Title	Practical Short-Length Coding Schemes for Binary Distributed Hypothesis Testing
Author(s)	Dupraz, Elsa; Adamou, Ismaila Salihou; Asvadi, Reza; Matsumoto, Tad
Citation	2024 IEEE International Symposium on Information Theory (IEEE ISIT 2024)
Issue Date	2024-07-15
Type	Conference Paper
Text version	author
URL	http://hdl.handle.net/10119/19325
Rights	This is the author's version of the work published at arXiv, DOI: 10.48550/arXiv.2405.07697. This work has been presented at International Symposium on Information Theory (IEEE ISIT 2024), Athens, Greece, July 7-12, 2024, and the paper is to be published in IEEE Xplore, Copyright (C) IEEE ISIT 2024. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Description	2024 IEEE International Symposium on Information Theory (IEEE ISIT 2024), Athens, Greece, July 7-12, 2024

Practical Short-Length Coding Schemes for Binary Distributed Hypothesis Testing

Elsa Dupraz[1], Ismaila Salihou Adamou[1], Reza Asvadi[2], and Tad Matsumoto[1,3]

[1] IMT Atlantique, CNRS UMR 6285, Lab-STICC, Brest, France
[2] Faculty of Electrical Engineering, Shahid Beheshti University, Tehran
[3] JAIST and University of Oulu (Emeritus)

Abstract—This paper investigates practical coding schemes for Distributed Hypothesis Testing (DHT). While the literature has extensively analyzed the information-theoretic performance of DHT and established bounds on Type-II error exponents through quantize and quantize-binning achievability schemes, the practical implementation of DHT coding schemes has not yet been investigated. Therefore, this paper introduces practical implementations of quantizers and quantize-binning schemes for DHT, leveraging short-length binary linear block codes. Furthermore, it provides exact analytical expressions for Type-I and Type-II error probabilities associated with each proposed coding scheme. Numerical results show the accuracy of the proposed analytical error probability expressions, and enable to compare the performance of the proposed schemes.

I. Introduction

In modern communication systems, the communication objective has evolved beyond the mere reconstruction of original information to encompass the application of Machine Learning tasks such as decision making or classification upon received data. This paper focuses on the specific case of Distributed Hypothesis Testing (DHT) [1]. In the DHT setup, the decoder aims to make a decision between two hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$, based on a coded version of the source X, and on some observed side information Y. The performance of a DHT scheme is typically evaluated from two error probabilities. Type-I error refers to deciding $\mathcal{H}_1$ while $\mathcal{H}_0$ was true, and Type-II error conversely involves selecting $\mathcal{H}_0$ when $\mathcal{H}_1$ is true. To fully address DHT, it is essential to investigate both information-theoretic performance limits and practical coding schemes for this setup.

From an information-theoretic perspective, DHT was initially introduced by Berger in [2]. Subsequently, Ahlswede and Csiszar established a lower bound on Type-II error-exponent through an achievability scheme based on a quantizer [3]. Notably, this scheme was found to be optimal for testing against independence [4]. Next, Shimokawa et al. improved the lower bound presented in [3], extending its applicability to general hypotheses, not restricted to testing against independence [5]. This enhancement was achieved by employing a quantize-binning achievability scheme. The optimality of the quantize-binning scheme was then investigated on several DHT problems. It was shown in [6] that this scheme is optimal for a certain class of testing against conditional independence problems, given that the tradeoff between quantization and binning is adressed properly. This analysis was further extended

to encompass more generalized hypotheses, including those involving independent and identically distributed (i.i.d.) binary sources [7], non-binary sources [8], and non-i.i.d. sources [9]. The impact of discrete memoryless channels [10], Multiple-Access channels [11], or two-hop relay networks [12] on the DHT performance was also analyzed. Multi-terminal source coding for DHT was also considered in [13].

While the DHT information-theoretic performance is now well known across a wide range of source models and hypotheses, the problem of designing practical coding schemes for this setup has been by far less investigated. This paper takes a step towards bridging this gap, by focusing on the scenario where the sources X and Y are binary.

Previous achievability proofs suggest to consider either quantizer-alone or quantize-binning coding schemes for DHT. Some existing works have already introduced practical binary quantizers [14], binning schemes [15], and quantize-binning schemes [16], all constructed with linear block codes. But the constructions of [14]–[16] primarily focus on source reconstruction and typically involve very long source sequences, often exceeding 10^5 bits. However, DHT inherently deals with short-length sequences, where just a few dozen bits may suffice for making the correct decision. And the construction of efficient short-length linear block codes is often known to be a challenging problem [17]. Consequently, an important question arises regarding whether binary quantizers and quantize-binning schemes are efficient structures for practical short-length DHT.

This paper addresses practical coding schemes for DHT by providing two main contributions. Firstly, it introduces and compares three practical coding schemes. The first scheme, named the truncation scheme, involves transmitting only the first ℓ bits of the source sequence $\mathbf{x}^n$ and serves as a performance baseline. The second and third schemes are practical quantizer-alone and quantize-binning schemes, both constructed with short-length binary linear block codes. Secondly, the paper provides exact analytical expressions for Type-I and Type-II error probabilities of the three considered coding schemes. These new analytical tools should enable the optimization and comparison of the proposed practical schemes across a wide range of source and code parameters. Numerical results validate the accuracy of the analytical error
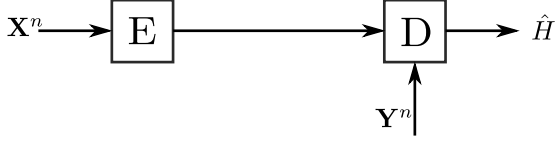
Fig. 1. Distributed hypothesis testing scheme

probabilities by demonstrating their consistency with Monte-Carlo simulations. Additionally, the paper compares the performance of the three schemes for sources of length $n = 31$ bits.

The outline of the paper is as follows. Section II describes the binary DHT problem. Section III presents the truncation scheme. Section IV introduces the quantizer scheme. Section V describes the quantize-binning scheme. Section VI shows and discusses numerical results.

II. PROBLEM STATEMENT

In what follows, $[\![1, M]\!]$ is the set of integers between 1 and M. Random variables are represented by capital letters, such as X, while their realizations are denoted by lower-case letters, like x. Vectors of length n, such as $\mathbf{X}^n$, are in bold. In addition, we use $w(\mathbf{x}^n)$ to denote the Hamming weight of the vector $\mathbf{x}^n$, and $d(\mathbf{x}^n, \mathbf{y}^n)$ to denote the Hamming distance between $\mathbf{x}^n$ and $\mathbf{y}^n$. The binomial coefficient of the pair of integers (n, k) with $k \le n$ is expressed as $\binom{n}{k}$.

A. DHT for binary sources

We consider binary source vectors $\mathbf{X}^n$ and $\mathbf{Y}^n$ both of length n. The encoder observes $\mathbf{X}^n$, whereas the decoder observes $\mathbf{Y}^n$, as illustrated in Fig. 1. The encoder sends a coded version of $\mathbf{X}^n$, while the decoder aims to make a decision between two hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$, based on both $\mathbf{Y}^n$ and the received coded data.

We assume that the n symbols of the sequences $\mathbf{X}^n$ and $\mathbf{Y}^n$ are i.i.d. and drawn according to random variables X and Y, respectively. Furthermore, X and Y are jointly distributed according to the model $Y = X \oplus E$, where E is a binary random variable independent of X, and $P(X = 1) = 1/2$. Additionally, we denote $p = \mathbb{P}(E = 1)$ with $0 < p \le 1/2$. The two hypotheses are expressed as:

$$\begin{cases} \mathcal{H}_0 : & p = p_0, \\ \mathcal{H}_1 : & p = p_1. \end{cases} \tag{1}$$

We assume, without loss of generality, that $p_0 < p_1$. It is worth noting that the probability distributions of both X and Y are independent of the chosen hypothesis, given $P(X = 1) = 1/2$. This model was investigated from an information-theoretic perspective for instance in [5], [7], [8]. Furthermore, when $p = 1/2$, the problem (1) reduces to testing against independence [3].

B. Error-exponent for binary DHT

We will now restate an existing lower bound on the error exponent for the problem defined in Equation (1), from the literature of information theory. Following the approach in [5], [6], we consider an encoding function:

$$f_n : \{0, 1\}^n \to [\![1, 2^v]\!], \tag{2}$$

and a decision function $g_n : [\![1, 2^v]\!] \times \{0, 1\}^n \to \{0, 1\}$. We consider a rate-limited setup in which $v/n \le R$.

For given functions (f_n, g_n), we define Type-I error probability α_n and Type-II error probability β_n as in [7] as

$$\alpha_n = \mathbb{P}(g_n(f_n(\mathbf{X}^n), \mathbf{Y}^n) = 1 | \mathcal{H}_0), \tag{3}$$
$$\beta_n = \mathbb{P}(g_n(f_n(\mathbf{X}^n), \mathbf{Y}^n) = 0 | \mathcal{H}_1). \tag{4}$$

For a given value $\epsilon \in (0, 1)$ such that $\alpha_n < \epsilon$, Type-II error exponent θ is defined as [7]

$$\lim_{n \to \infty} \sup \frac{1}{n} \log_2 \frac{1}{\beta_n} \ge \theta. \tag{5}$$

A generic lower bound on the error exponent θ is provided in [8]. Specifying this bound for the hypothesis testing problem defined in (1) leads to

$$\theta \le \sup_{\delta \in [0,1]} \min \left\{ R - [H_2(p_0 * \delta) - H_2(\delta)], \tag{6} \right.$$
$$\left. (p_0 * \delta) \log \frac{p_0 * \delta}{p_1 * \delta} + (1 - (p_0 * \delta)) \log \frac{1 - (p_0 * \delta)}{1 - (p_1 * \delta)} \right\}.$$

Here, H_2 is the binary entropy function, and $*$ is the binary convolution operator defined as $x * y = (1 - x)y + (1 - y)x$, with $0 \le x, y \le 1$.

C. Short-length nature of DHT

While the lower bound on the error exponent θ in (6) provides a scaling law for Type-II error probability, it remains an asymptotic result due to the limit as n tends to infinity in definition (5). Nevertheless, it confirms the intuition that the problem inherently involves short sequences. For instance, consider parameters $p_0 = 0.05$, $p_1 = 0.5$, $\delta = 0.1$, $R = 0.4$. When evaluating the quantity $e^{-n\theta}$ for these parameters with $n = 100$, the result is approximately 10^{-12}, and for $n = 50$, it yields approximately 10^{-6}. This strongly suggests that practical schemes should focus on values of n less than 50. Hence, we now introduce three practical coding schemes tailored for such short sequence lengths.

III. TRUNCATION SCHEME

A. Code construction

When considering DHT, there is no need to reconstruct all the exact values of the source bits $\mathbf{x}^n$. So a first straightforward solution consists of sending the first ℓ symbols of the source vector $\mathbf{x}^n$ at coding rate $R = \ell/n$. The decoder can then perform a standard Neyman-Pearson (NP) test [18] on the pair $(\mathbf{x}^\ell, \mathbf{y}^\ell)$.

Under a certain constraint $\alpha_n < \epsilon$ on Type-I error probability, the NP lemma [18] states that the following test:

$$\mathbb{P}_1(\mathbf{x}^\ell, \mathbf{y}^\ell) < \mu \mathbb{P}_0(\mathbf{x}^\ell, \mathbf{y}^\ell), \tag{7}$$

minimizes Type-II error probability β_n, where μ is a threshold value chosen to satisfy the Type-I error constraint. In (7), $\mathbb{P}_0$ and $\mathbb{P}_1$ are the joint probability distributions of $(\mathbf{x}^\ell, \mathbf{y}^\ell)$ under hypothesis $\mathcal{H}_0$ and under hypothesis $\mathcal{H}_1$, respectively. Given that $p_0 < p_1$, it is shown in [18] that the test described by (7) is equivalent to the condition:

$$\sum_{i=1}^{\ell} (x_i \oplus y_i) < \lambda_t, \tag{8}$$

where $\lambda_t \in \mathbb{N}$ is an integer threshold value chosen so as to satisfy the constraint $\alpha_n < \epsilon$. Interestingly, this test depends on the value of the parameter p_0 solely through the choice of the value of λ_t.

B. Theoretical analysis

For this scheme, analytical expressions of Type-I and Type-II error probabilities are given by [18]

$$\alpha_n^{(t)} = 1 - \sum_{j=0}^{\lambda_t} \binom{\ell}{j} p_0^j (1-p_0)^{\ell-j}, \tag{9}$$

$$\beta_n^{(t)} = \sum_{j=0}^{\lambda_t} \binom{\ell}{j} p_1^j (1-p_1)^{\ell-j}. \tag{10}$$

The truncation scheme can be seen as a "no-coding" setup [19]. In our numerical results, it will serve as a baseline when evaluating the performance of the proposed coding schemes.

IV. QUANTIZATION SCHEME

In the literature of information theory, the seminal work of [3] proposed to build a DHT coding scheme from a quantizer alone. We now introduce a practical short-length implementation of this scheme by using linear block codes.

A. Code construction

In order to perform binary quantization, we consider the generator matrix G_q of size $n \times m$ of a linear block code [20]. Then, for a given source vector $\mathbf{x}^n$ of length n, the encoder produces a vector $\mathbf{z}_q^m$ as [21]

$$\mathbf{z}_q^m = \arg\min_{\mathbf{z}^m} d(G_q \mathbf{z}^m, \mathbf{x}^n). \tag{11}$$

The codeword $\mathbf{z}_q^m$ is transmitted to the decoder at a code rate $R = m/n$.

In [14], [16], it is proposed to build efficient binary quantizers using low density generator matrices (LDGM). LDGM codes were considered so as to develop a low complexity message-passing algorithm called Bias-Propagation to solve (11). However, the schemes introduced in [14], [16] consider very long codes (more than 10^5 bits). Here, due to the short-length nature of the problem, we choose to discard the Bias-Propagation

algorithm since it may lead to an important loss in performance on the considered codes. Instead, we will solve (11) exactly by exhaustive search. Therefore, we consider any generator matrix G_q, not necessarily obtained from an LDGM code.

The decoder first computes the quantized vector $\mathbf{x}_q^n = G_q \mathbf{z}_q^m$. Then, since $\mathbb{P}(\mathbf{z}_q^m, \mathbf{y}^n) = \mathbb{P}(\mathbf{x}_q^n, \mathbf{y}^n)$, the NP test (7) reduces to

$$\sum_{i=1}^{n} (x_{q,i} \oplus y_i) < \lambda_q, \tag{12}$$

where λ_q is an integer threshold. Here, compared to the truncation scheme, the decision is taken from longer vectors $\mathbf{x}_q^n$ and $\mathbf{y}^n$ of dimensions $n > m$. On the other hand, the vector $\mathbf{x}_q^n$ contains quantization errors compared to $\mathbf{x}^n$.

B. Theoretical analysis

We now provide exact analytical expressions of Type-I and Type-II error probabilities for the quantization scheme. Consider the set of integers $\{E_\gamma^{(q)}\}_{\gamma \in [\![0, d_{\max}^{(q)}]\!]}$, where $E_\gamma^{(q)}$ is the number of words $\mathbf{x}^n$ of Hamming weight γ that belong to the decision region $\mathcal{C}_0^{(q)}$ of $\mathbf{x}_q^n = \mathbf{0}^n$. In other words, $\mathbf{x}^n \in \mathcal{C}_0^{(q)}$ means that the solution of (11) for $\mathbf{x}^n$ is $\mathbf{0}^m$. We further denote $N_0^{(q)} = \sum_{\gamma=0}^{d_{\max}^{(q)}} E_\gamma^{(q)}$.

Proposition 1. *For the quantization scheme and for a threshold value λ_q, Type-I and Type-II error probabilities are given by*

$$\alpha_n^{(q)} = 1 - \frac{1}{N_0^{(q)}} \sum_{\lambda=0}^{\lambda_q} \sum_{\gamma=0}^{d_{max}^{(q)}} \sum_{j=0}^{n} E_\gamma^{(q)} \Gamma_{\lambda,j,\gamma} p_0^j (1-p_0)^{n-j}, \tag{13}$$

$$\beta_n^{(q)} = \frac{1}{N_0^{(q)}} \sum_{\lambda=0}^{\lambda_q} \sum_{\gamma=0}^{d_{max}^{(q)}} \sum_{j=0}^{n} E_\gamma^{(q)} \Gamma_{\lambda,j,\gamma} p_1^j (1-p_1)^{n-j}, \tag{14}$$

where for $j = \gamma + \lambda - 2u$ and $0 \le u \le \min(\gamma, \lambda) \le n$,

$$\Gamma_{\lambda,j,\gamma} = \binom{\gamma}{u} \binom{n-\gamma}{\lambda-u}. \tag{15}$$

Proof. Since by symmetry the quantizer error probability is independent of the transmitted codeword [20], we consider the all-zero codeword $\mathbf{x}_q^n = \mathbf{0}$. We develop

$$\alpha_n^{(q)} = 1 - \sum_{\lambda=0}^{\lambda_q} \mathbb{P}_0(w(\mathbf{Y}^n) = \lambda) \tag{16}$$

$$= 1 - \sum_{\lambda=0}^{\lambda_q} \sum_{\gamma=0}^{d_{max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \mathbb{P}_0(w(\mathbf{Y}^n) = \lambda | w(\mathbf{X}^n) = \gamma)$$

$$= 1 - \sum_{\lambda=0}^{\lambda_q} \sum_{\gamma=0}^{d_{max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \sum_{j=0}^{n} \mathbb{P}_0(d(\mathbf{X}^n, \mathbf{Y}^n) = j) \frac{\Gamma_{\lambda,j,\gamma}}{\binom{n}{j}}$$

$$= 1 - \sum_{\lambda=0}^{\lambda_q} \sum_{\gamma=0}^{d_{max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \sum_{j=0}^{n} \binom{n}{j} p_0^j (1-p_0)^{n-j} \frac{\Gamma_{\lambda,j,\gamma}}{\binom{n}{j}}.$$

This gives (13). To obtain (14), we remark that $\beta_n^{(q)} = \sum_{\lambda=0}^{\lambda_q} \mathbb{P}_1(w(\mathbf{Y}^n) = \lambda)$ and follow the same steps as in (16), by replacing p_0 by p_1. □

V. QUANTIZE-BINNING SCHEME

We now propose a practical solution for the quantize-binning scheme which has been widely investigated in the literature of information theory for DHT [5], [6], [8].

A. Code construction

In the quantize-binning scheme, we consider as before a generator matrix G_q of size $n \times m$. We also resort to the parity check matrix H_b of size $k \times m$ of another linear block code. After using G_q for binary quantization as described in Section IV, the encoder uses the matrix H_b to compute

$$\mathbf{u}^k = H_b \mathbf{z}_q^m. \qquad (17)$$

The syndrom $\mathbf{u}^k$ is then transmitted to the decoder. In this case, the coding rate is given by $R = k/n$. At the decoder, in order to apply the NP test (7), we first identify by exhaustive search a vector $\hat{\mathbf{z}}_q^m$ as

$$\hat{\mathbf{z}}_q^m = \arg\min_{\mathbf{z}^m} \, d(G_q \mathbf{z}^m, \mathbf{y}^n) \text{ s.t. } H_b \mathbf{z}^m = \mathbf{u}^k. \qquad (18)$$

We then apply the following test:

$$\sum_{i=1}^{n} (\hat{x}_{q,i} \oplus y_i) < \lambda_{qb}, \qquad (19)$$

where $\hat{\mathbf{x}}_q^n = G_q \hat{\mathbf{z}}_q^m$, and λ_{qb} is an integer threshold.

Next, according to [8], the binning allows us to leverage the side information vector $\mathbf{y}^n$ so as to further reduce the coding rate. However, it also introduces a binning error probability which can impact Type-I and Type-II error probabilities. While this problem was well investigated in the asymptotic regime [8], we next discuss it for the considered short length code construction.

B. Theoretical analysis

We now consider the decision region $\mathcal{C}_0^{(qb)}$ for the all-zero codeword of the quantize-binning scheme. Especially, a side information vector $\mathbf{y}^n$ belongs to $\mathcal{C}_0^{(qb)}$ if the solution of (18) for this vector is $\hat{\mathbf{z}}_q^m = \mathbf{0}^m$. We then define the set of integers $\{E_\nu^{(qb)}\}_{\nu \in [\![0, d_{\max}^{(qb)}]\!]}$, where $E_\nu^{(qb)}$ is the number of words $\mathbf{y}^n$ of Hamming weight ν that belong to the decision region $\mathcal{C}_0^{(qb)}$. We also define the set of integers $\{A_t^{(qb)}\}_{t \in [\![0,n]\!]}$, where $A_t^{(qb)}$ is the number of codewords $\mathbf{x}_q^n$ of Hamming weight t such that there exists $\mathbf{z}_q^m$ that satisfies $\mathbf{x}_q^n = G_q \mathbf{z}_q^m$, and $H_b \mathbf{z}_q^m = \mathbf{0}^k$. As a result, the set $\{A_t^{(qb)}\}_{t \in [\![0,n]\!]}$ is the code weight distribution of the concatenated code.

Proposition 2. *For the quantize-binning scheme and for a threshold value λ_{qb}, Type-I and Type-II error probabilities are given by*

$$\alpha_n^{(qb)} = 1 - \mathbb{P}_B(p_0) - \mathbb{P}_{\bar{B}}(p_0), \qquad (20)$$

$$\beta_n^{(qb)} = \mathbb{P}_B(p_1) + \mathbb{P}_{\bar{B}}(p_1), \qquad (21)$$

where

$$\mathbb{P}_B(\delta) = \sum_{\nu=0}^{\min(d_{\max}^{(qb)}, \lambda_{qb})} \frac{E_\nu^{(qb)}}{\binom{n}{\nu}} \sum_{\gamma=0}^{d_{\max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \sum_{j=0}^{n} \Gamma_{\nu,j,\gamma} \delta^j (1-\delta)^{n-j}, \qquad (22)$$

$$\mathbb{P}_{\bar{B}}(\delta) = \sum_{i=0}^{n} \left[\left(\sum_{\gamma=0}^{d_{\max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \sum_{j=0}^{n} \Gamma_{i,j,w} \delta^j (1-\delta)^{n-j} \right) \times \left(\sum_{t=1}^{n} \sum_{\nu=0}^{\lambda_{qb}} \frac{E_\nu^{(qb)}}{\binom{n}{\nu}} \frac{A_t^{(qb)} \Gamma_{i,\nu,t}}{\binom{n}{i}} \right) \right]. \qquad (23)$$

Proof. We consider the all-zero codeword $\mathbf{x}_q^n = \mathbf{0}$. Under the hypothesis $\mathcal{H}_0$, we express

$$\alpha_n^{(qb)} = 1 - \mathbb{P}_0(\widehat{\mathcal{H}}_0, B) - \mathbb{P}_0(\widehat{\mathcal{H}}_0, \bar{B}). \qquad (24)$$

In this expression, B is the event that the correct sequence $\hat{\mathbf{x}}_q = \mathbf{x}_q$ was retrieved at the decoder, while $\bar{B}$ is the event that an incorrect sequence $\hat{\mathbf{x}}_q \neq \mathbf{x}_q$ was output by the decoder. In addition, $\widehat{\mathcal{H}}_0$ is the event that hypothesis $\mathcal{H}_0$ was decided at the decoder. We further denote $\mathbb{P}_B(p_0) = \mathbb{P}_0(\widehat{\mathcal{H}}_0, B)$ and $\mathbb{P}_{\bar{B}}(p_0) = \mathbb{P}_0(\widehat{\mathcal{H}}_0, \bar{B})$. We then express

$$\mathbb{P}_B(p_0) = \sum_{\nu=0}^{n} \mathbb{P}_0(w(\mathbf{Y}^n) = \nu) \mathbb{P}_0(\widehat{\mathcal{H}}_0, B | w(\mathbf{Y}^n) = \nu) \quad (25)$$

$$= \sum_{\nu=0}^{\min(d_{\max}^{(qb)}, \lambda_{qb})} \mathbb{P}_0(w(\mathbf{Y}^n) = \nu) \frac{E_\nu^{(qb)}}{\binom{n}{\nu}}. \qquad (26)$$

Next, by following the same steps as in the proof of Proposition 1, we show that

$$\mathbb{P}_0(w(\mathbf{Y}^n) = \nu) = \sum_{\gamma=0}^{d_{\max}^{(q)}} \frac{E_\gamma^{(q)}}{N_0^{(q)}} \sum_{j=0}^{n} \Gamma_{\nu,j,\gamma} p_0^j (1-p_0)^{n-j}, \quad (27)$$

which provides (22). We then write

$$\mathbb{P}_{\bar{B}}(p_0) = \sum_{i=0}^{n} \mathbb{P}_0(w(\mathbf{Y}^n) = i) \mathbb{P}_0(\widehat{\mathcal{H}}_0, \bar{B} | w(\mathbf{Y}^n) = i), \quad (28)$$

where $\mathbb{P}_0(w(\mathbf{Y}^n) = i)$ is given by (27). Next, we develop

$$\mathbb{P}_0(\widehat{\mathcal{H}}_0, \bar{B} | w(\mathbf{Y}^n) = i)$$

$$= \sum_{t=1}^{n} \sum_{\nu=0}^{\lambda_{qb}} \mathbb{P}_0(w(\hat{\mathbf{X}}_q^n) = t, d(\hat{\mathbf{X}}_q^n, \mathbf{Y}^n) = \nu | w(\mathbf{Y}^n) = i) \qquad (29)$$

$$= \sum_{t=1}^{n} \sum_{\nu=0}^{\lambda_{qb}} \frac{E_\nu^{(qb)}}{\binom{n}{\nu}} \frac{A_t^{(qb)} \Gamma_{i,\nu,t}}{\binom{n}{i}}. \qquad (30)$$

This provides the expression of $P_{\bar{B}}(p_0)$ in (23).

We obtain the expression of $\beta_n^{(qb)}$ from the previous equations by noticing that $\beta_n^{(qb)} = \mathbb{P}_B(p_1) + \mathbb{P}_{\bar{B}}(p_1)$.
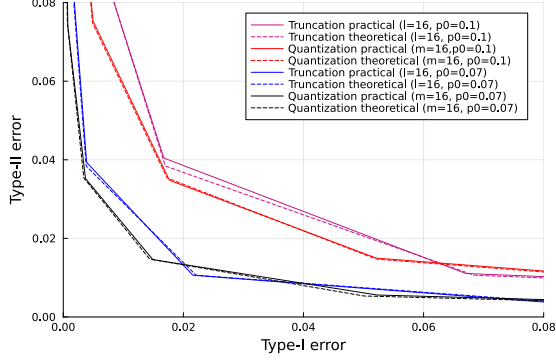
□

Fig. 2. ROC curve for the BCH code $(31, 16, 7)$ user as a quantizer, compared to the truncation scheme.

Fig. 3. ROC curve for the quantize-binning scheme built from the BCH code $(31, 16, 7)$ for quantization combined with the Reed-Muller code $(16, 5, 8)$ for binning

VI. NUMERICAL RESULTS

This section provides Monte-Carlo simulation results for the proposed code constructions, and compares them with the theoretical Type-I and Type-II error probabilities.

A. Truncation versus quantization

First of all, we evaluate the performance of the quantization scheme introduced in Section IV and compare it against the truncation scheme described in Section III. We set parameters $p_1 = 0.5$ (testing against independence), and $p_0 = 0.1$ or $p_0 = 0.07$. For the quantization, we consider the BCH $(31, 16)$-code with minimum distance $d_{\min} = 7$. As a result, after applying the quantizer, $m = 16$ bits are sent to the decoder. Therefore, we consider for comparison the truncation scheme with $\ell = 16$. For these two schemes, Fig. 2 shows the receiver operating characteristic (ROC) curves which provide the Type-II error with respect to the Type-I error, obtained for different threshold values $\lambda_t, \lambda_q \in [\![1, m]\!]$. Note that the ROC curves are usually considered for the evaluation of hypothesis tests. In Fig. 2, the plain curves come from Monte-Carlo simulations averaged other 10000 trials, while the dashed curves come from the error probability expressions provided in Sections III-B and IV-B.

For the considered two values of p_0, we observe that the quantizer scheme performs better than the truncation scheme. This is due to the fact that with the quantizer, the decision is made on $n = 31$ bits instead of $m = 16$ bits, although the quantized vector $\mathbf{x}_q^n$ contains errors compared to the original $\mathbf{x}^n$. In addition, we observe that the theoretical Type-I and Type-II error probabilities are closely consistent with the Monte Carlo results. This is because the error probability expressions take into account the considered code through the terms $E_\gamma^{(q)}$. As a result, the theoretical expressions are found to be relevant tools for the DHT code design.

B. Truncation versus quantize-binning

We now evaluate the performance of the quantize-binning scheme proposed in Section V compared to the truncation scheme. For the quantize-binning scheme, we consider the BCH $(31, 16)$ code for the quantizer, and the Reed-Muller
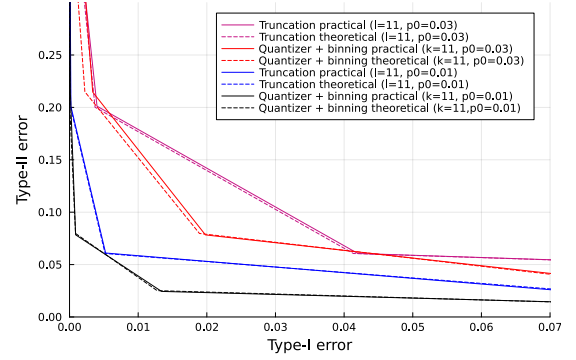
$(16, 5)$ code with $d_{\min} = 8$ for the binning part. As a result, only $k = 11$ coded bits are sent to the decoder. Therefore, for comparison, we consider the truncation scheme with $\ell = 11$. Fig. 3 shows the ROC curves for the considered two schemes, both for $p_1 = 0.35$ and $p_0 = 0.01$ or $p_0 = 0.03$. In this case again, plain curves come from Monte-Carlo simulations averaged over 10000 trials, and dashed curves come from the error probability expressions obtained in Sections III-B and V-B. We observe that the quantize-binning scheme performs much better than the truncation scheme, since it makes decision on $n = 31$ bits instead of $\ell = 11$ bits for the truncation scheme, despite the fact that both quantizer and binning can introduce errors. We also observe that the theoretical Type-I and Type-II error probabilities are closely consistent with the practical performance.

Finally, it is worth noting that the performance of the quantize-binning scheme strongly depends on the considered pair of codes used for quantization and binning. In this regard, the derived theoretical error probability expressions can serve as a useful tool for the design of efficient pairs of codes. Also we did not include the entropy-check condition of [8] in our quantize-and-binning scheme, since this did not bring any further improvement in terms of practical Type-I and Type-II error probabilities compared to the truncated scheme.

VII. CONCLUSION

In this paper, we have introduced two practical coding schemes for binary DHT, one built with a binary quantizer, and the other built with a quantize-binning scheme. Both schemes were designed from short linear block codes. For each considered scheme, we also derived theoretical expressions of Type-I and Type-II error probabilities. Simulation results demonstrated the superiority of the proposed schemes compared to the baseline truncation scheme, and also showed the accuracy of the proposed theoretical expressions. From a practical point of view, future works will include an interleaver design to improve the performance of the concatenated construction, as well as complexity reduction of the decoders so as to allow for larger code length to be considered.

REFERENCES

[1] S. Amari *et al.*, "Statistical inference under multiterminal data compression," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2300–2324, 1998.

[2] T. Berger, "Decentralized estimation and decision theory," in *IEEE Seven Springs Workshop on Information Theory, Mt. Kisco, NY*, 1979.

[3] R. Ahlswede and I. Csiszár, "Hypothesis testing with communication constraints," *IEEE Transactions on Information Theory*, vol. 32, no. 4, pp. 533–542, 1986.

[4] S. Watanabe, "On sub-optimality of random binning for distributed hypothesis testing," in *IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 2708–2713.

[5] H. Shimokawa and S. Amari, "Error bound of hypothesis testing with data compression," in *IEEE International Symposium on Information Theory (ISIT)*, 1994, p. 114.

[6] M. S. Rahman and A. B. Wagner, "On the optimality of binning for distributed hypothesis testing," *IEEE Transactions on Information Theory*, vol. 58, no. 10, pp. 6282–6303, 2012.

[7] E. Haim and Y. Kochman, "Binary distributed hypothesis testing via Körner-Marton coding," in *IEEE Information Theory Workshop (ITW)*, 2016, pp. 146–150.

[8] G. Katz, P. Piantanida, R. Couillet, and M. Debbah, "On the necessity of binning for the distributed hypothesis testing problem," in *IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 2797–2801.

[9] I. S. Adamou, E. Dupraz, and T. Matsumoto, "An information-spectrum approach to distributed hypothesis testing for general sources," in *Accepted at the Internation Zurich Seminar (IZS)*, 2024.

[10] S. Sreekumar and D. Gündüz, "Distributed hypothesis testing over discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2044–2066, 2019.

[11] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing over multi-access channels," in *IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[12] S. Salehkalaibar, M. Wigger, and L. Wang, "Hypothesis testing over the two-hop relay network," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4411–4433, 2019.

[13] S. Watanabe, "Neyman–pearson test for zero-rate multiterminal hypothesis testing," *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 4923–4939, 2017.

[14] J. Fridrich and T. Filler, "Binary quantization using belief propagation with decimation over factor graphs of ldgm codes," in *Proceedings of the 45th Allerton Conference on Coding, Communication, and Control*, 2007, pp. 495–501.

[15] Z. Xiong, A. D. Liveris, and S. Cheng, "Distributed source coding for sensor networks," *IEEE Signal Processing Magazine*, vol. 21, no. 5, pp. 80–94, 2004.

[16] M. J. Wainwright and E. Martinian, "Low-density graph codes that are optimal for binning and coding with side information," *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 1061–1079, 2009.

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

[18] E. L. Lehmann, J. P. Romano, and G. Casella, *Testing Statistical Hypotheses*. Springer, 2005, vol. 3.

[19] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: Lossy source-channel communication revisited," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1147–1158, 2003.

[20] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge university press, 2008.

[21] V. Chandar, E. Martinian, and G. W. Wornell, "Information embedding codes on graphs with iterative encoding and decoding," in *IEEE International Symposium on Information Theory (ISIT)*, 2006, pp. 866–870.