Bayanifar, Mahdi; Calderbank, Robert; Tirkkonen, Olav

Performance Analysis of Binary Chirp Decoding

Published in:
2023 IEEE Information Theory Workshop, ITW 2023

DOI:
10.1109/ITW55543.2023.10161617

Published: 01/01/2023

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Bayanifar, M., Calderbank, R., & Tirkkonen, O. (2023). Performance Analysis of Binary Chirp Decoding. In *2023 IEEE Information Theory Workshop, ITW 2023* (pp. 13-18). (IEEE Information Theory Workshop). IEEE. https://doi.org/10.1109/ITW55543.2023.10161617

Performance Analysis of Binary Chirp Decoding

Mahdi Bayanifar[1], Robert Calderbank[2] and Olav Tirkkonen[1]
[1]Department of Communications and Networking, Aalto University, Finland
[2]Department of Electrical and Computer Engineering, Duke University, NC 27708, USA
Email: {mahdi.bayanifar, olav.tirkkonen}@aalto.fi, robert.calderbank@duke.edu

Abstract—Binary Chirp (BC) codebooks consist of $N^{(\log_2 N+3)/2}$ lines in $\mathbb{C}^N$, equivalent up to overall phase rotations. Exploiting the underlying algebraic structure, the BCs allow suboptimal decoders with complexity $N(\log N)^2$, based on autocorrelations between the received signal and its permuted versions. We analyze the performance of these decoders in additive white Gaussian noise channels, providing lower bounds of decoding error probability, which are tight in the limits of low and high signal-to-noise ratio. Due to the autocorrelation nature of the receiver, the error probability becomes a function of order statistics of χ^2-distributed random variables. Our results can be used when dimensioning communication systems where BCs are used as component codes.

Index Terms—Binary Chirp, autocorrelation decoder, performance analysis

I. Introduction

CODEBOOKS of binary chirps (BCs) are highly structured Grassmannian line codebooks with high cardinality, and are invariant with respect to absolute phase and amplitude [1]. BCs represent subspaces of unit norm complex projective lines which have many desirable algebraic and geometrical features and are of interest in many applications in communication and information processing, e.g., compressed sensing [2]–[5], network coding [6], [7], random access [8], [9], Grassmannian quantization [10], etc. Also, the BCs are stabilizer states in the quantum computing [10]. Codebooks of BCs can be understood as exponentiated 2nd-order Reed-Muller codebooks, constructed based on m binary objects in m dimensions [1], [5], with the resulting codebooks having $N^{(\log_2 N+3)/2}$ elements in $N = 2^m$-dimensional complex space.

One of the key features of the BCs is existence of the low-complexity decoder. In [1], [2], Howard & al. presented a decoder that can find the closest codeword with $N(\log N)^2$ operations, with high probability. The decoder exploits the underlying dimensionality reduction from N complex to m binary dimensions, which is inherent in the algebraic structure governing the codes. Generalizations of the Howard algorithm have been recently discussed in [8], [10].

Motivated by the use of Binary Chirps in the contemporary problems of massive and unsourced [11] random access, see [8], [12], we analyze performance of the Howard algorithm. To the best of our knowledge, this has not been investigated in the literature. Getting an analytical handle on performance is crucial for dimensioning of systems where BCs act as component codes, such as [8], [12].

Instead of building the decoding result from cross-correlation against hypothetical transmitted signal hypotheses, the Howard decoder is based on autocorrelating the received signal with itself for m distinct permutations. This structure renders performance analysis tedious.

In the literature, performance analysis of autocorrelation detectors in Additive White Gaussian Noise (AWGN) channels has been mainly considered in the context of frequency hopping [13] and ultra-wideband [14]–[17], as well as in synchronization and cell search in cellular systems [18], [19]. The results of these studies do not carry far in the analysis of BC decoding. In the cellular scenarios, the problem is either related to timing estimation, not caring about the specifics of the signal [19], or finding the strongest signal from a very limited set of candidates [18]. In frequency hopping and ultra-wideband decoding, the problem setting is mostly related to the presence or absence of a signal in a certain time slot, or a certain frequency carrier. In the problem at hand, the number of possible codewords grows as a power of the dimension N.

In this paper, we first illustrate how the Howard algorithm effectively realizes decoding with an exponential reduction in dimension. We then provide two bounds for the decoding error probability rate for these codes. Specifically, these bounds are tight in the domains of low and high values of the Signal-to-Noise power Ratio (SNR). These bounds are expressed in terms of order statistics of χ^2-distributed variables. We examine the accuracy of the bounds by comparing them to simulated error probabilities, which gives insight into designing suitable codes for communication systems.

The paper is organized as follows. In Section II, we provide preliminaries about the Pauli group, BCs, the communication signal model, and the Howard algorithm for decoding the BCs. Section III dissects the error performance of the Howard decoder, and Section IV provides simulation results. Section V concludes the paper.

II. Preliminaries

In this section, first, we discuss the Pauli group, then introduce the binary chirp codebook of $N^{(\log N+3)/2}$ complex vectors in N dimensions, and finally describe the Howard decoder which has complexity $\mathcal{O}\left(N\log^2(N)\right)$.

A. Pauli Group

The 2×2 Pauli matrices are defined as

$$\mathbf{X} \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \mathbf{Z} \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \mathbf{Y} \triangleq i\mathbf{X}\mathbf{Z} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

These are Hermitian by construction. Considering binary vectors $\mathbf{a} = (a_1, ..., a_m), \mathbf{b} = (b_1, ..., b_m) \in \mathbb{F}_2^m$, we define the matrix $\mathbf{D} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{D}(\mathbf{a}, \mathbf{b}) \triangleq \mathbf{X}^{a_1}\mathbf{Z}^{b_1} \otimes \cdots \otimes \mathbf{X}^{a_m}\mathbf{Z}^{b_m}, \tag{1}$$

where $\otimes$ denotes the Kronecker product. The Pauli group or the Heisenberg-Weyl group $\mathcal{HW}_N$, is defined as $\mathcal{HW}_N \triangleq \left\{ i^k \mathbf{D}(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m \right\}$ where $k = 0, 1, 2, 3$. It can be seen that

$$\begin{aligned} \mathbf{D}(\mathbf{a}, \mathbf{b})\mathbf{D}(\mathbf{c}, \mathbf{d}) &= (-1)^{\mathbf{b}\mathbf{c}^T} \mathbf{D}(\mathbf{a} + \mathbf{c}, \mathbf{b} + \mathbf{d}) \\ &= (-1)^{\langle \mathbf{a}, \mathbf{b} | \mathbf{c}, \mathbf{d} \rangle} \mathbf{D}(\mathbf{c}, \mathbf{d})\mathbf{D}(\mathbf{a}, \mathbf{b}), \end{aligned} \tag{2}$$

where $\langle \mathbf{a}, \mathbf{b} | \mathbf{c}, \mathbf{d} \rangle \triangleq \mathbf{b}\mathbf{c}^T - \mathbf{a}\mathbf{d}^T$ is the symplectic inner product on $\mathbb{F}_2^{2m}$. Accordingly, $\mathbf{D}(\mathbf{a}, \mathbf{b})$ and $\mathbf{D}(\mathbf{c}, \mathbf{d})$ commute if and only if $\langle \mathbf{a}, \mathbf{b} | \mathbf{c}, \mathbf{d} \rangle = 0$.

Using binary vectors $\mathbf{v} \in \mathbb{F}^m$ to index the coordinates in $\mathbb{C}^N$, we can rewrite Eq. (1) as

$$\mathbf{D}(\mathbf{a}, \mathbf{b}) = \sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{\mathbf{b}\mathbf{v}^T} \mathbf{x}_{\mathbf{v}+\mathbf{a}} \mathbf{x}_{\mathbf{v}}^H, \tag{3}$$

where $\mathbf{x}_{\mathbf{v}}$ denotes the standard basis of $\mathbb{C}^N$, which $N = 2^m$. Also, $\mathbf{x}^H$ is the Hermitian of $\mathbf{x}$. Finally, we define corresponding Hermitian operators $\mathbf{E}(\mathbf{a}, \mathbf{b}) = i^{\mathbf{a}\mathbf{b}^T} \mathbf{D}(\mathbf{a}, \mathbf{b})$.

B. Binary Chirps

The set of Binary Chirps is given by unit norm vectors in $\mathbb{C}^N$ indexed by binary vectors $\mathbf{v}$, and of the form

$$\mathbf{w}_{\mathbf{S},\mathbf{b}} = \frac{1}{\sqrt{N}} \left[i^{\mathbf{v}^\mathbf{T}\mathbf{S}\mathbf{v} + 2\mathbf{b}^\mathbf{T}\mathbf{v}} \right]_{\mathbf{v} \in \mathbb{F}_2^m}, \tag{4}$$

where $\mathbf{S} \in \mathrm{Sym}(m; 2)$ is an $m \times m$ binary symmetric matrix, and $\mathbf{b} \in \mathbb{F}_2^m$ is a binary vector. A binary chirp codeword is the element-wise product of a mask sequence $\left[i^{\mathbf{v}^\mathbf{T}\mathbf{S}\mathbf{v}} \right]_{\mathbf{v} \in \mathbb{F}_2^m}$ and a Hadamard sequence $\left[(-1)^{\mathbf{b}^\mathbf{T}\mathbf{v}} \right]_{\mathbf{v} \in \mathbb{F}_2^m}$. Thus the set of BCs is an exponentiated second order Reed-Muller code, and they have many desirable algebraic and geometric features [1]–[4], [10].

Note that $\mathbf{H}_2 \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ denotes the 2×2 Walsh-Hadamard matrix, and $\mathbf{H} \triangleq \mathbf{H}_2^{\otimes m}$ is an $N \times N$ Walsh-Hadamard matrix. According to the definition, $\mathbf{H}_2 = \frac{1}{\sqrt{2}}(\mathbf{I} - \mathbf{X}\mathbf{Z})$, and then using the distributivity of the tensor product, we have

$$\begin{aligned} \mathbf{H} &= \otimes_{1=1}^m \mathbf{H}_2 = \otimes_{i=1}^m \frac{1}{\sqrt{2}}(\mathbf{I} - \mathbf{X}\mathbf{Z}) \\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} (-1)^{w(\mathbf{a})} \mathbf{D}(\mathbf{a}, \mathbf{a}) \end{aligned} \tag{5}$$

We can rewrite the BCs defined in Eq. (4) using coordinate-free manner as follows

$$\mathbf{W} = \mathbf{G}\mathbf{H}\mathbf{G}^H, \tag{6}$$

where $\mathbf{G} = \mathrm{diag}\left(i^{\mathbf{a}\mathbf{S}\mathbf{a}^T} \right), \mathbf{a} \in \mathbb{F}_2^m$ is a diagonal matrix with entries in $\{i^m\}_{m=0}^3$. This is a matrix where N BCs with the same $\mathbf{S}$ are columns, indexed by the binary vector $\mathbf{b}$. In the sequel, we will use this representation to identify the functionality of the Howard decoder—the operation to identify the binary symmetric matrix $\mathbf{S}$ does not depend on the column in $\mathbf{W}$.

C. Signal Model and Howard Decoder

Consider the received signal in an AWGN channel:

$$\mathbf{y} = \rho\,\mathbf{x} + \mathbf{n}, \tag{7}$$

where ρ characterizes the transmit power, $\mathbf{x}$ is the BC defined in Eq. (4), and the $\mathbf{n}$ is additive white complex-valued noise with $E\left\{\mathbf{n}\mathbf{n}^H\right\} = \mathbf{I}$. Note that taking the normalization of the BCs into account, the SNR is $\mathrm{SNR} = \rho^2/N$.

The noise components are given by $\mathbf{n} = \sum_{\mathbf{v}} n_{\mathbf{v}} \mathbf{x}_{\mathbf{v}}$. Decomposing these into real and imaginary parts as $n_{\mathbf{v}} = n_{\mathbf{v}}^{\mathcal{R}} + j n_{\mathbf{v}}^{\mathcal{I}}$, we have that $E\left\{ \left| n_{\mathbf{v}}^{\mathcal{R}} \right|^2 \right\} = E\left\{ \left| n_{\mathbf{v}}^{\mathcal{I}} \right|^2 \right\} = \frac{1}{2}$, and $E\left\{ n_{\mathbf{v}}^{\mathcal{R}} n_{\mathbf{v}}^{\mathcal{I}} \right\} = E\left\{ n_{\mathbf{v}}^{\mathcal{R}} n_{\mathbf{v}}^{\mathcal{R}} \right\} = E\left\{ n_{\mathbf{v}}^{\mathcal{I}} n_{\mathbf{v}}^{\mathcal{I}} \right\} = 0$.

A simple low-complexity algorithm for decoding the BCs has been proposed in [1], which contains the following steps:

1) For recovering the ith row of $\mathbf{S}$, construct a shifted version of the received signal as $\mathbf{y}(\mathbf{a} + \mathbf{e}_i)$, where $\mathbf{e}_i$ is the basis vector with 1 at position i and zeros in all other locations.
2) Compute the element-wise product of conjugate of the received signal with the shifted version: $\overline{\mathbf{y}(\mathbf{a})} \odot \mathbf{y}(\mathbf{a} + \mathbf{e}_i)$, where $\odot$ denotes the Hadamard or element-wise product operation.
3) Finally, calculate $\mathbf{H}\left(\overline{\mathbf{y}(\mathbf{a})} \odot \mathbf{y}(\mathbf{a} + \mathbf{e}_i) \right)$, and using the location of the maximum absolute value of this term, ith row can be identified. After finding all rows, the estimated $\mathbf{S}$ is used to identify the vector $\mathbf{b}$.

We note that in [1], after finding the first row, they suggested to use $\mathbf{e}_i + \mathbf{e}_{i-1}$ to find the i row, for $i = 2, ..., m$. This may help in multiple access scenarios. However, in this work, we concentrate on receiving a single BC scenario. In the sequel, it will become clear why this algorithm works.

III. Error Performance of Howard Decoder

In this section, first, we demonstrate how the Howard algorithm explained in the previous section, works, and then derive the block error rate for this decoder. Applying the Howard algorithm to the received signal (7), we get

$$\begin{aligned} \mathbf{H}\left(\overline{\mathbf{y}} \odot \mathbf{E}(\mathbf{e}_i, \mathbf{0})\,\mathbf{y} \right) &= \mathbf{H}\left((\rho\overline{\mathbf{x}} + \overline{\mathbf{n}}) \odot \mathbf{E}(\mathbf{e}_i, \mathbf{0})(\rho\mathbf{x} + \mathbf{n}) \right) \\ &= A_x + A_{xn} + A_{nx} + A_n. \end{aligned} \tag{8}$$

It can be seen that, for calculating (8), we need to provide insight into pairwise correlation, which is provided in the subsequent subsection.

A. Dissecting the Howard Decoder

The following lemmas will prove useful in analysis of the Howard algorithm.

Lemma 1. Considering the Pauli matrices of (1), if $\mathbf{a} \neq \mathbf{b}$ then $\mathbf{D}(\mathbf{a},\mathbf{c}) \odot \mathbf{D}(\mathbf{b},\mathbf{d}) = \mathbf{0}$.

Proof. Note that

$$(\mathbf{A} \otimes \mathbf{B}) \odot (\mathbf{C} \otimes \mathbf{D}) = (\mathbf{A} \odot \mathbf{C}) \otimes (\mathbf{B} \odot \mathbf{D}), \quad (9)$$

then, we have

$$\begin{aligned}\mathbf{D}(\mathbf{a},\mathbf{c}) \odot \mathbf{D}(\mathbf{b},\mathbf{d}) &= \left(\mathbf{x}^{a_1}\mathbf{z}^{c_1} \odot \mathbf{x}^{b_1}\mathbf{z}^{d_1}\right) \otimes \dots \\ &\quad \otimes \left(\mathbf{x}^{a_m}\mathbf{z}^{c_m} \odot \mathbf{x}^{b_m}\mathbf{z}^{d_m}\right). \quad (10)\end{aligned}$$

As can be seen from (3), the $\mathbf{x}$ Pauli matrix changes the position of diagonal to anti-diagonal elements. Hence, if $\mathbf{a} \neq \mathbf{b}$, then $\mathbf{x}^{a_i}\mathbf{z}^{c_i}$ will be mapped to different anti-diagonal elements than $\mathbf{x}^{b_i}\mathbf{z}^{d_i}$, and the result of the element-wise product will be a zero matrix. □

Lemma 2. Considering the Pauli matrices of (1), we have

$$\mathbf{D}(\mathbf{a},\mathbf{b}+\mathbf{c}) \odot \mathbf{D}(\mathbf{a},\mathbf{b}) = \mathbf{D}(\mathbf{a},\mathbf{c}). \quad (11)$$

Proof. Considering Eq. (3), the left-hand side reads

$$\begin{aligned}&\sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{(\mathbf{b}+\mathbf{c})\mathbf{v}^T} \mathbf{x}_{\mathbf{v}+\mathbf{a}}\mathbf{x}_{\mathbf{v}}^H \odot \sum_{\mathbf{u}\in\mathbb{F}_2^m} (-1)^{\mathbf{b}\mathbf{u}^T} \mathbf{x}_{\mathbf{u}+\mathbf{a}}\mathbf{x}_{\mathbf{u}}^H \\ &\quad \overset{(a)}{=} \sum_{\mathbf{u}\in\mathbb{F}_2^m} (-1)^{\mathbf{b}\mathbf{u}^T} \mathbf{x}_{\mathbf{u}+\mathbf{a}}\mathbf{x}_{\mathbf{u}}^H = \mathbf{D}(\mathbf{a},\mathbf{c}) \quad (12)\end{aligned}$$

where (a) comes from $\mathbf{x}_{\mathbf{v}+\mathbf{a}}\mathbf{x}_{\mathbf{v}}^H \odot \mathbf{x}_{\mathbf{u}+\mathbf{a}}\mathbf{x}_{\mathbf{u}}^H$ being non-zero if $\mathbf{u} = \mathbf{v}$, since $\mathbf{u}$ and $\mathbf{v}$ are the standard basis vectors in $\mathbb{C}^N$. □

Lemma 3. Considering the BCs of Eq. (6), the output of the Howard algorithm for the jth shift can be written as

$$\begin{aligned}&\mathbf{H}\left(\overline{\mathbf{W}(\mathbf{a})} \odot \mathbf{W}(\mathbf{a}+\mathbf{e}_j)\right) = \\ &\qquad \frac{-i^{\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T + 2w(\mathbf{S}_j)}}{\sqrt{N}} \sum_{\mathbf{v}\in\mathbf{F}_2^m} (-1)^{\mathbf{e}_j\mathbf{S}\mathbf{v}^T} \mathbf{x}_{\mathbf{S}_j}\mathbf{x}_{\mathbf{v}}^H \quad (13)\end{aligned}$$

where $\mathbf{S}_j$ denotes the jth row of $\mathbf{S}$.

Proof. By definition

$$\begin{aligned}\mathbf{W} &= \frac{1}{\sqrt{N}}\mathbf{G}\left(\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}(\mathbf{a},\mathbf{a})\right)\mathbf{G}^H \\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}(\mathbf{a},\mathbf{a}+\mathbf{a}\mathbf{S}) \quad (14)\end{aligned}$$

$$\overline{\mathbf{W}} = \frac{1}{\sqrt{N}} \sum_{a} i^{-w(\mathbf{a})}(-1)^{\mathbf{a}(\mathbf{a}\mathbf{S}+\mathbf{a})^T}\mathbf{E}(\mathbf{a},\mathbf{a}+\mathbf{a}\mathbf{S}), \quad (15)$$

where in Eq. (14), we used the fact that $\mathbf{G}\mathbf{E}(\mathbf{a},\mathbf{a})\mathbf{G}^H = \mathbf{E}(\mathbf{a},\mathbf{a}+\mathbf{a}\mathbf{S})$, which follows directly from (1). Eq. (15) results from (14) using the fact that $\mathbf{D}^T(\mathbf{a},\mathbf{b}) = (-1)^{\mathbf{a}\mathbf{b}^T}\mathbf{D}(\mathbf{a},\mathbf{b})$. Using Eq. (14), the shifted version of the codeword can be written as

$$\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{W} = \frac{1}{\sqrt{N}} \sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})-\mathbf{a}(\mathbf{S}+\mathbf{I})\mathbf{e}_j^T}\mathbf{E}(\mathbf{a}+\mathbf{e}_j,\mathbf{a}\mathbf{S}+\mathbf{a})$$

Using these, we get (16), where $\widetilde{\mathbf{S}} = \mathbf{S}+\mathbf{I}$, and (a) and (b) are achieved using lemma 1 and 2, respectively. The last term is diagonal matrix that will not affect the result and can be ignored. Now, we need to apply the Howard matrix as follows

$$\begin{aligned}&\mathbf{H}\sum_{\mathbf{a}\in\mathbb{F}_2^m} (-1)^{\mathbf{a}\mathbf{S}\mathbf{e}_j^T}\mathbf{D}(\mathbf{a},\mathbf{0}) \\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{u},\mathbf{a}\in\mathbf{F}_2^m} (-1)^{w(\mathbf{u})+\mathbf{a}\mathbf{S}\mathbf{e}_j^T+\mathbf{a}\mathbf{u}^T}\mathbf{D}(\mathbf{a}+\mathbf{u},\mathbf{u}) \\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{u},\mathbf{a},\mathbf{v}\in\mathbf{F}_2^m} (-1)^{w(\mathbf{u})+(\mathbf{a}+\mathbf{v})\mathbf{u}^T+\mathbf{a}\mathbf{S}\mathbf{e}_j^T}\mathbf{x}_{\mathbf{u}+\mathbf{a}+\mathbf{v}}\mathbf{x}_{\mathbf{v}}^H \\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^m} (-1)^{w(\mathbf{u})+\mathbf{u}\mathbf{v}^T}\mathbf{x}_{\mathbf{u}}\mathbf{x}_{\mathbf{v}}^H \sum_{\mathbf{a}\in\mathbb{F}_2^m} (-1)^{(\mathbf{u}+\mathbf{S}_j)\mathbf{a}^T} \\ &= \sqrt{N}(-1)^{w(\mathbf{S}_j)} \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{S}_j\mathbf{v}^T}\mathbf{x}_{\mathbf{S}_j}\mathbf{x}_{\mathbf{v}}^H \quad (17)\end{aligned}$$

where the last equality comes from the fact that

$$\sum_{\mathbf{a}\in\mathbf{F}_2^m} (-1)^{(\mathbf{u}+\mathbf{S}_j)\mathbf{a}^T} = \begin{cases} 0 & \mathbf{u} \neq \mathbf{S}_j \\ N & \mathbf{u} = \mathbf{S}_j \end{cases}. \quad (18)$$

Finally, by substituting Eq. (13) into Eq. (16), we get the result. □

B. Lower Bound on Block Error Rate

Considering Eq. (8) and using Lemma 3, we have

$$\begin{aligned}A_x &= \frac{\rho^2\alpha}{\sqrt{N}}\mathbf{x}_{\mathbf{S}_i} \\ A_{xn} &= \frac{\rho}{\sqrt{N}} \sum_{\mathbf{u}} \frac{1}{\sqrt{N}} \left(\sum_{\mathbf{v}} (-1)^{\mathbf{u}\mathbf{v}^T}\beta_{\mathbf{v}} n_{\mathbf{v}\oplus\mathbf{e}_i}\right)\mathbf{x}_{\mathbf{u}} \\ A_{nx} &= \frac{\rho}{\sqrt{N}} \sum_{\mathbf{u}} \frac{1}{\sqrt{N}} \left(\sum_{\mathbf{v}} (-1)^{\mathbf{u}(\mathbf{v}+\mathbf{e}_i)^T}\beta_{\mathbf{v}}^* n_{\mathbf{v}\oplus\mathbf{e}_i}^*\right)\mathbf{x}_{\mathbf{u}} \\ A_n &= \frac{1}{\sqrt{N}} \sum_{\mathbf{u}} \left(\sum_{\mathbf{v}} (-1)^{\mathbf{u}\mathbf{v}^T} n_{\mathbf{v}}^* n_{\mathbf{v}\oplus\mathbf{e}_i}\right)\mathbf{x}_{\mathbf{u}}, \quad (19)\end{aligned}$$

with $\alpha \triangleq i^{\mathbf{e}_i\mathbf{S}\mathbf{e}_i^T + 2\mathbf{b}\mathbf{e}_i^T}$, and $\beta_{\mathbf{v}} \triangleq i^{-\mathbf{v}\mathbf{S}\mathbf{v}^T - 2\mathbf{b}\mathbf{v}^T}$. Since $n_{\mathbf{v}}$ is a complex normal distribution, and $|\alpha|^2 = 1$, we can multiply all the above terms with α^*, which results in similar distribution. Also, since $|\beta_{\mathbf{v}}|^2 = 1$, distributions of $\beta_{\mathbf{v}} n_{\mathbf{v}\oplus\mathbf{e}_i}$ and $\beta_{\mathbf{v}}^* n_{\mathbf{v}\oplus\mathbf{e}_i}^*$ are the same as the distribution of $n_{\mathbf{v}\oplus\mathbf{e}_i}$ and $n_{\mathbf{v}\oplus\mathbf{e}_i}^*$, respectively. Hence, the error probability is independent of $\mathbf{S}$. To simplify the notation, we define

$$\begin{aligned}X_{\mathbf{u}} \triangleq \frac{1}{\sqrt{N}} \sum_{\mathbf{v}} &(-1)^{\mathbf{u}\mathbf{v}^T}\left(\rho n_{\mathbf{v}\oplus\mathbf{e}_i} + \rho(-1)^{\mathbf{u}\mathbf{e}_i^T} n_{\mathbf{v}\oplus\mathbf{e}_i}^*\right) \\ &+ \sum_{\mathbf{v}} (-1)^{\mathbf{u}\mathbf{v}^T} n_{\mathbf{v}}^* n_{\mathbf{v}\oplus\mathbf{e}_i} \quad (20)\end{aligned}$$

Then the probability of error in detecting the ith row using the Howard algorithm is

$$P_e = 1 - \Pr\left\{\left|\rho^2 + X_{\mathbf{s}_i}\right| > \left|X_{\mathbf{u}}\right|, \forall \mathbf{u} \in \mathbb{F}_2^n; \mathbf{u} \neq \mathbf{s}_i\right\}. \quad (21)$$

It can be seen that, depending on $\mathbf{u}$, $X_{\mathbf{u}}$ is either real or imaginary. Without loss of generality, we can consider

$$\overline{\mathbf{W}} \odot \mathbf{E}\left(\mathbf{e}_j, \mathbf{0}\right) \mathbf{W} = \frac{1}{N} \sum_{\mathbf{a} \in \mathbf{F}_2^m} i^{-w(\mathbf{a})} (-1)^{\mathbf{a}(\mathbf{aS}+\mathbf{a})^T} \mathbf{E}\left(\mathbf{a}, \mathbf{a}\widetilde{\mathbf{S}}\right) \odot \sum_{\mathbf{c} \in \mathbf{F}_2^m} i^{w(\mathbf{c})-\mathbf{c}\widetilde{\mathbf{S}}\mathbf{e}_j^T} \mathbf{E}\left(\mathbf{c}+\mathbf{e}_j, \mathbf{c}\widetilde{\mathbf{S}}\right)$$
$$= \frac{1}{N} \sum_{\mathbf{a},\mathbf{c} \in \mathbb{F}_2^m} \delta_{\mathbf{a},\mathbf{c}+\mathbf{e}_j} (-1)^{w(\mathbf{c})-w(\mathbf{a})} i^{\mathbf{cSc}^T-\mathbf{aSa}^T} D\left(\mathbf{a}, \mathbf{a}\widetilde{\mathbf{S}}\right) \odot D\left(\mathbf{c}+\mathbf{e}_j, \mathbf{c}\widetilde{\mathbf{S}}\right)$$
$$\overset{(a)}{=} \frac{1}{N} \sum_{\mathbf{a} \in \mathbb{F}_2^m} (-1)^{w(\mathbf{a})-w(\mathbf{a}\oplus\mathbf{e_j})} i^{\mathbf{aSa}^T-(\mathbf{a}\oplus\mathbf{e_j})\mathbf{S}(\mathbf{a}\oplus\mathbf{e_j})^T} D\left(\mathbf{a}+\mathbf{e}_j, \mathbf{a}\widetilde{\mathbf{S}}+\mathbf{e}_j\widetilde{\mathbf{S}}\right) \odot D\left(\mathbf{a}+\mathbf{e}_j, \mathbf{a}\widetilde{\mathbf{S}}\right)$$
$$\overset{(b)}{=} \frac{-1}{N} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{\mathbf{aSa}^T-(\mathbf{a}\oplus\mathbf{e_j})\mathbf{S}(\mathbf{a}\oplus\mathbf{e_j})^T} D\left(\mathbf{a}+\mathbf{e}_j, \mathbf{e}_j\widetilde{\mathbf{S}}\right) = \frac{-i^{\mathbf{e}_j\mathbf{S}\mathbf{e}_j}}{N} \sum_{\mathbf{a} \in \mathbb{F}_2^m} (-1)^{\mathbf{aSe}_j^T} D\left(\mathbf{a}, \mathbf{0}\right) \mathbf{D}\left(\mathbf{0}, \mathbf{e}_j\widetilde{\mathbf{S}}\right), \quad (16)$$

$$X_{\mathbf{u}} = \frac{2}{\sqrt{N}} \begin{cases} \sum_{\mathbf{v}} \rho(-1)^{\mathbf{uv}^T} \mathcal{R}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1}\right\} + \sqrt{N} \sum_{\substack{\mathbf{v} \in \mathbb{F}_2^N \\ \mathbf{v}(1)=0}} (-1)^{\mathbf{uv}^T} \mathcal{R}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1} n_{\mathbf{v}}^*\right\} & \text{if} \quad D_{\mathbf{u}} < 2^{m-1} \\ j \sum_{\mathbf{v}} \rho(-1)^{\mathbf{uv}^T} \mathcal{I}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1}\right\} + j\sqrt{N} \sum_{\substack{\mathbf{v} \in \mathbb{F}_2^N \\ \mathbf{v}(1)=0}} (-1)^{\mathbf{uv}^T} \mathcal{I}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1} n_{\mathbf{v}}^*\right\} & \text{if} \quad D_{\mathbf{u}} \geq 2^{m-1} \end{cases} \quad (22)$$

$\mathbf{e}_i = \mathbf{e}_1 = [1, 0, ..., 0]$. Then, it can be seen that, when the decimal equivalent of $\mathbf{u}$, i.e., $D_{\mathbf{u}}$, is less than 2^{m-1}, $X_{\mathbf{u}}$ is a real, otherwise it is imaginary. The corresponding explicit forms can be found in (22).

As in the case of performance analysis of autocorrelation decoder in ultra-wideband systems [16], we may proceed with the analysis in two cases, related to $\rho/\sqrt{N}$ being large or small.

For generic N, if SNR is large, i.e., $\rho >> 1$, we can approximate $X_{\mathbf{u}}$ as follows

$$X_{\mathbf{u}} = \frac{2\rho}{\sqrt{N}} \begin{cases} \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T} \mathcal{R}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1}\right\} & \text{if} \quad D_{\mathbf{u}} < 2^{m-1} \\ j \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T} \mathcal{I}\left\{n_{\mathbf{v}\oplus\mathbf{e}_1}\right\} & \text{if} \quad D_{\mathbf{u}} \geq 2^{m-1} \end{cases}$$

We can show that in this case, $X_{\mathbf{u}}$ is independent of $X_{\mathbf{u}'}$ for $\mathbf{u} \neq \mathbf{u}'$, since we have

$$E\left\{X_{\mathbf{u}} X_{\mathbf{u}'}\right\} = \frac{4\rho^2}{N} \sum_{\mathbf{v}} (-1)^{(\mathbf{u}+\mathbf{u}')\mathbf{v}^T} E\left\{\left(\mathcal{R}\left\{n_{\mathbf{v}\oplus\mathbf{e}_i}\right\}\right)^2\right\}$$
$$= \frac{2\rho^2}{N} \sum_{\mathbf{v}} (-1)^{(\mathbf{u}+\mathbf{u}')\mathbf{v}^T} = 0$$

which follows from the fact that $n_{\mathbf{v}}$ are i.i.d, while $E\left\{n_{\mathbf{v}}^2\right\} = 0$ and $E\left\{\left|n_{\mathbf{v}}\right|^2\right\} = 1$. Since each $X_{\mathbf{u}}$ is a linear combination of independent normally distributed random variables and uncorrelated with other samples $X_{\mathbf{u}'}$, they are independent of each other and have normal distribution, i.e., $X_{\mathbf{u}} \sim \mathcal{N}\left(0, 2\rho^2\right)$. For finding the error probability given in Eq. (21) in this case, we have

$$P_e = 1 - \Pr\left\{\left|X_{\mathbf{u}}\right|^2 < \left|\rho^2 + X_{\mathbf{S}_i}\right|^2, \forall \mathbf{u} \neq \mathbf{S}_i\right\}$$
$$= 1 - \frac{1}{2} \int_{-\infty}^{\infty} \left(2F_{X_{\mathbf{u}}}\left(\left|\rho^2 + x\right|\right) - 1\right)^{N-1} f(x) dx, \quad (23)$$

where $F_u(x) = \frac{1}{2\rho\sqrt{\pi}} \int_{-\infty}^{x} e^{-\frac{y^2}{4\rho^2}} dy$ is the cumulative distribution function (CDF) of $X_{\mathbf{u}}$, and $f(x) = \frac{1}{\rho\sqrt{\pi}} \exp\left\{x^2/4\rho^2\right\}$ is the probability density function (PDF) of a zero-mean normal distribution with variance $2\rho^2$. Since as we discussed earlier, the distributions are independent of $\mathbf{S}$, we set $\mathbf{S} = \mathbf{0}$, and thus $X_{\mathbf{S}}$ have a real normal distribution.

Another interesting limiting case is for generic SNR ρ when N is large. Then, we can approximate $X_{\mathbf{u}}$ as follows

$$X_{\mathbf{u}} \approx \sum_{\mathbf{v}} (-1)^{\mathbf{u}(\mathbf{v}+\mathbf{e}_i)^T} n_{\mathbf{v}\oplus\mathbf{e}_i}^* n_{\mathbf{v}} = \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T} n_{\mathbf{v}\oplus\mathbf{e}_i} n_{\mathbf{v}}^*$$

It can be shown that these variables are uncorrelated, since $E\left\{X_{\mathbf{u}}\right\} = \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T} E\left\{n_{\mathbf{v}\oplus\mathbf{e}_i} n_{\mathbf{v}}\right\} = 0$. Also, we have

$$E\left\{X_{\mathbf{u}} X_{\mathbf{u}'}\right\} = \sum_{\mathbf{v},\mathbf{x}} (-1)^{\mathbf{uv}^T+\mathbf{u}'\mathbf{x}^T} E\left\{n_{\mathbf{v}\oplus\mathbf{e}_i} n_{\mathbf{v}}^* n_{\mathbf{x}\oplus\mathbf{e}_i} n_{\mathbf{x}}^*\right\},$$

where the inner expectations can be non-zero in two different cases: 1) if $\mathbf{x} = \mathbf{v}$, which results in $E\left\{n_{\mathbf{v}\oplus\mathbf{e}_i}^2 \left(n_{\mathbf{v}}^*\right)^2\right\} = E\left\{n_{\mathbf{v}\oplus\mathbf{e}_i}^2\right\} E\left\{\left(n_{\mathbf{v}}^*\right)^2\right\} = 0$; 2) if $\mathbf{x} = \mathbf{v} \oplus \mathbf{e}_i$, which results in $E\left\{n_{\mathbf{v}\oplus\mathbf{e}_i} n_{\mathbf{v}}^* n_{\mathbf{v}} n_{\mathbf{v}\oplus\mathbf{e}_i}^*\right\} = E\left\{\left|n_{\mathbf{v}}\right|^2 \left|n_{\mathbf{v}\oplus\mathbf{e}_i}\right|\right\} = 1$, which by substitution leads to

$$E\left\{X_{\mathbf{u}} X_{\mathbf{u}'}\right\} = (-1)^{\mathbf{u}'\mathbf{e}_i^T} \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T+\mathbf{u}'\mathbf{v}^T},$$

which again is non-zero if $\mathbf{u} = \mathbf{u}'$. Then $X_{\mathbf{u}}$ is independent of $X_{\mathbf{u}'}$ for $\mathbf{u} \neq \mathbf{u}'$, because they are Gaussian. For large values of N, we may use the law of large numbers (LLN), that means $X_{\mathbf{u}} = N\frac{1}{N} \sum_{\mathbf{v}} (-1)^{\mathbf{uv}^T} x_{\mathbf{v}}$, where $x_{\mathbf{v}} = 2n_{\mathbf{v}}^{\mathcal{R}} n_{\mathbf{v}\oplus\mathbf{e}_i}^{\mathcal{R}}$. Hence, according to the LLN, $X_{\mathbf{u}} \sim \left(0, N^2\right)$. Using a similar procedure as in Eq. (23), we have

$$P_e = 1 - E_{X_{\mathbf{S}_i}} \left\{ \prod_{\mathbf{u} \neq \mathbf{S}_i} \Pr\left\{\left|X_{\mathbf{u}}\right|^2 < \left|\rho^2 + X_{\mathbf{S}_i}\right|^2\right\} \right\}$$
$$= 1 - \frac{1}{N\sqrt{2\pi}} \int_{-\infty}^{\infty} \left(2F_x\left(\left|\rho^2 + x\right|\right) - 1\right)^{N-1} e^{-\frac{x^2}{2N^2}} dx \quad (24)$$

where $F_x(x) = \frac{1}{N\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{y^2}{2N^2}} dy$ is the CDF of $X_{\mathbf{u}}$.

Inspecting the argumentation leading to (23) and (24), we identify χ^2 distributed random variates and their order

statistics. Denoting the χ^2 distribution with non-centrality r, the number of degrees of freedom N, and variance σ^2 by $\chi^2_N(r,\sigma^2)$, we have the following proposition.

Proposition 1. Consider an N-dimensional binary chirp transmission $\mathbf{w_{S,b}}$ of (4) in an AWGN-channel with SNR ρ. At the receiver, the first step in decoding is to identify a row of $\mathbf{S}$ by finding the maximum autocorrelation (13). In the limits $\sqrt{N}/\rho \to \infty$ and $\rho/\sqrt{N} \to \infty$, the probability of error is asymptotically lower bounded by

$$P_r = \Pr\{Y_{N-1} > Z\} \tag{25}$$

where Y_{N-1} is the maximum order statistic of $N-1$ samples drawn independently from $\chi^2_N(0,\sigma^2)$, and Z is distributed as $\chi^2_N(\rho^2,\sigma^2)$. For $\sqrt{N}/\rho \to \infty$, the variance is $\sigma^2 = N^2$, while for $\rho/\sqrt{N} \to \infty$, we have $\sigma^2 = 2\rho^2$.

Proof. In (23) and (24), $X_{\mathbf{u}}$ and $X_{\mathbf{S}_i}$ are either real or imaginary normal variates. However, as it is mentioned, the distribution is independent of $\mathbf{S}$, and we can consider $\mathbf{S} = \mathbf{0}$. The value of P_r in the statement then follows from (23) and (24) using the definitions of χ^2 distributions and order statistics. This is a lower bound for error probability for any receiver assuming that the first row is correctly decoded. □

Above, we computed the probability of error in decoding one row in the $m \times m$ binary symmeteric matrix $\mathbf{S}$, characterizing a BC in (4). For correctly decoding the binary chirp, all rows have to be correctly decoded, along with the binary vector $\mathbf{b}$ selecting a row from the matrix $\mathbf{W}$ of (6). In the decoder in [1], the rows in $\mathbf{S}$ are independently decoded. If the randomness causing row detection errors were independent, we would get a lower bound for the error probability as

$$P_{e,\text{approx}} = 1 - (1 - P_r)^m \tag{26}$$

where P_r is the probability of error of decoding one row. The errors in decoding different rows, however, are strongly correlated. Accordingly, this is an approximation of error probability, not a bound.

In [8], a list decoding and backtracking based algorithm is used, where decoding of rows in $\mathbf{S}$ is not independent; symmetricity of $\mathbf{S}$ is enforced, and in [10], projections were used to improve subsequent decoding performance. Our results provide a lower bound of performance for both.

IV. Numerical Results

In this section, we provide simulation results for measuring the accuracy of the proposed lower bounds for the error probability of the BC. In Fig. 1, we compare the simulation result of error probability and the error probability of detecting a row using the Howard algorithm for small values of N and high SNR regime, considering $m = 2$. We can see that by increasing ρ, the performance gap between the bound and the simulation result decreases, first term in Eq. (22) dominates the overall sum. Also, it is seen that approximated error probability is close to the simulation result.

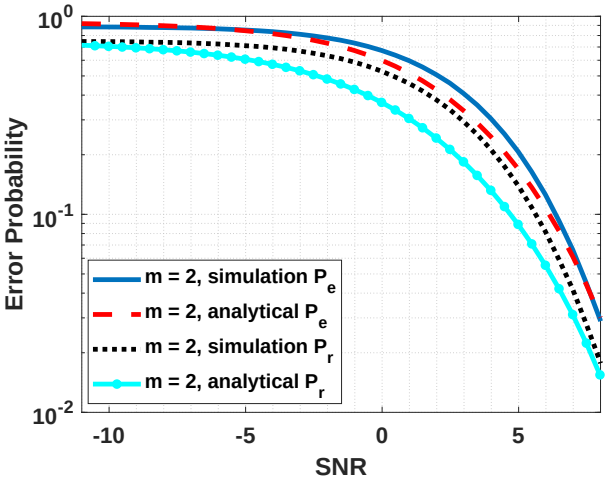

Fig. 1. Comparing the the approximated P_r and P_e of the Howard decoder with the simulation result in high SNR regime with $m = 2$.

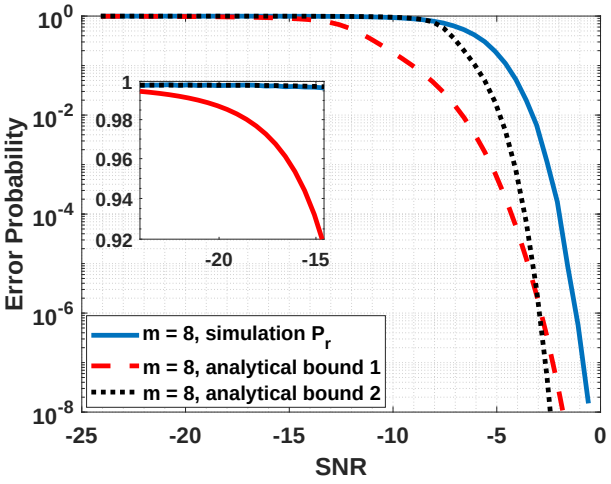

Fig. 2. Comparing the approximated error probabilities of the Howard decoder with the simulation result, $m = 8$.

Fig. 2 illustrates the error probability of a single row for both approximated bounds, for which we set $m = 8$. It is seen that, for low values of ρ, the second bound performs better than the first bound. However, by increasing the value of ρ, the error performance gap between the first bound and the simulation result shrinks. Hence, for different values of N, there exists a threshold value of ρ, that either the first or second bound perform better, and we can use this threshold to get a better approximation for the error probability of a single row. The cross-over point between the two approximations is at SNR 0 dB, as expected.

V. Conclusion

We have analyzed the performance of low-complexity decoding of binary chirp codebooks in N dimensions. In future work we shall extend the analysis to list decoders, considered in [8], [10]. Assuming that multiaccess interference is approximated by AWGN, the developed analytical

tools can be used in dimensioning massive and unsourced access methods where BCs are used as component codes.

Acknowledgments

This work was funded in part by the Academy of Finland (grant 334539).

References

[1] S. D. Howard, A. R. Calderbank, and S. J. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes," in Conference on Information Sciences and Systems, March 2008, pp. 11–15.

[2] L. Applebaum, S. D. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: Deterministic compressed sensing measurements for fast recovery," Applied and Computational Harmonic Analysis, vol. 26, no. 2, pp. 283 – 290, 2009.

[3] R. Calderbank, S. Howard, and S. Jafarpour, "A sublinear algorithm for sparse reconstruction with ℓ_2/ℓ_2 recovery guarantees," in 2009 3rd IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), 2009, pp. 209–212.

[4] ——, "Construction of a large class of matrices satisfying a statistical isometry property," in IEEE Journal of Selected Topics in Signal Processing, Special Issue on Compressive Sensing, vol. 4, no. 2, 2010, pp. 358–374.

[5] L. Zhang and D. Guo, "Neighbor discovery in wireless networks using compressed sensing with Reed-Muller codes," in 2011 Internat. Symp. Modeling and Optimization of Mobile, Ad Hoc, and Wireless Networks, 2011, pp. 154–160.

[6] R. Kötter and F. Kschischang, "Coding for errors and erasures in random network coding," IEEE Trans. Inf. Th., vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[7] T. Etzion and H. Zhang, "Grassmannian codes with new distance measures for network coding," tit, vol. 65, no. 7, pp. 4131–4142, 2019.

[8] R. Calderbank and A. Thompson, "CHIRRUP: a practical algorithm for unsourced multiple access," Information and Inference: A Journal of the IMA, no. iaz029, 2019, https://doi.org/10.1093/imaiai/iaz029.

[9] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, "Grant-free non-orthogonal multiple access for IoT: A Survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1805–1838, 2020.

[10] T. Pllaha, E. Heikkilä, R. Calderbank, and O. Tirkkonen, "Low-complexity grassmannian quantization based on binary chirps," in IEEE Wireless Communications and Networking Conference (WCNC), 2022, pp. 1105–1110.

[11] Y. Polyanskiy, "A perspective on massive random-access," in 2017 IEEE International Symposium on Information Theory (ISIT), 2017, pp. 2523–2527.

[12] P. Yang, D. Guo, and H. Yang, "Massive access in multi-cell wireless networks using Reed-Muller codes," arXiv preprint:2003.11568, 2020.

[13] A. Polydoros and K. Woo, "LPI detection of frequency-hopping signals using autocorrelation techniques," IEEE J. Selected Areas in Commun., vol. 3, no. 5, pp. 714–726, 1985.

[14] R. Hoctor and H. Tomlinson, "Delay-hopped transmitted-reference RF communications," in IEEE Conf. Ultra Wideband Systems and Tech., 2002, pp. 265–269.

[15] J. Choi and W. Stark, "Performance of ultra-wideband communications with suboptimal receivers in multipath channels," IEEE J. Selected Areas in Commun., vol. 20, no. 9, pp. 1754–1766, 2002.

[16] T. Quek and M. Win, "Performance analysis of ultrawide bandwidth transmitted-reference communications," in IEEE Vehicular Tech. Conf. (VTC-Spring), vol. 3, May 2004, pp. 1285–1289.

[17] J. Font-Segura, G. Vazquez, and J. Riba, "Nonuniform sampling walls in wideband signal detection," IEEE Trans. Sign. Proc., vol. 62, no. 1, pp. 44–55, 2014.

[18] J.-C. Lin, Y.-T. Sun, and H. V. Poor, "Initial synchronization exploiting inherent diversity for the LTE sector search process," IEEE Transactions on Wireless Communications, vol. 15, no. 2, pp. 1114–1128, 2016.

[19] D. W. Lin, "An analysis of the performance of ML blind OFDM symbol timing estimation," IEEE Transactions on Signal Processing, vol. 66, no. 20, pp. 5324–5337, 2018.