Error Probability of Distributed Arithmetic Coding

Yong Fang, Nan Yang, and Jun Chen, *Senior Member, IEEE*

***Abstract*— Distributed Arithmetic Coding (DAC) is an interesting realization of Slepian-Wolf coding that performs nonlinear coset-like partition for equiprobable binary sources. Just as in other coding problems, it is a very important issue to theoretically predict the decoding error probability of DAC. This letter proposes a plausible solution to this difficult issue. Our analyses are based on the concept of coexisting interval introduced in our previous work. Specifically, we use it to deduce the probability that two given codewords coexist in the same coset. Experimental results confirm the correctness of our theoretical analyses.**

***Index Terms*— Distributed arithmetic coding, Slepian-Wolf coding, coexisting interval, frame error rate.**

I. Introduction

DISTRIBUTED Arithmetic Coding (DAC) [1] is an interesting realization of Slepian-Wolf coding [2]. Although there are a lot of researches surrounding DAC, most of them focus on the applications or extensions of DAC, and there are very few theoretical analyses.

It is well-known that for equiprobable binary sources, DAC can be classified into coset codes. For any coset code, there are three important theoretical problems of increasing difficulty: (a) *decoder design*; (b) *Hamming distance distribution*; and (c) *decoding error probability*. The situations for DAC are even more challenging, because the non-linearity of DAC brings another theoretical problem: *coset cardinality distribution*. In our previous work on DAC, we addressed the issues of *coset cardinality distribution* [3], *decoder design* [4], and *Hamming distance distribution* [5]. Now in this letter, we try to handle the most difficult problem—*theoretical prediction of decoding error probability*. The tool for our analyses is *coexisting interval* [6] (originally named as *risky interval* in [5]), which was defined in our previous work to derive the Hamming distance distribution for DAC [5], [6]. On the basis of coexisting interval, this letter proposes an enumerative algorithm to predict the decoding error probability of DAC, whose correctness is confirmed by experiments. However, we should point out that the proposed algorithm in its current form is not suitable for the large-code-length regime due to its high complexity. Nevertheless, it suggests a principled approach to theoretically predicting the decoding error probability for DAC and paves the way for further development.

The rest of this letter is arranged as below. Sect. II briefly reviews the background knowledge of DAC and coexisting interval. Sect. III shows how to calculate the decoding error probability of DAC if all but the last symbol of each block are known at the decoder. Sect. IV first shows how to calculate the decoding error probability of DAC if all but the last two symbols of each block are known at the decoder, and then generalizes the enumerative algorithm to the case that there are an arbitrary number of erroneous symbols. Sect. V gives some experimental results to verify the analyses. Finally, Sect. VI concludes this letter.

II. Review of Coexisting Interval

For equiprobable binary sources, the symbol-to-interval mapping rule of a rate-R distributed arithmetic codec is

$$x \to [x(1-q), q + x(1-q)), \tag{1}$$

where $x \in \mathbb{B} \triangleq \{0,1\}$ and $q = 2^{-R}$. The rate-R distributed arithmetic encoder maps every length-n binary block $x^n \triangleq (x_1, \ldots, x_n) \in \mathbb{B}^n$ onto a real number over $[0, 2^{nR} - 1]$ [5] (for simplicity, we assume $nR \in \mathbb{Z}$ in this letter):

$$s(x^n) \triangleq (1-q) q^{-(n+1)} \sum_{i=1}^{n} x_i q^i. \tag{2}$$

Let $[i:j) \triangleq \{i, i+1, \ldots, j-1\}$ be a set of integers. The rate-R DAC bitstream of x^n is

$$m(x^n) \triangleq \lceil s(x^n) \rceil \in [0 : 2^{nR}) \subset \mathbb{Z}, \tag{3}$$

where $\lceil \cdot \rceil$ denotes the ceiling function. The (n, R) distributed arithmetic code is to a great extent like a channel code that partitions source space $\mathbb{B}^n$ into 2^{nR} cosets. Let us denote the m-th DAC coset as $\mathcal{C}_m \triangleq \{x^n : \lceil s(x^n) \rceil = m\}$. Since the coset $\mathcal{C}_0$ includes only one codeword 0^n [5], we will ignore the case $m = 0$ in the following. Let $j^d \triangleq (j_1, \ldots, j_d)$ and $b^d \triangleq (b_1, \ldots, b_d)$. We define the following set:

$$\mathcal{J}_{n,d} \triangleq \{j^d : 1 \le j_1 < j_2 < \cdots < j_d \le n\}. \tag{4}$$

For $j^d \in \mathcal{J}_{n,d}$ and $b^d \in \mathbb{B}^d$, we define [5]

$$\begin{aligned} \tau(j^d, b^d) &\triangleq (1-q) q^{-(n+1)} \sum_{d'=1}^{d} (-1)^{b_{d'}} q^{j_{d'}} \\ &= -\tau(j^d, b^d \oplus 1^d). \end{aligned} \tag{5}$$

Manuscript received August 13, 2021; revised September 14, 2021; accepted September 18, 2021. Date of publication September 22, 2021; date of current version December 10, 2021. The work was supported by the National Key Research and Development Program of China (grant no. 2020YFB0505602), the Open Research Fund of the Shaanxi Province Key Laboratory of Information Communication Network and Security, China (grant no. ICNS202002), the National Science Foundation of China (grant no. 62071377), and the Natural Science Basic Research Program of Shaanxi Province, China (grant no. 2021JM-188). The associate editor coordinating the review of this letter and approving it for publication was M.-R. Sadeghi. *(Corresponding author: Yong Fang.)*

Yong Fang and Nan Yang are with the School of Information Engineering, Chang'an University, Xi'an, Shaanxi 710064, China (e-mail: fy@chd.edu.cn; nyang@chd.edu.cn).

Jun Chen is with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4K1, Canada (e-mail: chenjun@mcmaster.ca).

Digital Object Identifier 10.1109/LCOMM.2021.3114591

1558-2558 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: McMaster University. Downloaded on September 27,2023 at 20:58:12 UTC from IEEE Xplore. Restrictions apply.

For interval $\mathcal{I} = (a, b]$, we define $(a, b] + \tau \triangleq (a + \tau, b + \tau]$.

Definition of Coexisting Interval: For $m \in [1 : 2^{nR})$,

$$\mathcal{I}_m(j^d, b^d) \triangleq \{(m-1, m] - \tau(j^d, b^d)\} \cap (m-1, m]. \quad (6)$$

Physical Meaning of Coexisting Interval: Consider two binary blocks $x^n \in \mathbb{B}^n$ and $\tilde{x}^n \in \mathbb{B}^n$. Let $z^n = x^n \oplus \tilde{x}^n$. Let $[n] \triangleq \{1, \ldots, n\}$. Assume $z_{j^d} \triangleq (z_{j_1}, \ldots, z_{j_d}) = 1^d$ and $z_{[n]\setminus j^d} = 0^{n-d}$. From (2) and (5), it is easy to know

$$s(\tilde{x}^n) = s(x^n) + \tau(j^d, x_{j^d}). \quad (7)$$

The following properties of $\mathcal{I}_m(j^d, b^d)$ are obvious:

- $\mathcal{I}_m(j^d, b^d)$ and $\mathcal{I}_m(j^d, b^d \oplus 1^d)$ are almost symmetric around $(m - 0.5)$ (except at the ends of intervals).
- If $|\tau(j^d, b^d)| \geq 1$, $\mathcal{I}_m(j^d, b^d) = \mathcal{I}_m(j^d, b^d \oplus 1^d) = \emptyset$; If $0 \leq \tau(j^d, b^d) < 1$, $\mathcal{I}_m(j^d, b^d) = (m-1, m-\tau(j^d, b^d)]$; If $-1 < \tau(j^d, b^d) \leq 0$, $\mathcal{I}_m(j^d, b^d) = (m - 1 - \tau(j^d, b^d), m]$.
- Let $|\mathcal{I}|$ be the length of continuous interval $\mathcal{I}$. Then $|\mathcal{I}_m(j^d, b^d)| = |\mathcal{I}_m(j^d, b^d \oplus 1^d)| = \ell(j^d, b^d)$, where

$$\ell(j^d, b^d) \triangleq \max(0, 1 - |\tau(j^d, b^d)|) \in [0, 1]. \quad (8)$$

If $s(x^n) \in \mathcal{I}_m(j^d, x_{j^d})$, then

$$\lceil s(\tilde{x}^n) \rceil = \lceil s(x^n) + \tau(j^d, x_{j^d}) \rceil = \lceil s(x^n) \rceil = m, \quad (9)$$

i.e., x^n and $\tilde{x}^n$ coexist in the same coset $\mathcal{C}_m$. Otherwise, if $s(x^n) \in (m-1, m] \setminus \mathcal{I}_m(j^d, x_{j^d})$, then $x^n \in \mathcal{C}_m$ but $\tilde{x}^n \notin \mathcal{C}_m$, *i.e.*, they do not coexist in the same coset.

Definition of Coexisting Interval Set:

$$\mathcal{I}(j^d, b^d) \triangleq \left\{\mathcal{I}_m(j^d, b^d) : m \in [1 : 2^{nR})\right\}. \quad (10)$$

According to (5), the definition of $\tau(j^d, b^d)$, and (6), the definition of $\mathcal{I}_m(j^d, b^d)$, the following theorem holds obviously.

Theorem 1: Let X^n and $\tilde{X}^n$ be two binary blocks. Let $Z^n = X^n \oplus \tilde{X}^n$, where $Z_{[n]\setminus j^d} = 0^{n-d}$ and $Z_{j^d} = 1^d$. Given $X_{j^d} = b^d$, the necessary and sufficient condition for $\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil$, *i.e.*, X^n and $\tilde{X}^n$ coexist in the same coset, is $s(X^n) \in \mathcal{I}(j^d, b^d)$. We denote this equivalence as

$$\{\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil\} \leftrightarrow \{s(X^n) \in \mathcal{I}(j^d, X_{j^d})\}. \quad (11)$$

If $\lceil s(X^n) \rceil = m$, $s(X^n)$ will be uniformly distributed over $(m-1, m]$ as $n \to \infty$ [5], so we have the following theorem.

Theorem 2: Given $X_{j^d} = b^d$, as code length n approaches infinity, the probability of $s(X^n)$ falling into $\mathcal{I}(j^d, b^d)$ is equal to $\ell(j^d, b^d)$. Define the event $\mathcal{E} \triangleq \{s(X^n) \in \mathcal{I}(j^d, b^d)\}$. Then

$$\lim_{n\to\infty} \Pr\{\mathcal{E} | X_{j^d} = b^d\} = \lim_{n\to\infty} \ell(j^d, b^d). \quad (12)$$

III. Analysis on the Last Symbol

Equipped with the concept of coexisting interval, we can make use of it to compute the decoding error probability of DAC. Due to the difficult nature of this problem, we will start with some simple cases. It was found in [5] that the residual errors of DAC after decoding usually happen at the end of each block, so we will begin with the simplest case: *All but the last* symbol of each block are known at the decoder. Note that in [4], the simplest case has been analyzed without utilizing coexisting interval. Now in this section, we will show how to handle the simplest case with the help of coexisting interval.

Let X^n be the source and Y^n be the side information available only at the decoder. Assume that the correlation between X^n and Y^n is modeled as a *binary symmetric channel* (BSC) with crossover probability ϵ. Let $Z^n = X^n \oplus Y^n$. Then the event $X_i \neq Y_i$ is equivalent to the event $Z_i = 1$. On receiving DAC bitstream $M = \lceil s(X^n) \rceil$, the ideal distributed arithmetic decoder will search through the coset $\mathcal{C}_M$ to find the codeword closest (in Hamming distance) to Y^n, which is denoted by $\hat{X}^n$, and takes it as the estimate of X^n. The *frame-error-rate* (FER) after decoding is $\Pr\{e\}$, where e denotes the event $\{\hat{X}^n \neq X^n | Y^n\}$. If X^{n-1} is known at the decoder, then $\hat{X}^{n-1} \equiv X^{n-1}$. The conditional FER given X^{n-1} is

$$\Pr\{e|X^{n-1}\} = \Pr\{\hat{X}_n \neq X_n | Y_n\} < \Pr\{e\}. \quad (13)$$

Let us define $\tilde{X}^n \triangleq (X^n \oplus (0^{n-1}, 1))$, which is called *shadow codeword* of X^n. Note that:

- If $\lceil s(X^n) \rceil \neq \lceil s(\tilde{X}^n) \rceil$, decoding will always succeed, regardless of side information Y^n;
- If $\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil$, decoding correctness purely depends on Y_n.

By Theorem 1, the equivalent event of $\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil$ is $s(X^n) \in \mathcal{I}(n, X_n)$:

$$\{\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil\} \leftrightarrow \{s(X^n) \in \mathcal{I}(n, X_n)\}. \quad (14)$$

Now it is obvious that

$$\Pr\{\hat{X}_n \neq X_n | Y_n\} = \Pr\{\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil\} \cdot \Pr\{X_n \neq Y_n\}, \quad (15)$$

where $\Pr\{X_n \neq Y_n\} = \epsilon$ and

$$\Pr\{\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil\} = \sum_{b\in\mathbb{B}} \Pr\{X_n = b\} \cdot \Pr\{s(X^n) \in \mathcal{I}(n, b) | X_n = b\}. \quad (16)$$

By Theorem 2, we can obtain

$$\lim_{n\to\infty} \Pr\{\lceil s(X^n) \rceil = \lceil s(\tilde{X}^n) \rceil\} = \lim_{n\to\infty} (\ell(n, 0) + \ell(n, 1))/2 = 1 - (1 - q)q^{-1}. \quad (17)$$

Finally, we obtain the lower bound [4]

$$\lim_{n\to\infty} \Pr\{\hat{X}_n \neq X_n | Y_n\} = (2 - 2^R)\epsilon. \quad (18)$$

IV. Analysis on the Last Two Symbols

After understanding the simplest case, now we consider a slightly more complex case: *All but the last two* symbols of each block are known at the decoder. It will be seen that the analysis in the second simplest case is much more difficult than that in the simplest case, and the extension from case one to case two is not straightforward. Let $\Pr\{e|X^{n-2}\}$ be the conditional FER given X^{n-2} at the decoder, then

$$\Pr\{e|X^{n-2}\} = \Pr\{\hat{X}^n_{n-1} \neq X^n_{n-1} | Y^n_{n-1}\}, \quad (19)$$

Authorized licensed use limited to: McMaster University. Downloaded on September 27,2023 at 20:58:12 UTC from IEEE Xplore. Restrictions apply.

where $X_{n-1}^n = (X_{n-1}, X_n)$. Define $(2^2-1) = 3$ shadow codewords of X^n:

$$\begin{cases} \tilde{X}_{01}^n = (X^n \oplus (0^{n-2}, 0, 1)) \\ \tilde{X}_{10}^n = (X^n \oplus (0^{n-2}, 1, 0)) \\ \tilde{X}_{11}^n = (X^n \oplus (0^{n-2}, 1, 1)). \end{cases} \tag{20}$$

Let $\mathcal{E}_{01} \triangleq \{\lceil s(\tilde{X}_{01}^n)\rceil = \lceil s(X^n)\rceil\}$ and $\bar{\mathcal{E}}_{01} \triangleq \{\lceil s(\tilde{X}_{01}^n)\rceil \neq \lceil s(X^n)\rceil\}$. $\mathcal{E}_{10}$, $\bar{\mathcal{E}}_{10}$, $\mathcal{E}_{11}$, and $\bar{\mathcal{E}}_{11}$ are similarly defined. Then

$$\begin{cases} \mathcal{E}_{01} \leftrightarrow \{s(X^n) \in \mathcal{I}(n, X_n)\} \\ \mathcal{E}_{10} \leftrightarrow \{s(X^n) \in \mathcal{I}(n-1, X_{n-1})\} \\ \mathcal{E}_{11} \leftrightarrow \{s(X^n) \in \mathcal{I}((n-1, n), X_{n-1}^n)\}. \end{cases} \tag{21}$$

A. Enumeration of Event Combinations

There are $2^{2^2-1} = 2^3 = 8$ event combinations in total.

1) $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} \cap \bar{\mathcal{E}}_{11}$: The decoding succeeds always.
2) $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \bar{\mathcal{E}}_{11}$: If $Y_n \neq X_n$, the decoding fails, so the failure probability is ϵ.
3) $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11}$: As case 2, the failure probability is ϵ.
4) $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11}$: If $Z_{n-1}^n = 1^2$, the decoding fails; if $Z_{n-1}^n = (1,0)$ or $(0,1)$, $d_H(Y^n, \tilde{X}_{11}^n) = d_H(Y^n, X^n) = 1$, where $d_H(\cdot,\cdot)$ denotes the Hamming distance function, so the failure probability is 0.5. The overall failure probability is

$$\begin{aligned} &\Pr\{Z_{n-1}^n = 1^2\} \\ &\quad + (1/2)\left(\Pr\{Z_{n-1}^n = (1,0)\} + \Pr\{Z_{n-1}^n = (0,1)\}\right) \\ &= \epsilon^2 + (1/2)(\epsilon(1-\epsilon) + (1-\epsilon)\epsilon) = \epsilon. \end{aligned} \tag{22}$$

5) $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11}$: If $Y_n \neq X_n$, the decoding will fail; if $Z_{n-1}^n = (1,0)$, we have $d_H(Y^n, \tilde{X}_{01}^n) = 2$ and $d_H(Y^n, \tilde{X}_{11}^n) = d_H(Y^n, X^n) = 1$, so the failure probability is 0.5. The overall failure probability is

$$\begin{aligned} &\Pr\{Y_n \neq X_n\} + (1/2)\Pr\{Z_{n-1}^n = (1,0)\} \\ &\quad = \epsilon + \epsilon(1-\epsilon)/2 = \epsilon(3-\epsilon)/2. \end{aligned} \tag{23}$$

6) $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11}$: This case is a mirror image of case 5 by swapping the roles of (X_{n-1}, Y_{n-1}) and (X_n, Y_n), so the failure probability is also $\epsilon(3-\epsilon)/2$.
7) $\mathcal{E}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11}$: The decoding succeeds only if $X_{n-1}^n = Y_{n-1}^n$, so the failure probability is

$$1 - \Pr\{Z_{n-1}^n = 0^2\} = 1 - (1-\epsilon)^2 = \epsilon(2-\epsilon). \tag{24}$$

8) $\mathcal{E}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11}$: The decoding succeeds only if $X_{n-1}^n = Y_{n-1}^n$, so the failure probability is also $\epsilon(2-\epsilon)$.

The failure probabilities in case 7 and case 8 are the same, so we merge them to obtain

$$(\mathcal{E}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11}) \cup (\mathcal{E}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11}) = \mathcal{E}_{01} \cap \mathcal{E}_{10}. \tag{25}$$

Finally, we will obtain

$$\begin{aligned} &\Pr\{e|X^{n-2}\} \\ &= \epsilon(2-\epsilon) \cdot \Pr\{\mathcal{E}_{01} \cap \mathcal{E}_{10}\} \\ &\quad + \epsilon \cdot \left(\Pr\{\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \bar{\mathcal{E}}_{11}\} + \Pr\{\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11}\}\right. \\ &\quad \left. + \Pr\{\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11}\}\right) + \epsilon(3-\epsilon)/2 \cdot \left(\Pr\{\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11}\}\right. \\ &\quad \left. + \Pr\{\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11}\}\right). \end{aligned} \tag{26}$$

The problem now is how to determine the probabilities of $\mathcal{E}_{01}$, $\mathcal{E}_{10}$, and $\mathcal{E}_{11}$. To achieve this goal, we should consider different b^2. Let $\Pr\{e|X^{n-2}, X_{n-1}^n = b^2\}$ be the FER given X^{n-2} known at the decoder and $X_{n-1}^n = b^2$. Then

$$\Pr\{e|X^{n-2}\} = \frac{1}{4} \sum_{b^2 \in \mathbb{B}^2} \Pr\{e|X^{n-2}, X_{n-1}^n = b^2\}. \tag{27}$$

B. Enumeration of Last Two Symbols

1) Case $X_{n-1}^n = 0^2$: According to the definition of $\tau(j^d, b^d)$, we have

$$\begin{cases} \tau(n, 0) = (1-q)q^{-1} > 0 \\ \tau(n-1, 0) = (1-q)q^{-2} > 0 \\ \tau((n-1, n), 0^2) = \tau(n, 0) + \tau(n-1, 0) > 0. \end{cases} \tag{28}$$

If $q \in (0.5, 1)$, then $\tau(n, 0) \in (0, 1)$, $\tau(n-1, 0) \in (0, 2)$, and $\tau((n, n-1), 0^2) \in (0, 3)$. Thus,

$$\begin{cases} \mathcal{I}_m(n, 0) = ((m-1), (m - \tau(n, 0))] \neq \emptyset \\ \mathcal{I}_m(n-1, 0) = ((m-1), (m - \min(1, \tau(n-1, 0)))] \\ \mathcal{I}_m((n, n-1), 0^2) = \\ \qquad ((m-1), (m - \min(1, \tau((n, n-1), 0^2)))]. \end{cases} \tag{29}$$

It is easy to get

$$0 < \tau(n, 0) < \tau(n-1, 0) < \tau((n, n-1), 0^2). \tag{30}$$

Hence,

$$\mathcal{I}((n, n-1), 0^2) \subset \mathcal{I}(n-1, 0) \subset \mathcal{I}(n, 0). \tag{31}$$

It can be seen that $\mathcal{I}(n, 0)$ is always non-empty, but $\mathcal{I}(n-1, 0)$ and $\mathcal{I}((n, n-1), 0^2)$ may or may not be empty, depending on the value of q. By solving $\tau(n-1, 0) = 1$, we get $2q = (\sqrt{5}-1)$; by solving $\tau((n, n-1), 0^2) = 1$, we get $2q = \sqrt{2}$. Hence we divide the interval $2q \in (1, 2)$ into three sub-intervals.

- $1 < 2q \leq (\sqrt{5}-1)$: It is easy to get $1 \leq \tau(n-1, 0) < \tau((n, n-1), 0^2)$, so $\mathcal{I}(n-1, 0) = \mathcal{I}((n, n-1), 0^2) = \emptyset$. An example is shown in Fig. 1(a) and Fig. 1(b).
- $(\sqrt{5}-1) < 2q \leq \sqrt{2}$: It is easy to get $\tau(n-1, 0) < 1 \leq \tau((n, n-1), 0^2)$, so $\mathcal{I}(n-1, 0) \neq \emptyset$ and $\mathcal{I}((n, n-1), 0^2) = \emptyset$. An example of this case is illustrated by Fig. 1(c) and Fig. 1(d).
- $\sqrt{2} < 2q < 2$: It is easy to get $\tau(n-1, 0) < \tau((n, n-1), 0^2) < 1$. Hence, $\mathcal{I}(n-1, 0) \neq \emptyset$ and $\mathcal{I}((n, n-1), 0^2) \neq \emptyset$.

According to Theorem 1, given $X_{n-1}^n = 0^2$, we have

- $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \bar{\mathcal{E}}_{11} = \mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} = \mathcal{E}_{01} \setminus \mathcal{E}_{10}$.
- $\mathcal{E}_{01} \cap \mathcal{E}_{10} = \mathcal{E}_{10}$.
- $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11} = \bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11} = \emptyset$.
- $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11} = \bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11} = \emptyset$.

Finally, we get

$$\begin{aligned} &\Pr\{e|X^{n-2}, X_{n-1}^n = 0^2\} \\ &\qquad = \epsilon \cdot \Pr\{\mathcal{E}_{01} \setminus \mathcal{E}_{10}\} + \epsilon(2-\epsilon) \cdot \Pr\{\mathcal{E}_{10}\}. \end{aligned} \tag{32}$$

Authorized licensed use limited to: McMaster University. Downloaded on September 27,2023 at 20:58:12 UTC from IEEE Xplore. Restrictions apply.

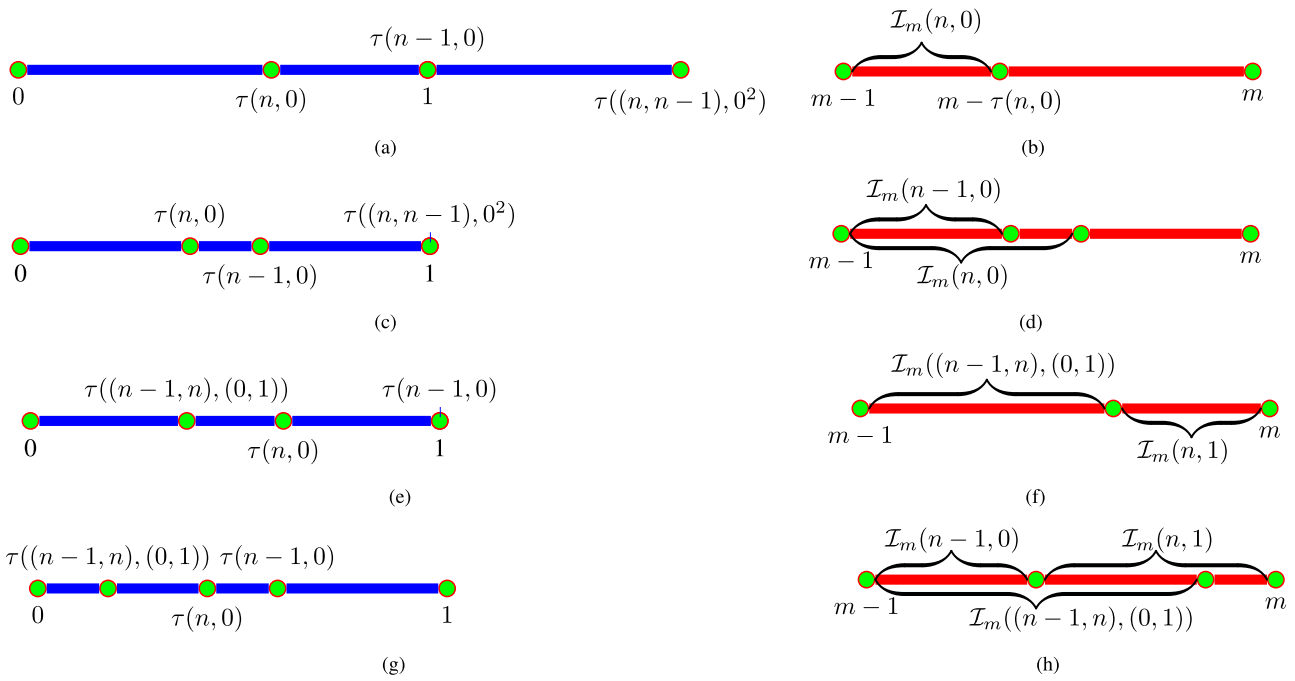

Fig. 1. Examples of $\tau(j^d, b^d)$ and $\mathcal{I}_m(j^d, b^d)$. (a) and (b): $b^2 = 0^2$ and $2q = \sqrt{5} - 1$. (c) and (d): $b^2 = 0^2$ and $2q = \sqrt{2}$. (e) and (f): $b^2 = (0,1)$ and $2q = \sqrt{5} - 1$. (g) and (h): $b^2 = (0,1)$ and $2q = \sqrt{2}$.

According to Theorem 1, we have

$$\begin{cases} \{\mathcal{E}_{01} \setminus \mathcal{E}_{10}\} \leftrightarrow \{s(X^n) \in \{\mathcal{I}(n,0) \setminus \mathcal{I}(n-1,0)\}\} \\ \mathcal{E}_{10} \leftrightarrow \{s(X^n) \in \mathcal{I}(n-1,0)\}. \end{cases} \tag{33}$$

According to Theorem 2, we have

$$\begin{cases} \lim\limits_{n\to\infty} \Pr\{\mathcal{E}_{10}\} = \lim\limits_{n\to\infty} \ell(n-1,0) \\ \qquad\qquad = 1 - \lim\limits_{n\to\infty} \min(1, \tau(n-1,0)) \\ \lim\limits_{n\to\infty} \Pr\{\mathcal{E}_{01} \setminus \mathcal{E}_{10}\} = \lim\limits_{n\to\infty} (\ell(n,0) - \ell(n-1,0)) \\ \qquad\qquad = \lim\limits_{n\to\infty} (\min(1, \tau(n-1,0)) - \tau(n,0)). \end{cases} \tag{34}$$

2) Case $X_{n-1}^n = (0,1)$: Similarly, we can obtain

$$\begin{cases} \tau(n,1) = -\tau(n,0) = -(1-q)q^{-1} < 0 \\ \tau((n-1,n),(0,1)) = \tau(n-1,0) - \tau(n,0) > 0, \end{cases} \tag{35}$$

where $\tau(n-1,0)$ and $\tau(n,0)$ are given by (28). For $q \in (0.5, 1)$, $0 < \tau((n-1,n),(0,1)) < \tau(n,0) < 1$, so

$$\begin{cases} \mathcal{I}_m(n,1) = ((m-1+\tau(n,0)), m] \neq \emptyset \\ \mathcal{I}_m((n-1,n),(0,1)) = \\ \quad ((m-1),(m-\tau((n-1,n),(0,1)))] \neq \emptyset. \end{cases} \tag{36}$$

Since $\tau((n-1,n),(0,1)) < \tau(n,0) < \tau(n-1,0)$, we have

$$\mathcal{I}(n-1,0) \subset \mathcal{I}((n-1,n),(0,1)). \tag{37}$$

Therefore, some event combinations can be simplified as

- $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \bar{\mathcal{E}}_{11} = \mathcal{E}_{01} \cap \bar{\mathcal{E}}_{11}$.
- $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \mathcal{E}_{11} = \bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10}$.
- $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11} = \emptyset$.

Depending on the value of q, event combinations can be further simplified as below

- $1 < 2q \leq (\sqrt{5} - 1)$: Clearly, $1 \leq \tau(n-1,0)$, so $\mathcal{I}(n-1,0) = \mathcal{I}(n,1) \cap \mathcal{I}((n-1,n),(0,1)) = \emptyset$. Equivalently, $\mathcal{E}_{10} = \mathcal{E}_{01} \cap \mathcal{E}_{11} = \emptyset$. If $2q = \sqrt{5} - 1$, the interval $(0, 2^{nR} - 1]$ is fully covered by $\mathcal{I}(n,1)$ and $\mathcal{I}((n-1,n),(0,1))$, so $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{11} = \emptyset$. An example is shown in Fig. 1(e) and Fig. 1(f).
- $(\sqrt{5} - 1) < 2q < 2$: Clearly, $\tau(n-1,0) < 1$, so $\mathcal{I}(n-1,0) \neq \emptyset$. In addition, $\mathcal{I}(n,1) \cap \mathcal{I}((n-1,n),(0,1)) \neq \emptyset$ and $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{11} = \emptyset$. Further, it is easy to obtain
  - $(\sqrt{5} - 1) < 2q \leq \sqrt{2}$: $\mathcal{I}(n,1) \cap \mathcal{I}(n-1,0) = \emptyset$. Equivalently, $\mathcal{E}_{01} \cap \mathcal{E}_{10} = \emptyset$. When $2q = \sqrt{2}$, the interval $(0, 2^{nR} - 1]$ is fully covered by $\mathcal{I}(n,1)$ and $\mathcal{I}(n-1,0)$, so $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} = \emptyset$. An example of this case is shown in Fig. 1(g) and Fig. 1(h).
  - $\sqrt{2} < 2q < 2$: $\mathcal{I}(n,1) \cap \mathcal{I}(n-1,0) \neq \emptyset$ and hence $\bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} = \emptyset$.

Then $\Pr\{e|X^{n-2}, X_{n-1}^n = (0,1)\}$ can be calculated by the same procedure as described for the case $X_{n-1}^n = 0^2$. For conciseness, we omit the details.

3) Case $X_{n-1}^n = (1,b)$: Due to the symmetry of $\tau(j^d, b^d \oplus 1^d) = -\tau(j^d, b^d)$, the analysis of case $X_{n-1}^n = (1,b)$ is exactly the same as that of $X_{n-1}^n = (0,b)$, so only $2^{2-1} = 2$ cases $b^2 = 0^2$ and $b^2 = (0,1)$ need to be considered.

Analysis on the General Case: After understanding the above analyses, we can extend the method to the general case. Given X^{n-t} known at the decoder, there are $2^t - 1$ shadow codewords and we can enumerate 2^{2^t-1} event combinations. For each event combination, we enumerate 2^{t-1} symbol combinations. Finally, we make use of Theorem 1 and Theorem 2 to calculate the FER. Obviously, the order of complexity is $O(2^{2^t-1} \cdot 2^{t-1}) = O(2^{2^t+t-2})$. As t increases, the complexity will go up sharply. It is left to our future work to reduce the computational complexity.

Authorized licensed use limited to: McMaster University. Downloaded on September 27,2023 at 20:58:12 UTC from IEEE Xplore. Restrictions apply.

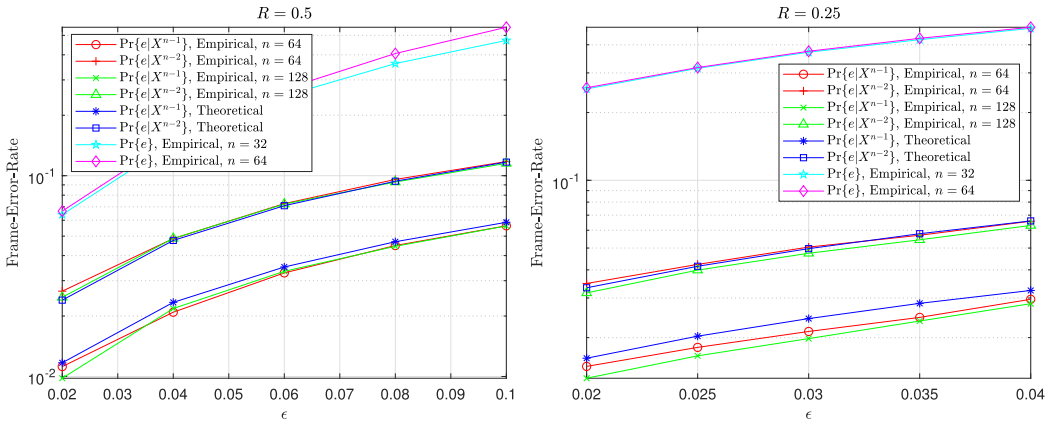

Fig. 2. Theoretical and empirical results of decoding error probability of DAC, where e denotes the event $\{\hat{X}^n \neq X^n|Y^n\}$.

V. Experimental Results

We consider two rates $R = 0.5$ and $R = 0.25$. When $R = 0.5$, according to (18), we have $\Pr\{e|X^{n-1}\} = (2-\sqrt{2})\epsilon \approx 0.5858\epsilon$. Then we consider $\Pr\{e|X^{n-2}\}$. For $X_{n-1}^n = 0^2$,

$$\begin{cases} \tau(n,0) = \sqrt{2}-1 \approx 0.4142 \\ \tau(n-1,0) = 2-\sqrt{2} \approx 0.5858 \\ \tau((n-1,n),0^2) = 1 \end{cases} \tag{38}$$

and

$$\begin{cases} \mathcal{I}_m(n,0) \approx (m-1, m-0.4142] \\ \mathcal{I}_m(n-1,0) \approx (m-1, m-0.5858] \\ \mathcal{I}_m((n-1,n),0^2) = \emptyset. \end{cases} \tag{39}$$

Thus we can get

$$\Pr\{e|X^{n-2}, X_{n-1}^n = 0^2\} \approx 0.1716\epsilon + 0.4142\epsilon(2-\epsilon). \tag{40}$$

For $X_{n-1}^n = (0,1)$, we have

$$\begin{cases} \tau(n,1) = 1-\sqrt{2} \approx -0.4142 \\ \tau((n-1,n),(0,1)) = 3-2\sqrt{2} \approx 0.1716 \end{cases} \tag{41}$$

and

$$\begin{cases} \mathcal{I}_m(n,1) \approx (m-0.5858, m] \\ \mathcal{I}_m((n-1,n),(0,1)) \approx (m-1, m-0.1716]. \end{cases} \tag{42}$$

Hence, $\mathcal{I}_m(n,1) \cap \mathcal{I}_m(n-1,0) = \emptyset$ and $\mathcal{I}_m(n,1) \cup \mathcal{I}_m(n-1,0) = (m-1,m]$. We define

$$\mathcal{R}(a,b) \triangleq \left\{(m-a, m-b] : m \in [1 : 2^{nR})\right\}. \tag{43}$$

Then the event combinations can be further simplified as:

- $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{11} \leftrightarrow \{s(X^n) \in \mathcal{R}(0.1716, 0)\}$;
- $\mathcal{E}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11} \leftrightarrow \{s(X^n) \in \mathcal{R}(0.5858, 0.1716)\}$;
- $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} = \mathcal{E}_{10} \leftrightarrow \{s(X^n) \in \mathcal{R}(1, 0.5858)\}$;
- $\bar{\mathcal{E}}_{01} \cap \mathcal{E}_{10} \cap \bar{\mathcal{E}}_{11} = \bar{\mathcal{E}}_{01} \cap \bar{\mathcal{E}}_{10} \cap \mathcal{E}_{11} = \mathcal{E}_{01} \cap \mathcal{E}_{10} = \emptyset$.

Therefore,

$$\Pr\{e|X^{n-2}, X_{n-1}^n = (0,1)\} \approx 0.1716\epsilon + 0.4142\epsilon(3-\epsilon). \tag{44}$$

Finally, when $R = 0.5$, we have

$$\begin{aligned} &\Pr\{e|X^{n-2}\} \\ &\approx \frac{1}{2}\left(0.1716\epsilon + 0.4142\epsilon(2-\epsilon) + 0.1716\epsilon + 0.4142\epsilon(3-\epsilon)\right) \\ &= 1.2071\epsilon - 0.4142\epsilon^2. \end{aligned} \tag{45}$$

Similarly, following the above analysis, when $R = 0.25$, we have $\Pr\{e|X^{n-1}\} = (2-2^{0.25})\epsilon \approx 0.8108\epsilon$ and

$$\begin{aligned} \Pr\{e|X^{n-2}\} &\approx \frac{1}{2}\left(1.5858\epsilon - 0.775\epsilon^2 + 1.775\epsilon - 0.775\epsilon^2\right) \\ &= 1.6804\epsilon - 0.775\epsilon^2. \end{aligned} \tag{46}$$

To verify the correctness of the above analyses, we compare theoretical results with empirical ones in Fig. 2. Experimental settings are shown in figure titles. It can be seen that the theoretical results closely match the empirical ones, providing supporting evidences for the correctness of our analyses [7]. It can be found from Fig. 2 that $\Pr\{e\}$ and $\Pr\{e|X^{n-t}\}$ almost stay the same for different code lengths, *i.e.*, $\Pr\{e\}$ and $\Pr\{e|X^{n-t}\}$ do not depend on code length. In addition, by comparing Fig. 2(a) and Fig. 2(b), it can be found that at the same ϵ, the FER will be higher if the rate R is reduced.

VI. Conclusion

Error probability analysis of coset codes is a challenging problem. This letter makes an attempt on this problem for DAC. We propose an enumerative method based on coexisting intervals, which is validated by the experimental results. However, a brute-force implementation of this method is not feasible for large code length due to the quick growth in complexity. Finding a more efficient implementation is a worthwhile endeavor for future research.

References

[1] 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.

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

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

[4] 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.

[5] 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.

[6] Y. Fang, V. Stankovic, S. Cheng, and E.-H. Yang, "Analysis on tailed distributed arithmetic codes for uniform binary sources," *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4305–4319, Oct. 2016.

[7] *DAC FER*. Accessed: Sep. 22, 2021. [Online]. Available: https://github.com/fy79/DAC-FER

Authorized licensed use limited to: McMaster University. Downloaded on September 27,2023 at 20:58:12 UTC from IEEE Xplore. Restrictions apply.