{B}^{|z^n|}$. Similarly, $x_{\mathcal{Z}^c} \in \mathbb{B}^{n-|z^n|}$ is also formed. Now we define

$$\begin{aligned} \tau_{n,R}(w^n) &:= (1 - 2^{-R}) \sum_{i=0}^{n-1} w_i 2^{(n-i)R} \\ &= (1 - 2^{-R}) \sum_{i \in \mathcal{Z}} w_i 2^{(n-i)R}. \end{aligned} \tag{19}$$

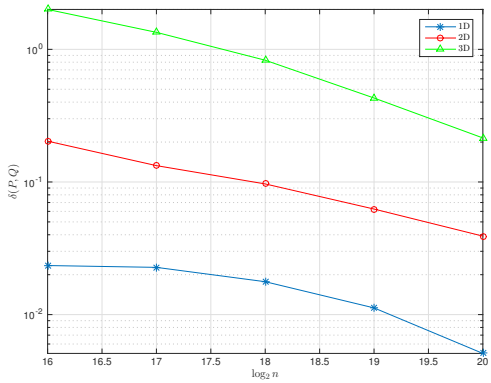
Obviously, $\tau_{n,R}(-w^n) = -\tau_{n,R}(w^n)$ and $|\tau_{n,R}(w^n)| \le s(1^n) = (2^{nR} - 1)$.



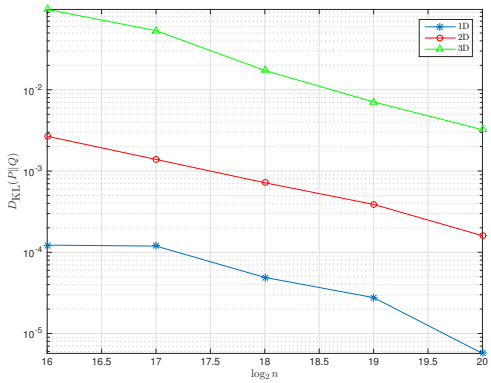
(a) Sample Behavior.



(b) Approximate PDF.



(c) Total Variation Distance (TVD).



(d) KL Divergence.

Fig. 1. (a) GS ceiling-error samples versus LC samples. The LC method is realized by the MATLAB function $\mathrm{rand}()$. The number of samples for each sequence is 200. For the GS, the common ratio is $r = 1.1$ and the initial term is $a = 1$. The mean of samples is 0.4820 for GS and 0.4926 for LC. The variance of samples is 0.0885 for GS and 0.0789 for LC. (b) Approximate PDF of GS ceiling errors. The common ratio is $r = 1 + 10^{-4}$ and the initial term is $a = 100$. We collect 2^{18} samples and discretize interval $[0, 1)$ into $m = 64$ cells. The mean of samples is 0.5, the same as the mean of $\mathcal{U}(0, 1)$, and the variance is 0.0834, close to $1/12 = 0.0833$, the variance of $\mathcal{U}(0, 1)$. (c) and (d) TVD and KLD of GS ceiling errors, respectively. The initial term is $a = 10^{10}$ and the common ratio is $r = 1 + 10^{-5}$. The number of samples n varies from 2^{16} to 2^{20}. The space $[0, 1)^k$ is divided into m^k equal-size cells, where $m = 16$.

A. Root Coexisting Interval

Obviously, if only w^n and $x_{\mathcal{Z}^c}$ are known, x^n and z^n can be deduced exactly. Hence, we rewrite $\mathcal{I}(x^n, z^n)$ as $\mathcal{I}(w^n, x_{\mathcal{Z}^c})$ and define

$$\begin{cases} \delta^-(w^n) := \mathbf{1}_{\tau_{n,R}(w^n)<0} \cdot \min(1, |\tau_{n,R}(w^n)|) \\ \delta^+(w^n) := \mathbf{1}_{\tau_{n,R}(w^n)>0} \cdot \min(1, |\tau_{n,R}(w^n)|) \end{cases}. \tag{20}$$

It is easy to see that $\delta^-(w^n)+\delta^+(w^n)\equiv\min(1,|\tau_{n,R}(w^n)|)\leq 1$ and $\delta^-(w^n)\cdot\delta^+(w^n)\equiv 0$. We can now rewrite (10) as

$$\begin{aligned}\mathcal{I}(w^n,x_{\mathcal{Z}^c}) &= \left((m(x^n)-1)+\delta^-(w^n),m(x^n)-\delta^+(w^n)\right]\\ &= \left\{m(x^n)-\mathcal{I}(w^n)\right\},\end{aligned}\tag{21}$$

where

$$\mathcal{I}(w^n):=\left[\delta^+(w^n),1-\delta^-(w^n)\right)\subseteq[0,1).\tag{22}$$

We call $\mathcal{I}(w^n)$ the w^n*-root coexisting interval*. Obviously, there are $|\mathbb{T}^n|=3^n$ root coexisting intervals in total. Since $\mathcal{I}(w^n,x_{\mathcal{Z}^c})$ is a shifted version of $\mathcal{I}(w^n)$, each root coexisting interval in fact leads $2^{n-|w^n|}$ coexisting intervals. Clearly, $\mathcal{I}(w^n)=\emptyset$ if $|\tau_{n,R}(w^n)|\geq 1$ and for all $x_{\mathcal{Z}^c}\in\mathbb{B}^{n-|w^n|}$,

$$|\mathcal{I}(w^n,x_{\mathcal{Z}^c})|=|\mathcal{I}(w^n)|=(1-|\tau_{n,R}(w^n)|)^+.\tag{23}$$

Coexisting Interval versus Risky Interval In [20], the concept of *risky interval* was proposed, which is similar to the *coexisting interval* to some extent. Below we discuss their differences. A risky interval can be denoted by $\mathcal{I}_{m,\mathcal{Z}}^{(x_{\mathcal{Z}})}$, where $m\in[0:2^{nR})$ is codebook index. It is obvious that given $x^n\neq 0^n$, $\mathcal{I}(w^n)=1-\mathcal{I}_{1,\mathcal{Z}}^{(x_{\mathcal{Z}})}$. It is proved in [20] that given $\mathcal{Z}$ and $x_{\mathcal{Z}}$, $|\mathcal{I}_{m,\mathcal{Z}}^{(x_{\mathcal{Z}})}|$'s are the same for all $m\in[1:2^{nR})$. As a sub-vector of x^n, $x_{\mathcal{Z}}$ in fact leads $2^{n-|z^n|}$ different x^n's. It can be easily shown that given $x^n\neq 0^n$, for all $x_{\mathcal{Z}^c}\in\mathbb{B}^{n-|z^n|}$,

$$\mathcal{I}(w^n,x_{\mathcal{Z}^c})\in\{\mathcal{I}_{m,\mathcal{Z}}^{(x_{\mathcal{Z}})}:m\in[1:2^{nR})\}.\tag{24}$$

B. Approximate Expression of HDS

With w^n and $x_{\mathcal{Z}^c}$, we can obtain

$$\psi_{n,R}(d)=2^{-d}\sum_{w^n:|w^n|=d}\rho(w^n),\tag{25}$$

where

$$\rho(w^n):=2^{-(n-d)}\sum_{x_{\mathcal{Z}^c}\in\mathbb{B}^{n-d}}\mathbf{1}_{\mathcal{I}(w^n,x_{\mathcal{Z}^c})}(s(x^n)).\tag{26}$$

According to (21), we have

$$\mathbf{1}_{\mathcal{I}(w^n,x_{\mathcal{Z}^c})}(s(x^n))=\mathbf{1}_{\mathcal{I}(w^n)}(m(x^n)-s(x^n)).\tag{27}$$

Let us rewrite (2) as

$$\begin{aligned} s(x^n) &= (1-2^{-R})\left(\sum_{i\in\mathcal{Z}}(1-w_i)2^{(n-i)R-1}+\sum_{i\in\mathcal{Z}^c}x_i2^{(n-i)R}\right) \\ &= c(\mathcal{Z})+\varphi(x_{\mathcal{Z}^c})-\tau_{n,R}(w^n)/2, \end{aligned} \tag{28}$$

where

$$\begin{cases} c(\mathcal{Z}) := (1-2^{-R})\sum_{i\in\mathcal{Z}}2^{(n-i)R-1} \\ \varphi(x_{\mathcal{Z}^c}) := (1-2^{-R})\sum_{i\in\mathcal{Z}^c}x_i2^{(n-i)R} \end{cases}. \tag{29}$$

Similarly, we can obtain

$$s(x^n\oplus z^n) = c(\mathcal{Z})+\varphi(x_{\mathcal{Z}^c})+\tau_{n,R}(w^n)/2. \tag{30}$$

Note the following three points:

- $(m(x^n)-s(x^n))\in[0,1)$ is actually the ceiling error of $s(x^n)$;
- for each given w^n, both $c(\mathcal{Z})$ and $\tau_{n,R}(w^n)$ are fixed for all $x_{\mathcal{Z}^c}\in\mathbb{B}^{n-|w^n|}$;
- $\varphi(x_{\mathcal{Z}^c})$ is the partial sum of a geometric series.

According to Conject. 1, we affirm that $(m(x^n)-s(x^n))$'s for different $x_{\mathcal{Z}^c}\in\mathbb{B}^{n-|w^n|}$ perform like the samples of i.i.d. random variables that are uniformly distributed over $[0,1)$. Hence for a given w^n, if there are a large number of $x_{\mathcal{Z}^c}$'s, $\rho(w^n)$ will be approximately equal to the ratio of the length of $\mathcal{I}(w^n)$ to that of $[0,1)$, i.e.,

$$\rho(w^n)\approx|\mathcal{I}(w^n)| = (1-|\tau_{n,R}(w^n)|)^+. \tag{31}$$

Finally, we obtain

$$\psi_{n,R}(d)\approx 2^{-d}\sum_{w^n:|w^n|=d}(1-|\tau_{n,R}(w^n)|)^+. \tag{32}$$

Given $|w^n|=d$, there are $\binom{n}{d}2^d$ different w^n's, so the complexity of computing $\psi_{n,R}(d)$ via (32) is $O(\binom{n}{d}2^d)$. Since $\sum_{d=0}^n\binom{n}{d}2^d=3^n$, the total complexity of computing all $\psi_{n,R}(d)$'s for $d\in[0:n]$ via (32) is $O(3^n)$, which is, for large n, far lower than $O(4^n)$. As for calculating $\tau_{n,R}(w^n)$, it can be found from (19) that the complexity is $O(n)$. It is easy to find that (32) is in fact equivalent to equation (46) in [20]. However, it must be pointed out that (31) holds only when $(n-|w^n|)$ is large, i.e., there are a large number of distinct $x_{\mathcal{Z}^c}$'s, because $\rho(w^n)$ is the average of $2^{n-|w^n|}$ binary terms as shown by (26).

C. Case of Small $(n-|w^n|)$

Given w^n, the number of distinct $x_{\mathcal{Z}^c}$'s is $2^{n-|w^n|}$, decreasing as $|w^n|$ goes up. For $(n-|w^n|)$ not very large, there are only a few distinct $x_{\mathcal{Z}^c}$'s, so $|\mathcal{I}(w^n)|$ may not be a good approximation of $\rho(w^n)$ in this case. Nevertheless, if only n is sufficiently large, $\psi_{n,R}(d)$ for any $d<n$ can still be well approximated by (32) because its right side is the sum of $\binom{n}{d}2^d$ pseudo-independent terms. However, $\psi_{n,R}(n)$ is still hard to find. If $|w^n|=n$, we have $z^n=1^n$, $\mathcal{Z}=[0:n)$, and $\mathcal{Z}^c=\emptyset$. Thus, $\varphi(x_{\mathcal{Z}^c})=0$ and

$$c(\mathcal{Z})=(1-2^{-R})\sum_{i=1}^{n}2^{iR-1}=(2^{nR}-1)/2. \tag{33}$$

We can then obtain

$$\begin{cases} s(x^n)=2^{nR-1}-(1+\tau_{n,R}(w^n))/2 \\ s(x^n\oplus z^n)=2^{nR-1}-(1-\tau_{n,R}(w^n))/2 \end{cases}. \tag{34}$$

If $|\tau_{n,R}(w^n)|<1$, $(1\pm\tau_{n,R}(w^n))/2\in(0,1)$ and hence for any $nR\in\mathbb{Z}$,

$$m(x^n)=m(x^n\oplus z^n)=2^{nR-1}\in\mathbb{Z}, \tag{35}$$

i.e., x^n and $(x^n\oplus z^n)$ always belong to the 2^{nR-1}-th codebook. Thus if $|w^n|=n$,

$$\rho(w^n)=\mathbf{1}_{|\tau_{n,R}(w^n)|<1}=\mathbf{1}_{|\tau_{n,R}(x^n,1^n)|<1}\in\mathbb{B}, \tag{36}$$

showing that $\rho(w^n)$ cannot be approximated by $(1-|\tau_{n,R}(w^n)|)^+$. Now we get

$$\psi_{n,R}(n)=2^{-n}\sum_{x^n\in\mathbb{B}^n}\mathbf{1}_{|\tau_{n,R}(x^n,1^n)|<1}. \tag{37}$$

Since $\psi_{n,R}(n)$ is the average of 2^n binary terms, we have $\psi_{n,R}(n)<1$. According to (34), given $|w^n|=n$, if $|\tau_{n,R}(w^n)|<1$, $s(x^n)\in((2^{nR-1}-1),2^{nR-1})$, and vice versa. Hence,

$$\mathbf{1}_{|\tau_{n,R}(x^n,1^n)|<1}=\mathbf{1}_{((2^{nR-1}-1),2^{nR-1})}(s(x^n)). \tag{38}$$

According to (37) and (38), we can obtain

$$\psi_{n,R}(n)=\Pr\left(s(X^n)\in((2^{nR-1}-1),2^{nR-1})\right). \tag{39}$$

According to Conject. 1, given $|\tau_{n,R}(w^n)|<1$, $|\tau_{n,R}(w^n)|$ is approximately uniformly distributed over $[0,1)$ for nR sufficiently large. Therefore,

$$\left(\sum_{x^n\in\mathbb{B}^n}(1-|\tau_{n,R}(x^n,1^n)|)^+\right)\approx\frac{1}{2}\left(\sum_{x^n\in\mathbb{B}^n}\mathbf{1}_{|\tau_{n,R}(x^n,1^n)|<1}\right), \tag{40}$$

showing that the approximate value of $\psi_{n,R}(n)$ given by (32) is roughly half of its exact value given by (15), which explains experimental results accurately (cf. Subsect. IX-A).

V. HDS OF TAILED DAC

A. Review of Tailed DAC Encoding

Tailed DAC divides each source block x^n into body x^{n-t} and tail x_{n-t}^n. Let us use the (n, R, t) DA code to stand for a tailed DA code with length n, rate R, and tail length t. Each tail symbol is always coded at rate 1, so the mapping rule is: $0 \to [0, 2^{-1})$ and $1 \to [2^{-1}, 1)$. To compress x^n at the average rate R, each body symbol should be coded at rate $r = \frac{nR-t}{n-t} \leq R$, so the mapping rule is: $0 \to [0, 2^{-r})$ and $1 \to [(1-2^{-r}), 1)$. It is easy to get $(n-t)(1-r) = n(1-R)$. To guarantee $r \geq 0$, t must not be larger than nR, so $t \in [0 : nR]$. (Obviously, tailless DAC is a special form of tailed DAC obtained by setting $t = 0$ and $r = R$.) The final interval after coding x^n is still $[l(x^n), l(x^n) + 2^{-nR})$, where

$$l(x^n) = (1 - 2^{-r}) \sum_{i=0}^{n-t-1} x_i 2^{-ir} + \sum_{i=n-t}^{n-1} x_i 2^{n(1-R)-1-i}. \tag{41}$$

Because $nR = (n-t)r + t$, we have

$$s(x^n) = 2^t(1 - 2^{-r}) \sum_{i=0}^{n-t-1} x_i 2^{(n-t-i)r} + \sum_{i=n-t}^{n-1} x_i 2^{n-1-i}. \tag{42}$$

The scaled final interval is still $[s(x^n), s(x^n) + 1)$ and $s(x^n) \leq (2^{nR} - 1)$. It can also be seen that $m(x^n) \in [0 : 2^{nR})$ still holds.

B. Calculation of HDS for Tailed DAC

According to the definition of $\tau_{n,R}(w^n)$, we can obtain

$$\begin{aligned} \tau_{n,R}(w^n) &= 2^t(1 - 2^{-r}) \sum_{i=0}^{n-t-1} w_i 2^{(n-t-i)r} + \sum_{i=n-t}^{n-1} w_i 2^{n-1-i} \\ &= 2^t \tau_{n-t,r}(w^{n-t}) + \tau_{t,1}(w_{n-t}^n). \end{aligned} \tag{43}$$

The exact and approximate values of $\psi_{n,R}(d)$ can be computed via (15) and (32), respectively.

An Extreme Case. When $t = nR$, $r = (1 - 2^{-r}) = 0$, so $\tau_{n,R}(w^n) = \tau_{t,1}(w_{n-t}^n) \in \mathbb{Z}$, i.e., $\tau_{n,R}(w^n)$ purely depends on w_{n-t}^n and is always an integer. Thus, if $z_{n-t}^n \neq 0^t$, x^n and $(x^n \oplus z^n)$ cannot coexist in the same codebook, i.e., $\psi_{n,R}(d) = 0$ for $d > (n-t) = n(1-R)$. In addition, since $\tau_{n,R}(w^n)$ is not related to w^{n-t}, it is easy to see that, when $t = nR$,

$$\psi_{n,R}(d) = \begin{cases} \binom{n(1-R)}{d}, & d \in [0 : n(1-R)] \\ 0, & d \in (n(1-R) : n] \end{cases}. \tag{44}$$

C. Removal of Closely-Spaced Fellow Codewords

Though experiments show that tailed DAC is better than tailless DAC [3], [4], there is no theoretical explanation on the superiority of tailed DAC over tailless DAC. Below, we will reveal that closely-spaced fellow codewords can be removed by increasing tail length, which explains the superiority of tailed DAC over tailless DAC. Due to computation complexity and to keep the exposition simple, we consider below only two special cases $\psi_{n,R}(1)$ and $\psi_{n,R}(2)$. To begin with, we give the following claim.

Claim 1 If $|z^{n-t}| = 0$ and $|z_{n-t}^n| > 0$, then $m(x^n) \neq m(x^n \oplus z^n)$. Conversely, if $|z^n| > 0$ and $m(x^n) = m(x^n \oplus z^n)$, then $|z^{n-t}| > 0$.

In plain words, if a pair of codewords coexist in the same codebook, it is impossible that these two codewords differ from each other only in tails. The proof of Claim 1 is obvious and is omitted. With the help of Claim 1, we explain below why $\psi_{n,R}(1)$ and $\psi_{n,R}(2)$ will tend to 0 as t increases. Then, we discuss the general case of $\psi_{n,R}(d)$ when $d > 2$.

1) 1-Away Fellow Codewords: Given $|w^n| = 1$, there are two sub-cases: $|w^{n-t}| = 0$ and $|w_{n-t}^n| = 1$; $|w^{n-t}| = 1$ and $|w_{n-t}^n| = 0$. According to Claim 1, in the former sub-case, it is certain that $m(x^n) \neq m(x^n \oplus z^n)$. Hence, we need to consider only the later sub-case, which means $\tau_{n,R}(w^n) = 2^t \tau_{n-t,r}(w^{n-t})$. Given $|w^{n-t}| = 1$, we can obtain from (43) that

$$|\tau_{n-t,r}(w^{n-t})| \geq (1 - 2^{-r})2^r = (2^r - 1) \tag{45}$$

and further $|\tau_{n,R}(w^n)| \geq 2^t(2^r - 1)$. Suppose that $t \leq \frac{nR}{2}$. Then $r \geq \frac{R}{2-R}$. Hence $2^t(2^r - 1) \geq 2^t(2^{\frac{R}{2-R}} - 1)$. For large n, increasing t will make $2^t(2^{\frac{R}{2-R}} - 1) \geq 1$. An example of $2^t(2^r - 1)$ is given in Fig. 2(a) for $n = 64$ and $R = 0.5$, which shows that $2^t(2^r - 1)$ increases monotonously for small t. Hence, it is possible to make $|\tau_{n,R}(w^n)| \geq 1$, i.e., $\mathcal{I}(w^n) = \emptyset$, hold always for all w^n's satisfying $|w^n| = 1$ by increasing t. In other words, 1-away fellow codewords can be removed by simply increasing tail length t, even for finite code length n.

2) 2-Away Fellow Codewords: Given $|w^n| = 2$, there are three sub-cases: $|w^{n-t}| = 0$ and $|w_{n-t}^n| = 2$; $|w^{n-t}| = 2$ and $|w_{n-t}^n| = 0$; $|w^{n-t}| = |w_{n-t}^n| = 1$. According to Claim 1, in the first sub-case, $m(x^n) \neq m(x^n \oplus z^n)$, so we need to consider only the later two sub-cases.

In the sub-case of $|w^{n-t}| = 2$ and $|w_{n-t}^n| = 0$, we have $\tau_{n,R}(w^n) = 2^t \tau_{n-t,r}(w^{n-t})$. It is easy

to get from (43) that, given $|w^{n-t}| = 2$,

$$|\tau_{n-t,r}(w^{n-t})| \geq (1-2^{-r})(2^{2r}-2^r) = (2^r-1)^2. \tag{46}$$

Thus, given $|w^{n-t}| = 2$ and $|w_{n-t}^n| = 0$, $|\tau_{n,R}(w^n)| \geq 2^t(2^r-1)^2$. Still suppose that $t \leq \frac{nR}{2}$, which is followed by $2^t(2^r-1)^2 \geq 2^t(2^{\frac{R}{2-R}}-1)^2$. For large n, increasing t will make $2^t(2^{\frac{R}{2-R}}-1)^2 \geq 1$, as shown by Fig. 2(a), where $n = 64$ and $R = 0.5$. Hence, it is possible to make $|\tau_{n,R}(w^n)| \geq 2^t(2^r-1)^2 \geq 1$, i.e., $\mathcal{I}(w^n) = \emptyset$, hold always for all w^n's satisfying $|w^{n-t}| = 2$ and $|w_{n-t}^n| = 0$ by increasing tail length t.

In the sub-case of $|w^{n-t}| = |w_{n-t}^n| = 1$, we have $|\tau_{n-t,r}(w^{n-t})| = (2^r-1)2^{ir}$ for $i \in [0:(n-t))$ and $|\tau_{t,1}(w_{n-t}^n)| = 2^j$ for $j \in [0:t)$. Let $\gamma_i := (2^r-1)2^{t+ir}$. Then, we have $|\tau_{n,R}(w^n)| = |\gamma_i \pm 2^j|$, where $(i,j) \in [0:(n-t)) \times [0:t)$. Since $\gamma_i > 0$ for all $i \in [0:(n-t))$ and $2^j \geq 1$ for all $j \in [0:t)$, $|\gamma_i + 2^j| > 1$ holds always. Thus, it is unnecessary to consider $|\gamma_i + 2^j|$. As for $|\gamma_i - 2^j|$, there are $(n-t) \times t$ possible values for $(i,j) \in [0:(n-t)) \times [0:t)$. For n very large and $t \ll n$, $r \approx R$ and thus $(\gamma_{i+1} - \gamma_i)$ increases w.r.t. t, i.e., γ_i's tend to be sparser as t increases. Hence as t increases, it is less likely that γ_i's fall within $(2^j-1, 2^j+1)$'s. An example is given in Fig. 2(b) to confirm this point, where

$$\Delta_i := \min(\gamma_i - 2^{\lfloor \log_2 \gamma_i \rfloor}, 2^{\lceil \log_2 \gamma_i \rceil} - \gamma_i). \tag{47}$$

As shown by Fig. 2(b), as t increases, fewer Δ_i's will be less than 1 and when $t > 6$, there is no Δ_i less than 1. Therefore, it is possible to make $|\tau_{n,R}(w^n)| = |\gamma_i \pm 2^j| \geq 1$, i.e., $\mathcal{I}(w^n) = \emptyset$, hold always for all w^n's satisfying $|w^{n-t}| = |w_{n-t}^n| = 1$ by increasing t.

Based on the above analyses, we conclude that 2-away fellow codewords can be removed by simply increasing tail length t, even for finite code length n.

3) General Case: The analysis of the general case $d > 2$ is more complex, but the principle is similar to the above cases. From (43), we have

$$|\tau_{n,R}(w^n)| = \begin{cases} \left|2^t|\tau_{n-t,r}(w^{n-t})| - |\tau_{t,1}(w_{n-t}^n)|\right|, & \tau_{n-t,r}(w^{n-t}) \cdot \tau_{t,1}(w_{n-t}^n) < 0 \\ 2^t|\tau_{n-t,r}(w^{n-t})| + |\tau_{t,1}(w_{n-t}^n)|, & \tau_{n-t,r}(w^{n-t}) \cdot \tau_{t,1}(w_{n-t}^n) \geq 0 \end{cases}. \tag{48}$$

From (19), we have $|\tau_{n-t,r}(w^{n-t})| \in [0, (2^{(n-t)r}-1)]$ and $|\tau_{t,1}(w_{n-t}^n)| \in [0:2^t) \subset \mathbb{Z}$. Further, $2^t|\tau_{n-t,r}(w^{n-t})| \in [0, (2^{nR}-2^t)]$ and $|\tau_{n,R}(w^n)| \in [0, (2^{nR}-1)]$. Therefore,

$$\left(2^t|\tau_{n-t,r}(w^{n-t})|, |\tau_{t,1}(w_{n-t}^n)|\right) \in [0, (2^{nR}-2^t)] \times [0:2^t). \tag{49}$$

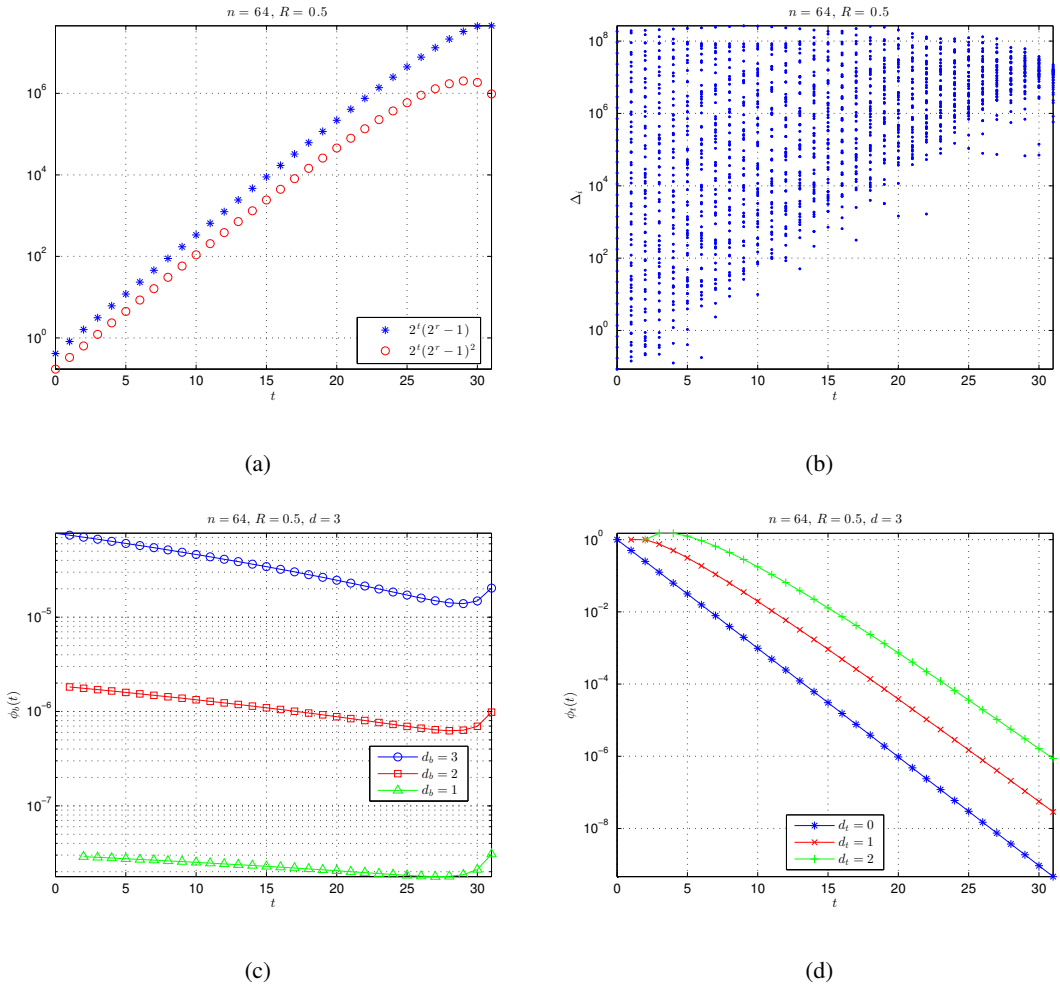


Fig. 2. (a) $2^t(2^r-1)$ and $2^t(2^r-1)^2$ versus tail length t. (b) Distribution of Δ_i, defined by (47), versus tail length t. (c) Conditional body density. (d) Conditional tail density.

Given $|w_{n-t}^n| > 0$, we have

$$2^t|\tau_{n-t,r}(w^{n-t})| + |\tau_{t,1}(w_{n-t}^n)| \geq |\tau_{t,1}(w_{n-t}^n)| \geq 1. \tag{50}$$

Thus, we need to consider only the sub-case of

$$|\tau_{n,R}(w^n)| = \left|2^t|\tau_{n-t,r}(w^{n-t})| - |\tau_{t,1}(w_{n-t}^n)|\right|. \tag{51}$$

The conditional "density" of $2^t|\tau_{n-t,r}(w^{n-t})|$ over $[0,(2^{nR}-2^t)]$ given $|w^{n-t}| = d_b \leq (n-t)$, which will be referred to as *conditional body density* for brevity, is defined as

$$\phi_b(t) := \frac{|\{w^{n-t} : |w^{n-t}| = d_b\}|}{2^{nR}-2^t} = \frac{\binom{n-t}{d_b}2^{d_b}}{2^{nR}-2^t}. \tag{52}$$

It is easy to see that

$$\binom{n-(t+1)}{d_b} = \frac{n-t-d_b}{n-t}\binom{n-t}{d_b} = (1-\frac{d_b}{n-t})\binom{n-t}{d_b}. \tag{53}$$

Since $(2^{nR}-2^{t+1}) = (2^{nR}-2^t-2^t)$, we have

$$\frac{2^{nR}-2^{t+1}}{2^{nR}-2^t} = 1-\frac{2^t}{2^{nR}-2^t} = 1-\frac{1}{2^{nR-t}-1}. \tag{54}$$

Thus,

$$\phi_b(t+1) = \frac{1-\frac{d_b}{n-t}}{1-\frac{1}{2^{nR-t}-1}}\phi_b(t). \tag{55}$$

Note the following two points:

- Both $\frac{d_b}{n-t}$ and $\frac{1}{2^{nR-t}-1}$ are monotonously-increasing and convex over $t \in [0:nR]$;
- For nR large enough, $\frac{d_b}{n-t}|_{t=0} = \frac{d_b}{n} > \frac{1}{2^{nR-t}-1}|_{t=0} = \frac{1}{2^{nR}-1}$, and $\frac{d_b}{n-t}|_{t=nR} = \frac{d_b}{n(1-R)} < \frac{1}{2^{nR-t}-1}|_{t=nR} = \infty$.

Hence, there must exist $t^* \in [0, nR] \subset \mathbb{R}$ that makes $\frac{d_b}{n-t^*} = \frac{1}{2^{nR-t^*}-1}$, and $\frac{d_b}{n-t} > \frac{1}{2^{nR-t}-1}$ for $t < t^*$ and $\frac{d_b}{n-t} < \frac{1}{2^{nR-t}-1}$ for $t > t^*$. Further, we have $\phi_b(t+1) < \phi_b(t)$ for $t < t^*$ and $\phi_b(t+1) > \phi_b(t)$ for $t > t^*$, i.e., $\phi_b(t)$ is monotonously decreasing over $t \in [0 : \lceil t^* \rceil]$ and monotonously increasing over $t \in [\lceil t^* \rceil : nR]$. Some examples of $\phi_b(t)$ are given in Fig. 2(c), which show that t^* is usually very close to nR.

The conditional "density" of $|\tau_{t,1}(w_{n-t}^n)|$ over $[0:2^t)$ given $|w_{n-t}^n| = d_t \le t$, which will be referred to as *conditional tail density* for brevity, is defined as

$$\phi_t(t) := \frac{|\{w_{n-t}^n : |w_{n-t}^n| = d_t\}|}{2^t} = \frac{\binom{t}{d_t}2^{d_t}}{2^t} = \binom{t}{d_t}2^{d_t-t}. \tag{56}$$

Hence, $\phi_t(t+1) = \frac{t+1}{2(t-d_t+1)}\phi_t(t)$. It is easy to see that $\frac{t+1}{2(t-d_t+1)}|_{t=2d_t-1} = 1$, i.e., $\phi_t(2d_t) = \phi_t(2d_t-1)$. Thus, $\phi_t(t)$ is monotonously increasing over $t \in [d_t : 2d_t)$ and monotonously decreasing over $t \in [2d_t : nR]$. Some examples of $\phi_t(t)$ are given in Fig. 2(d).

Since both $\phi_b(t)$ and $\phi_t(t)$ decrease monotonously over $t \in [2d_t : \lceil t^* \rceil]$, $2^t|\tau_{n-t,r}(w^{n-t})|$ ($|\tau_{t,1}(w_{n-t}^n)|$, resp.) will tend to be sparser over $[0, (2^{nR}-2^t)]$ ($[0:2^t)$, resp.) as t increases. Further, from the statistical viewpoint, $\left|2^t|\tau_{n-t,r}(w^{n-t})| - |\tau_{t,1}(w_{n-t}^n)|\right|$ will tend to be larger as t increases. Thus, it is possible to make $|\tau_{n,R}(w^n)| \ge 1$ for all w^n's satisfying $|w^n| = d = d_b+d_t \ll n$ by increasing t. In other words, for n sufficiently large and $d \ll n$, $\psi_{n,R}(d)$ will tend to 0 as t increases. However, note that as d increases, larger t is required to make $\psi_{n,R}(d) = 0$. For example, Fig. 2 shows that $\psi_{n,R}(1) = 0$ when $t > 1$, but $t > 6$ is required to make $\psi_{n,R}(2) = 0$. This point will be verified with experiments in Sect. IX.

VI. Codebook Cardinality Spectrum

A. Definitions

The projection of $m(X^n)$ onto $[0, 2^{nR}) \subset \mathbb{R}$ is $U_{0,n} := 2^{-nR} m(X^n) \in [0, 1)$. We define the level-$i$ projection of bitstream $m(X^n)$ as $U_{i,n} = u_i(X^n)$, where

$$u_i(X^n) := \begin{cases} 2^{ir}\left(U_{0,n} - l(X^i)\right), & i \in [0 : (n-t)] \\ 2^{i-n(1-R)}\left(U_{0,n} - l(X^i)\right), & i \in [(n-t) : n] \end{cases}. \tag{57}$$

We call $U_{0,n}$ the initial bitstream projection and $U_{n,n}$ the final bitstream projection. Note that $U_{i,n}$ is defined over $[0, 1) \subset \mathbb{R}$, so its pdf exists and is called the level-i CCS. Let us denote the level-i CCS by $f^{(i)}_{n,R,t}(u)$. Especially, the subscript t can be dropped if $t = 0$, i.e., $f^{(i)}_{n,R}(u) = f^{(i)}_{n,R,0}(u)$. The conditional pdf of $U_{i,n}$ given $X_j = x$ is called the conditional level-i CCS given $X_j = x$ and denoted by $f^{(i,j)}_{n,R,t}(u|x)$. The subscript t can be dropped if $t = 0$, i.e., $f^{(i,j)}_{n,R}(u|x) = f^{(i,j)}_{n,R,0}(u|x)$. To simplify notation, $f^{(i,i)}_{n,R,t}(u|x)$ is abbreviated to $f^{(i)}_{n,R,t}(u|x)$.

B. Calculation of CCS

Below, we derive $f^{(n)}_{n,R,t}(u)$ based on Conject. 2. Since $U_{n,n} = m(X^n) - s(X^n)$,

$$f_{U_{n,n}|X^n}(u|x^n) = \delta(u - (m(x^n) - s(x^n))), \tag{58}$$

where $f_{U_{n,n}|X^n}(u|x^n)$ is the conditional pdf of $U_{n,n}$ given $X^n = x^n$ and $\delta(u)$ is the Dirac delta function. Therefore,

$$\begin{aligned} f^{(n)}_{n,R,t}(u) &= \sum_{x^n \in \mathbb{B}^n} \Pr(X^n = x^n)\delta(u - (m(x^n) - s(x^n))) \\ &= 2^{-n} \sum_{x^n \in \mathbb{B}^n} \delta(u - (m(x^n) - s(x^n))). \end{aligned} \tag{59}$$

As shown by Conject. 2, $(m(x^n) - s(x^n))$'s for different x^n's perform like the samples of i.i.d. random variables that are uniformly distributed over $[0, 1)$. Thus, for n sufficiently large, $U_{n,n}$ is weakly correlated with X^n and $f^{(n)}_{n,R,t}(u) \approx \Pi(u)$, where

$$\Pi(u) := \begin{cases} 1, & 0 \le u < 1 \\ 0, & u < 0 \ \text{ or } \ u \ge 1 \end{cases}. \tag{60}$$

According to (57), for $i \in [(n-t) : n)$,

$$U_{i,n} = U_{i+1,n}/2 + X_i/2 = U_{n,n}2^{i-n} + \sum_{i'=i}^{n-1} X_{i'} 2^{(i-i')-1}. \tag{61}$$

For n sufficiently large, $U_{n,n}$ is weakly correlated with X^n, so $U_{i,n}$, the weighted sum of $U_{n,n}$ and X_i^n, is weakly correlated with X^i (note that X^i is independent of X_i^n). Thus, the pdf of $U_{i,n}$ is the convolution of the pdf of $U_{i+1,n}/2$ and that of $X_i/2$. Since $aX_i \sim \frac{1}{2}\left(\delta(x)+\delta(x-a)\right)$,

$$\begin{aligned} f_{n,R,t}^{(i)}(u) &\approx 2f_{n,R,t}^{(i+1)}(2u) \otimes \left(\delta(u)+\delta(u-2^{-1})\right) 2^{-1} \\ &= f_{n,R,t}^{(i+1)}(2u) + f_{n,R,t}^{(i+1)}(2u-1). \end{aligned} \tag{62}$$

where $\otimes$ denotes the convolution operation. We can then obtain $f_{n,R,t}^{(i)}(u) \approx f_{n,R,t}^{(n)}(u) \approx \Pi(u)$ for all $i \in [(n-t):n)$.

As for $i \in [0:(n-t))$, it is easy to see that $f_{n,R,t}^{(i)}(u) \approx f_{n-t,r}^{(i)}(u)$, where $r = \frac{nR-t}{n-t}$, i.e., the level-i CCS of the (n,R,t) tailed DA code approximates to the level-i CCS of the $(n-t,r)$ tailless DA code, so we will discuss only the (n,R) tailless DA code below. According to (57),

$$U_{i,n} = U_{i+1,n}2^{-R} + (1-2^{-R})X_i = U_{n,n}2^{(i-n)R} + (1-2^{-R})\sum_{i'=i}^{n-1} X_{i'}2^{(i-i')R}. \tag{63}$$

It can be seen that, for n sufficiently large, $U_{i,n}$ is weakly correlated with X^i and

$$\begin{aligned} f_{n,R}^{(i)}(u) &\approx 2^R f_{n,R}^{(i+1)}(u2^R) \otimes \left(\delta(u)+\delta(u-(1-2^{-R}))\right) 2^{-1} \\ &= \left(f_{n,R}^{(i+1)}(u2^R) + f_{n,R}^{(i+1)}(u2^R-(2^R-1))\right) 2^{R-1} \\ &\approx \left(\Pi(u2^{(n-i)R}) \otimes \lambda_{n-i,R}(u)\right) 2^{(n-i)(R-1)}, \end{aligned} \tag{64}$$

where

$$\lambda_{n',R}(u) := \bigotimes_{i'=0}^{n'-1} \left(\delta(u)+\delta(u-(1-2^{-R})2^{-i'R})\right) = \sum_{x^{n'}\in\mathbb{B}^{n'}} \delta(u-l(x^{n'})). \tag{65}$$

It is interesting that $2^{-n}\lambda_{n,R}(u)$ is actually the pdf of $l(X^n)$. Since $\lim_{n\to\infty} 2^{nR}\Pi(u2^{nR}) = \delta(u)$, for n sufficiently large and $i \ll n$, we have $f_{n,R}^{(i)}(u) \approx \lambda_{n-i,R}(u) \approx \lambda_{\infty,R}(u)$.

C. Conditional CCS

For n sufficiently large, $U_{i,n}$ is weakly correlated with X^i, so for the (n,R) tailless DA code, $f_{n,R}^{(i,j)}(u|x) \approx f_{n,R}^{(i)}(u)$ for $i > j$. As for $f_{n,R}^{(i)}(u|x)$, we have

$$\begin{aligned} f_{n,R}^{(i)}(u|x) &\approx 2^R f_{n,R}^{(i+1,i)}((u2^R - x(2^R-1))|x) \\ &\approx 2^R f_{n,R}^{(i+1)}(u2^R - x(2^R-1)). \end{aligned} \tag{66}$$

It is obvious that

$$f_{n,R}^{(i)}(u) = \sum_{x\in\mathbb{B}} \Pr(X_i = x) f_{n,R}^{(i)}(u|x) = \frac{1}{2}\sum_{x\in\mathbb{B}} f_{n,R}^{(i)}(u|x). \tag{67}$$

Let $p_i(x|u) := \Pr(X_i = x|U_{i,n} = u)$. According to Bayes' theorem, we can obtain

$$p_i(x|u) = \frac{\Pr(X_i = x) f_{n,R}^{(i)}(u|x)}{f_{n,R}^{(i)}(u)} = \frac{f_{n,R}^{(i)}(u|x)}{2f_{n,R}^{(i)}(u)}. \tag{68}$$

VII. ACC and Rate Loss of Tailed DAC

With the help of CCS, we will derive below the ACC and rate loss of tailed DAC, which is helpful for us to understand the properties of DA codes. The deduction of ACC is rather simple. According to the analyses in [19], it is easy to show that the ACC of the (n, R, t) tailed DA code is approximately $\eta 2^{n(1-R)}$, where

$$\eta := \int_0^1 \left(f_{n,R,t}^{(0)}(u)\right)^2 du. \tag{69}$$

We call η the *ACC scaling factor*. Obviously, $\eta \geq 1$ and the equality holds only if $f_{n,R,t}^{(0)}(u) = \Pi(u)$. On the contrary, the deduction of rate loss is much more difficult, as shown below.

A. Deduction of Rate Loss

Since $f_{n,R,t}^{(0)}(u) \approx f_{n-t,r}^{(0)}(u)$, only the (n, R) tailless DA code is considered in this subsection for simplicity. We deduce $H(X^n|m(X^n))$ first, which measures the remaining uncertainty of X^n given $m(X^n)$. Since $m(X^n)$ is a deterministic function w.r.t. X^n, we have $H(X^n) = H(m(X^n)) + H(X^n|m(X^n))$. Because $m(X^n) \in [0 : 2^{nR})$, we have $H(m(X^n)) \leq nR$ and the equality holds only if $m(X^n)$ is uniformly distributed over $[0 : 2^{nR})$. Further, because $U_{0,n} = 2^{-nR} m(X^n)$, we have $H(X^n|m(X^n)) = H(X^n|U_{0,n})$.

Lemma VII.1 (Decomposition of Conditional Entropy)**.** *For n sufficiently large,*

$$H(X^n|m(X^n)) = H(X^n|U_{0,n}) \approx \sum_{i=0}^{n-1} H(X_i|U_{i,n}). \tag{70}$$

Proof: By the chain rule, we can get

$$H(X^n|U_{0,n}) = \sum_{i=0}^{n-1} H(X_i|U_{0,n}, X^i) \overset{(a)}{=} \sum_{i=0}^{n-1} H(X_i|U_{0,n}), \tag{71}$$

where (a) is because X^n is the tuple of i.i.d. random variables. Further, because $U_{i,n}$ is weakly correlated with X^i for n sufficiently large, it can be seen that $U_{0,n}$, $U_{i,n}$, and X_i approximately form a Markov chain. Thus, $H(X_i|U_{0,n}) \approx H(X_i|U_{i,n})$ for n sufficiently large. ■

Lemma VII.2 (Symbol-wise Rate Loss)**.** *Let $h(\cdot)$ denote the differential entropy. For n sufficiently large, the rate loss of coding X_i with the (n, R) tailless DA code is*

$$H(X_i|U_{i,n}) - (1-R) \approx h(U_{i+1,n}) - h(U_{i,n}). \tag{72}$$

Proof: It is easy to show that

$$H(X_i|U_{i,n}) = \int_0^1 f_{n,R}^{(i)}(u) H(X_i|U_{i,n}=u)du, \tag{73}$$

where

$$H(X_i|U_{i,n}=u) = -\sum_{x\in\mathbb{B}} p_i(x|u)\log_2 p_i(x|u). \tag{74}$$

By substituting (68) into (74), we obtain

$$\begin{aligned} f_{n,R}^{(i)}(u)H(X_i|U_{i,n}=u) &= -f_{n,R}^{(i)}(u)\sum_{x\in\mathbb{B}} p_i(x|u)\log_2 p_i(x|u) \\ &= -\frac{1}{2}\sum_{x\in\mathbb{B}} f_{n,R}^{(i)}(u|x)\left(\log_2 f_{n,R}^{(i)}(u|x) - 1 - \log_2 f_{n,R}^{(i)}(u)\right) \\ &\overset{(a)}{=} f_{n,R}^{(i)}(u)\left(1+\log_2 f_{n,R}^{(i)}(u)\right) - \frac{1}{2}\left(\sum_{x\in\mathbb{B}} f_{n,R}^{(i)}(u|x)\log_2 f_{n,R}^{(i)}(u|x)\right), \end{aligned} \tag{75}$$

where (a) comes from $f_{n,R}^{(i)}(u) = \frac{1}{2}\sum_{x\in\mathbb{B}} f_{n,R}^{(i)}(u|x)$. Further,

$$H(X_i|U_{i,n}) = 1 - h(U_{i,n}) + \frac{1}{2}\sum_{x\in\mathbb{B}} h(U_{i,n}|X_i=x). \tag{76}$$

According to the properties of differential entropy and (66), $h(U_{i,n}|X_i=x) \approx h(U_{i+1,n}) - R$ for n sufficiently large. Hence,

$$\begin{aligned} H(X_i|U_{i,n}) &\approx 1 - h(U_{i,n}) + h(U_{i+1,n}) - R \\ &= (1-R) + (h(U_{i+1,n}) - h(U_{i,n})). \end{aligned} \tag{77}$$

Since X_i is coded at rate R, the rate loss is $(h(U_{i+1,n}) - h(U_{i,n})) \geq 0$. ■

According to Lem. VII.2, it is obvious that $h(U_{i,n})$ is monotonically increasing w.r.t. i. Since $f_{n,R}^{(i)}(u)$ is defined over $[0,1)$, we have $h(U_{i,n}) \leq 0$ and the equality holds iff $U_{i,n}$ is uniformly-distributed over $[0,1)$. Therefore, $h(U_{0,n}) \leq \cdots \leq h(U_{n,n}) \leq 0$. As $(n-i) \to \infty$, both $f_{n,R}^{(i)}(u)$ and $f_{n,R}^{(i+1)}(u)$ will converge to $f_{\infty,R}^{(0)}(u)$ and thus $(h(U_{i+1,n}) - h(U_{i,n})) \to 0$. Hence, for each $x^n \in \mathbb{B}^n$, the symbols far from the end can be compressed near-losslessly with the (n,R) DA code, and the rate loss comes mainly from ending symbols.

Theorem VII.3 (Block-wise Rate Loss)**.** *For n sufficiently large, the total rate loss of coding X^n with the (n,R) tailless DA code is*

$$H(X^n|m(X^n)) - n(1-R) \approx -h(U_{0,n}). \tag{78}$$

Proof: Based on Lems. VII.1 and VII.2, it is easy to obtain

$$H(X^n|m(X^n)) = H(X^n|U_{0,n}) \approx n(1-R) + h(U_{n,n}) - h(U_{0,n}). \tag{79}$$

Since $m(X^n)$ is represented by nR bits, the remaining uncertainty of X^n given $m(X^n)$ is lower bounded by $H(X^n) - nR = n(1-R)$. Thus, the total rate loss of coding X^n with the (n,R) tailless DA code is $H(X^n|m(X^n)) - n(1-R) = h(U_{n,n}) - h(U_{0,n})$. For n sufficiently large, $U_{n,n}$ is almost uniformly distributed over $[0,1)$ and thus $h(U_{n,n}) \approx 0$. ■

B. Physical Meaning of Rate Loss

The rate loss of DA codes can be explained intuitively with an example. We first compress X^n with the (n,R) DAC encoder to obtain bitstream $m(X^n)$ and then compress X^n with the standard AC encoder parameterized with the probability set $\{p_i(x|u)\}$ to obtain another bitstream $\hat{m}(X^n)$. Obviously, the length of $m(X^n)$ is always nR and the expected length of $\hat{m}(X^n)$ is about $n(1-R) - h(U_{0,n})$. Thus, the total length of $m(X^n)$ and $\hat{m}(X^n)$ is about $n - h(U_{0,n}) > n$. It can be shown that the error-free recovery of X^n is achievable by the interaction between the DAC decoder of $m(X^n)$ and the standard AC decoder of $\hat{m}(X^n)$. First, according to $U_{0,n}$, the DAC decoder can obtain $p_0(x|u)$, which is used by the AC decoder to recover X_0 exactly. Next according to $U_{0,n}$ and X_0, the DAC decoder can obtain $U_{1,n}$ and $p_1(x|u)$, which is then used by the AC decoder to recover X_1 exactly. Such operations are repeated until X_{n-1} is recovered. This example shows that X^n can be exactly represented by two bitstreams $m(X^n)$ and $\hat{m}(X^n)$, whose total length is slightly larger than $H(X^n) = n$.

C. Effects of Tail Length

Now we discuss the effect of tail length t on the ACC and rate loss of DA codes. The initial CCS of the (n, R, t) tailed DA code is approximate to that of the $(n-t, r)$ tailless DA code, where $r = \frac{nR-t}{n-t}$, so for the (n, R, t) tailed DA code, the ACC scaling factor is

$$\eta \approx \int_0^1 \left(f^{(0)}_{n-t,r}(u)\right)^2 du \tag{80}$$

and the rate loss is

$$-h(U_{0,n}) \approx \int_0^1 f^{(0)}_{n-t,r}(u) \log_2 f^{(0)}_{n-t,r}(u) du. \tag{81}$$

Note that $f^{(0)}_{n-t,r}(u)$ is subject to two parameters, t and r, that depend on each other, so both η and $-h(U_{0,n})$ behave strangely w.r.t. t.

We discuss the case of $t \ll nR$ first. Experiments show that $f^{(0)}_{n',r}(u)$ converges very fast as n' increases, so $f^{(0)}_{n-t,r}(u) \approx f^{(0)}_{\infty,r}(u)$ for $t \ll nR$. Thus given $t \ll nR$, the ACC and rate loss of the (n, R, t) tailed DA code almost purely depends on r, the coding rate of body symbols. It is easy to see that $f^{(0)}_{\infty,r}(u)$ tends to be spikier as r decreases. Two extreme cases are $f^{(0)}_{\infty,1}(u) = \Pi(u)$ and $f^{(0)}_{\infty,0}(u) = \delta(u - 0.5)$ [18]. Hence, both η and $-h(U_{0,n})$ are monotonously decreasing w.r.t. r. For example, in the extreme case of $r = 1$, we have $\eta = 1$ and $-h(U_{0,n}) = 0$; while in the other extreme case of $r = 0$, we have $\eta = -h(U_{0,n}) = \infty$. Further, because r is monotonously decreasing w.r.t. t, both η and $-h(U_{0,n})$ of the (n, R, t) DA code are monotonously increasing w.r.t. $t \ll nR$. Thus, from the viewpoint of decoding complexity, increasing tail length t will cause a negative effect.

Next we consider the case of $t \approx nR$. According to the definition of r, for small $(nR - t)$, r is very sensitive to t, so $f^{(0)}_{n-t,r}(u)$ cannot be approximated by $f^{(0)}_{\infty,r}(u)$. Instead, for $t \approx nR$, $f^{(0)}_{n-t,r}(u)$ will tend to be flatter as t increases (cf. Fig. 5(a) in Sect. IX), meaning that both ACC and rate loss will become smaller. In the extreme case of $t = nR$, we have $f^{(0)}_{n-t,r}(u) \approx \Pi(u)$, $\eta = 1$, and $-h(U_{0,n}) = 0$, hence the ACC is equal to $2^{n(1-R)}$ and there is no rate loss. The reason for this point is: When $t = nR$, x^n_{n-t} is transmitted in its uncoded form, while x^{n-t} is not transmitted. These analyses will be further verified by experiments in Sect. IX.

VIII. Numerical Calculation of ACC and Rate Loss

To obtain η and $-h(U_{0,n})$, one must know $f^{(0)}_{n,R,t}(u)$ first. Since $f^{(0)}_{n,R,t}(u) \approx f^{(0)}_{n-t,r}(u)$, where $r = \frac{nR-t}{n-t}$, for n sufficiently large, only $f^{(0)}_{n,R}(u)$ is considered below. It is usually very complex to

calculate $f_{n,R}^{(0)}(u)$ directly by (64) as it involves the convolution of a lot of terms, so we propose a numerical algorithm below. To begin with, the interval $[0,1)$ is discretized into N equal-length cells. For N sufficiently large, $f_{n,R}^{(i)}(u)$ for $u \in [0,1)$ can be approximated by $f_{n,R}^{(i)}(k/N)$, where $k \in [0:N)$. For simplicity, $f_{n,R}^{(i)}(k/N)$ will be abbreviated to $f_{n,R}^{(i)}(k)$, while the meanings of $f_{n,R}^{(i)}(k|x)$ and $p_i(x|k)$ are similar. Initially, $f_{n,R}^{(n)}(k) \equiv 1$ for all $k \in [0:N)$. Let $H = \mathrm{rnd}(N2^{-R})$ and $L = (N-H)$. First, we calculate

$$f_{n,R}^{(i)}(k|x) = \begin{cases} f_{n,R}^{(i+1)}(\mathrm{rnd}((k-xL)2^R)), & k \in \{xL + [0:H)\} \\ 0, & k \in \{(1-x)H + [0:L)\} \end{cases}. \tag{82}$$

Then $f_{n,R}^{(i)}(k|x)$ is normalized by

$$f_{n,R}^{(i)}(k|x) = N f_{n,R}^{(i)}(k|x) \Big/ \sum_{k=0}^{N-1} f_{n,R}^{(i)}(k|x)\ . \tag{83}$$

Next we obtain $f_{n,R}^{(i)}(k) = \frac{1}{2}\sum_{x\in\mathbb{B}} f_{n,R}^{(i)}(k|x)$ and $p_i(x|k) = f_{n,R}^{(i)}(k|x)/(2f_{n,R}^{(i)}(k))$. Finally, the ACC scaling factor can be obtained through

$$\eta \approx \frac{1}{N}\sum_{k=0}^{N-1}\left(f_{n,R}^{(0)}(k)\right)^2 \tag{84}$$

and the block-wise rate loss can be obtained through

$$-h(U_{0,n}) \approx \frac{1}{N}\sum_{k=0}^{N-1} f_{n,R}^{(0)}(k)\log_2 f_{n,R}^{(0)}(k). \tag{85}$$

In fact, the above numerical algorithm is very similar to the one proposed in [18], except that the clip operation, which bounds $\mathrm{rnd}((k-xL)2^R)$ to be within $[0:N)$, is ignored in (82). Let us first explain why the clip operation in (82) is unnecessary for the case of $x=0$. In (82), if $x=0$, we have $0 \le \mathrm{rnd}(k2^R) \le \mathrm{rnd}((H-1)2^R)$ for $k \in [0:H)$. Since $H = \mathrm{rnd}(N2^{-R})$, we have $(H - N2^{-R}) \in (-0.5, 0.5]$ and further $(H-1) \le (N2^{-R} - 0.5)$, which is followed by $(H-1)2^R \le (N - 2^{R-1})$. Since $2^{R-1} \in (0.5,1)$ for $R \in (0,1)$, we have $(N-2^{R-1}) \in (N-1, N-0.5)$. Therefore,

$$0 \le \mathrm{rnd}(k2^R) \le \mathrm{rnd}((H-1)2^R) \le \mathrm{rnd}(N-2^{R-1}) < N, \tag{86}$$

showing that $\mathrm{rnd}(k2^R)$ never goes beyond $[0:N)$ and thus the clip operation is unnecessary in (82) when $x=0$. As for the case of $x=1$, the analysis is very similar, so it is omitted. Removing the clip operation from (82) will reduce the computational complexity.

TABLE I

EXAMPLES OF $\psi_{n,R}(n)$

R	$1/6$	$2/6$	$3/6$	$4/6$	$5/6$
Experimental	0.7089	0.1406	0.0267	0.0077	0.0011
(32)	0.3826	0.0689	0.0133	0.0031	0.0004
(37)	0.7065	0.1377	0.0269	0.0059	0.0010

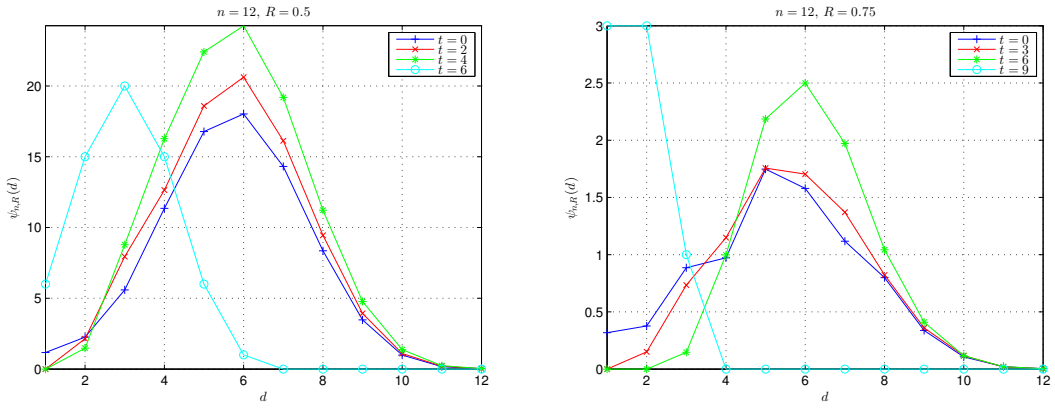
IX. EXPERIMENTAL RESULTS

This section presents four experiments to verify the above analysis from different aspects. We use the first experiment to verify the correctness of (37), the refined formula for $\psi_{n,R}(n)$. Then some examples of the HDS of tailed DAC are given. Next, we show how $\psi_{n,R}(d)$ for small d varies w.r.t. tail length t. Finally, some examples are given to illustrate how the ACC and rate loss of tailed DA codes varies w.r.t. tail length t.

A. *Refined Formula for* $\psi_{n,R}(n)$

Table I gives some examples of $\psi_{n,R}(n)$ for $n = 12$ and $t = 0$. The experimental results are obtained by a real 32-bit DAC codec through the method described in [20]. According to (39), the principle of the method in [20] is to generate a lot of source blocks and count the number of source blocks x^n's whose $s(x^n)$'s fall within $((2^{nR-1}-1), 2^{nR-1})$. Let $ntries$ be the number of trials. According to the central limit theorem, for $ntries$ sufficiently large and $\psi_{n,R}(n)$ not too near to 0 or 1, the experimental result of $\psi_{n,R}(n)$ averaged over $ntries$ trials approximately obeys the normal distribution $\mathcal{N}(\mu, \sigma^2)$, where $\mu = \psi_{n,R}(n)$ and $\sigma^2 = \frac{\psi_{n,R}(n)(1-\psi_{n,R}(n))}{ntries} \leq \frac{1}{4*ntries}$. As $ntries$ increases, σ^2 will go down and when $ntries = 10^4$, $\sigma \leq 1/200$. According to the 3-sigma rule, when $ntries = 10^4$, the probability that the experimental result of $\psi_{n,R}(n)$ falls within $(\psi_{n,R}(n) - 3/200, \psi_{n,R}(n) + 3/200)$ is larger than 99.7%. Thus, each experimental result in Tab. I, which is the average over 10^4 trials, is statistically solid.

In Table I, (32) gives exactly the same results of $\psi_{n,R}(n)$ as reported in [20], while (37) gives the refined results of $\psi_{n,R}(n)$. It can be seen that the results of $\psi_{n,R}(n)$ obtained from (37) are very close to those results obtained from the real DAC codec. It can also be seen that the results of $\psi_{n,R}(n)$ obtained from (32) are roughly half of those results obtained from the



(a) (b)

Fig. 3. Examples of DAC HDS for different tail lengths, where code length $n = 12$. The results are obtained by (32) with refined $\psi_{n,R}(n)$ using (37). (a) $R = 0.5$. (b) $R = 0.75$.

real DAC codec. Similar results are also obtained for other settings of n and R. These findings convincingly support the correctness of (37) and the analysis in Subsect. IV-C.

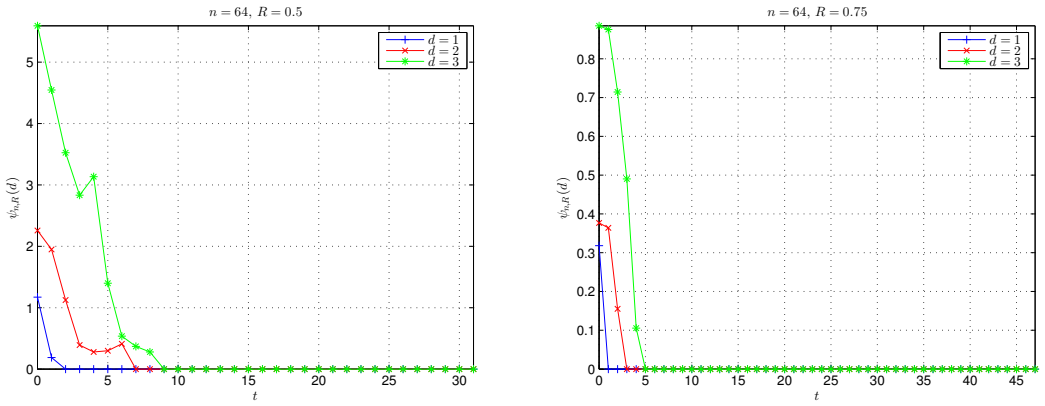
Another finding from Tab. I is that $\psi_{n,R}(n)$ is monotonically decreasing w.r.t. R. As $R \to 0$, $f^{(0)}_{n,R}(u)$ will tend to $\delta(u - 0.5)$, so $\psi_{n,R}(n)$ will tend to 1; while as $R \to 1$, $f^{(0)}_{n,R}(u)$ will tend to $\Pi(u)$, so $\psi_{n,R}(n)$ will tend to 0.

B. HDS of Tailed DAC

The second experiment studies the effect of tail length t on the HDS of DA codes. Some examples are given in Fig. 3, where code length $n = 12$. The results in Fig. 3 are obtained by (32) with refined $\psi_{n,R}(n)$ using (37). In Fig. 3(a), we set $R = 0.5$ and thus $t \in [0 : nR] = [0 : 6]$. In Fig. 3(b), we set $R = 0.75$ and thus $t \in [0 : nR] = [0 : 9]$. It can be seen that, as t increases (not very near to bitstream length nR), $\psi_{n,R}(d)$ will tend to be smaller (and even become 0 in some cases) for small d but tend to be larger for large d. Note that the HDS when $t = nR$ is very different from the HDS's in other cases. Thus, the correctness of (44) is verified.

C. Closely-Spaced Fellow Codewords

The third experiment studies the effect of tail length t on $\psi_{n,R}(d)$ for small d. Two examples are given in Fig. 4, where code length $n = 64$ and code rate $R = 0.5$ or 0.75. The results in Fig.



(a) (b)

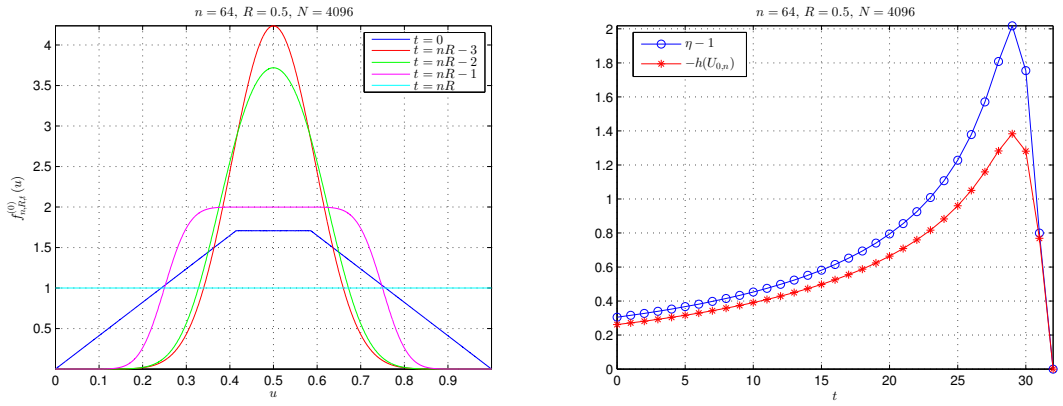
Fig. 4. Effect of tail length on $\psi_{n,R}(d)$ for small d, where $n = 64$. The results are obtained by (32). (a) $R = 0.5$. (b) $R = 0.75$.

4 are obtained by (32). It can be seen that in general, $\psi_{n,R}(d)$ for small d tends to be smaller as t increases, implying that closely-spaced fellow codewords can be removed by increasing tail length t (not very near to bitstream length nR). However, it must be pointed out that the decrease of $\psi_{n,R}(d)$ for small d w.r.t. t is not strictly monotonous, so tail length t should be carefully chosen in practice to optimize the overall performance.

D. Average Codebook Cardinality and Rate Loss

The last experiment studies the effect of tail length t on the ACC and rate loss of DA codes. Since both ACC and rate loss are closely related to the initial CCS, some examples of $f^{(0)}_{n,R,t}(u)$ are given in Fig. 5(a), where $n = 64$ and $R = 0.5$. By comparing the curve of $t = 0$ with the curve of $t = (nR - 3)$, it can be seen that for t not very close to nR, $f^{(0)}_{n,R,t}(u)$ does tend to be spikier as t increases. However, as t approaches nR, there is an opposite trend, i.e., $f^{(0)}_{n,R,t}(u)$ tends to be flatter. In the extreme case of $t = nR$, $f^{(0)}_{n,R,t}(u)$ is uniform over $[0, 1)$.

Correspondingly, some examples of $(\eta - 1)$ and $-h(U_{0,n})$ versus t are given in Fig. 5(b), where $n = 64$ and $R = 0.5$. Note that η and $-h(U_{0,n})$ are obtained by (84) and (85), respectively. It can be seen that, for t not very near to nR, both η and $-h(U_{0,n})$ will go up as t increases, meaning a higher decoding complexity and a larger rate loss. This is the negative effect of increasing tail length. As t approaches nR, there is an opposite trend: Both η and $-h(U_{0,n})$ will go down. In



(a) (b)

Fig. 5. Examples of initial CCS, ACC scaling factor, and rate loss of DA codes, were $n = 64$ and $R = 0.5$. The results are obtained by the numerical algorithm given in Sect. VIII with cell number $N = 4096$. (a) Initial CCS of DA codes versus tail length. (b) ACC scaling factor and rate loss of DA codes versus tail length.

the extreme case of $t = nR$, $\eta = 1$ and $-h(U_{0,n}) = 0$. The reason is: When $t = nR$, $X^{n(1-R)}$ is not transmitted, while $X^n_{n(1-R)}$ is transmitted in its uncoded form, so there is no rate loss for uniform binary sources. However, as shown by (44) and Fig. 3, the HDS is indeed a binomial function when $t = nR$, so DAC's performance is very poor in this case.

X. Conclusion

This paper discusses the effect of tail length on DA codes from two aspects: HDS and CCS. Both exact and approximate HDS formulas are derived for tailless DAC and extended to tailed DAC. It is revealed that closely-spaced fellow codewords can be removed by increasing tail length to a value not near to bitstream length, which explains the superiority of tailed DAC over tailless DAC. On the basis of CCS, the ACC and rate loss of tailed DAC are derived and it is shown that increasing tail length to a value not near to bitstream length will raise decoding complexity and rate loss. These findings indicate that increasing tail length will usually bring both positive (removing closely-spaced fellow codewords) and negative (raising decoding complexity and rate loss) effects, so tail length should be selected carefully to optimize the overall performance. However, it is also found that the effects of tail length are sometimes surprising, e.g., $\psi_{n,R}(d)$ for small d may not be strictly decreasing w.r.t. t. Thus, optimizing tail length of DA codes is a very difficult open issue in practice that will be tackled in the future.

REFERENCES

[1] J. Rissanen, "Generalized Kraft inequality and arithmetic coding," *IBM J. Research & Development*, vol. 20, no. 3, pp. 198–203, May 1976.

[2] I. Witten, R. Neal, and J. Cleary, "Arithmetic coding for data compression," *Commun. of the ACM*, vol. 30, no. 6, pp. 520–540, Jun. 1987.

[3] M. Grangetto, E. Magli, and G. Olmo, "Distributed arithmetic coding," *IEEE Commun. Lett.*, vol. 11, no. 11, pp. 883–885, Nov. 2007.

[4] M. Grangetto, E. Magli, and G. Olmo, "Distributed arithmetic coding for the Slepian-Wolf problem," *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2245–2257, Jun. 2009.

[5] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[6] J. Garcia-Frias and Y. Zhao, "Compression of correlated binary sources using turbo codes," *IEEE Commun. Lett.*, vol. 5, no. 10, pp. 417–419, Oct. 2001.

[7] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[8] M. Grangetto, E. Magli, and G. Olmo, "Security applications of distributed arithmetic coding," in: *Proc. 18th European Signal Process. Conf.* (EUSIPCO-2010), pp.2151–2155, Aalborg, Denmark, Aug. 23–27, 2010.

[9] X. Artigas, S. Malinowski, C. Guillemot, and L. Torres, "Overlapped quasi-arithmetic codes for distributed video coding," in: *Proc. IEEE ICIP*, 2007, vol. II, pp. 9–12.

[10] S. Malinowski, X. Artigas, C. Guillemot, and L. Torres, "Distributed coding using punctured quasi-arithmetic codes for memory and memoryless sources," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4154–4158, Oct. 2009.

[11] X. Chen and D. Taubman, "Distributed source coding based on punctured conditional arithmetic codes," in: *Proc. IEEE ICIP*, pp. 3713–3716, Sep. 2010.

[12] X. Chen and D. Taubman, "Coupled distributed arithmetic coding," in: *Proc. IEEE ICIP*, pp. 341–344, Sep. 2011.

[13] J. Zhou, K. Wong, and J. Chen, "Distributed block arithmetic coding for equiprobable sources," *IEEE Sensors Journal*, vol. 13, no. 7, pp. 2750–2756, Jul. 2013.

[14] M. Grangetto, E. Magli, R. Tron, and G. Olmo, "Rate-compatible distributed arithmetic coding," *IEEE Commun. Lett.*, vol. 12, no. 8, pp. 575–577, Aug. 2008.

[15] M. Grangetto, E. Magli, and G. Olmo, "Distributed joint source-channel arithmetic coding," in: *Proc. IEEE Int'l Conf. Image Process. (ICIP)*, 2010, pp. 3717–3720.

[16] Y. Keshtkarjahromi, M. Valipour, and F. Lahouti, "Multi-level distributed arithmetic coding with nested lattice quantization," in: *Proc. IEEE Data Compression Conference (DCC)*, pp. 382–391, Mar. 26–28, 2014.

[17] Z. Wang, Y. Mao, and I. Kiringa, "Non-binary distributed arithmetic coding," in: *Proc. IEEE 14th Canadian Workshop Inform. Theory (CWIT)*, pp. 5–8, Jul. 2015.

[18] Y. Fang, "DAC spectrum of binary sources with equally-likely symbols," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1584–1594, Apr. 2013.

[19] Y. Fang and L. Chen, "Improved binary DAC codec with spectrum for equiprobable sources," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 256–268, Jan. 2014.

[20] Y. Fang, V. Stankovic, S. Cheng, and E.-H. Yang, "Hamming Distance spectrum of DAC codes for equiprobable binary sources," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1232–1245, Mar. 2016.