Extended Binary Chirps: Hierarchy Level Analysis and Low Complex Decoder

Aalto university

Abstract

Here is the abstract!!

Index Terms

Binary Chirp, Extended Binary Chirps, Clifford Hierarchy level, Howard algorithm

I. Introduction

THIS the introduction part: I think it is better to start by IoT and then describe BC, and then describe the Howard decoder, then extended BC papers and Finally explain that what we will do in this paper.

Also about the paper organization: It is better to start with preliminaries, then talk about Howard algorithm and how it works and extended BCs and finally numerical results.

In preliminaries part, first introduce Pauli group, then the Hierarchy levels and finally definition of BC.

In Howard algorithm part, first describe the Howard algorithm and then show that how it really works. Then describe why we need to consider $|e_i + e_{i+1} >$?

In extended BC, first describe

II. Preliminaries and System Model

In this section, we provide a mathematical framework for our analysis. To do so, first, we discuss the Heisenberg-Weyl group and also the Clifford Hierarchy levels, then, define the binary chirps.

A. Heisenberg-Weyl Group and Clifford Hierarchy

For a given $m \in \mathbb{N}$, consider $|0\rangle \triangleq \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle \triangleq \begin{bmatrix}0\\1\end{bmatrix}$ as the computational basis of $\mathcal{C}^2$. Considering $\mathbf{V} = (v_1, v_2, ..., v_m)$, where $v_i \in \{0,1\}, \forall i = 1, ..., m$, then $|\mathbf{v}\rangle = |v_1\rangle \otimes |v_2\rangle \otimes ... \otimes |v_m\rangle$ is the standard basis of $\mathbb{C}^N$, where $N = 2^m$, and $\mathbf{A} \otimes \mathbf{B}$ denotes the Kronecker (Tensor) product between $\mathbf{A}$ and $\mathbf{B}$.

The 2×2 Pauli matrices are defined as follows

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

It can be seen that the Pauli matrices are Hermitian. Define a m-fold Kronecker product or $N \times N$ $\mathbf{D}$-matrix with binary vectors $\mathbf{a} = (a_1, ..., a_m), \mathbf{b} = (b_1, ..., b_m) \in \mathbb{F}_2^m$ as

$$\mathbf{D}(\mathbf{a}, \mathbf{b}) \triangleq \mathbf{X}^{a_1}\mathbf{Z}^{b_1} \otimes \cdots \otimes \mathbf{X}^{a_m}\mathbf{Z}^{b_m}. \tag{2}$$

Part of this work has been published in Wireless Communications and Networking Conference (WCNC) in [1].

The Heisenberg-Weyl group, $\mathcal{HW}_N$, is defined as $\mathcal{HW}_N \triangleq \left\{i^k \mathbf{D}\left(\mathbf{a},\mathbf{b}\right) \mid \mathbf{a},\mathbf{b} \in \mathbb{F}_2^m,\ k=0,1,2,3\right\}$, in which its order is $4N^2$. It can be seen from Eq. (2) that

$$\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)\mathbf{D}\left(\mathbf{c},\mathbf{d}\right) = \left(-1\right)^{\mathbf{b}\mathbf{c}^T}\mathbf{D}\left(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}\right) = \left(-1\right)^{\langle \mathbf{a},\mathbf{b}|\mathbf{c},\mathbf{d}\rangle}\mathbf{D}\left(\mathbf{c},\mathbf{d}\right)\mathbf{D}\left(\mathbf{a},\mathbf{b}\right), \tag{3}$$

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 $\mathbb{F}_2^{2m}$. It can be seen from Eq. (3) that $\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)$ and $\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)$ commute iff $\langle \mathbf{a},\mathbf{b}|\mathbf{c},\mathbf{d}\rangle = 0$. According to the definition, we can rewrite Eq. (2) as

$$\mathbf{D}\left(\mathbf{a},\mathbf{b}\right) = \sum_{\mathbf{v}\in\mathbb{F}_2^m} \left(-1\right)^{\mathbf{b}\mathbf{v}^T} |\mathbf{v}+\mathbf{a}\rangle\langle\mathbf{v}|. \tag{4}$$

Finally, the Hermitian $N \times N$ Pauli matrices are of the form $\mathbf{E}(\mathbf{a},\mathbf{b}) = i^{\mathbf{a}\mathbf{b}^T}\mathbf{D}(\mathbf{a},\mathbf{b})$, where the exponent is taken in modulo 4. It is clearly Hermitian, since according to the definition $\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)^T = \left(-1\right)^{\mathbf{a}\mathbf{b}^T}\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)$.

One of the fundamental concepts for universal quantum computation is the Clifford Hierarchy of unitary operators [2], [3]. The first level of the Clifford Hierarchy is the Pauli group; $\mathcal{C}_1 = \mathcal{P}$ and higher levels are defined recursively, especially the level n is defined as

$$\mathcal{C}_n = \left\{\mathbf{G} \in \mathbb{U}_N \,\middle|\, \mathbf{G}\mathbf{P}\mathbf{G}^H \subseteq \mathcal{C}_{n-1}\right\}, \tag{5}$$

where $\mathbb{U}_N$ denotes the group of unitary $N \times N$ matrices. The second level, $\mathcal{C}_2$, describes the Clifford group and denoted by $\text{Cliff}_N \triangleq \left\{g \in \mathbb{U}_N \mid \mathbf{g}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\mathbf{g}^H = \mathbf{E}\left(\mathbf{a}',\mathbf{b}'\right)\right\}$. That means Cliff_N maps an element of Pauli to another element, and also, it can be seen that the Cliff_N is the normalizer of $\mathcal{HW}_N$. It is well-known fact that the automorphism induced by $\mathbf{g} \in \text{Cliff}_N$ satisfies

$$\mathbf{g}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\mathbf{g}^H = \pm\mathbf{E}\left(\left[\mathbf{a},\mathbf{b}\right]\mathbf{F}_g\right), \tag{6}$$

where $\mathbf{F}_g$ is a symplectic matrix, i.e., $\mathbf{F}_g\mathbf{\Omega}\mathbf{F}_g^T = \mathbf{\Omega}$, where $\mathbf{\Omega} = \begin{bmatrix}\mathbf{0}_m & \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{0}_m\end{bmatrix}$, in which $\mathbf{0}_m$ and $\mathbf{I}_m$ are all zero and identity $m \times m$ matrices, respectively.

B. Binary Chirps

The unit norm vectors indexed by $\mathbf{v}$ as follows

$$\mathbf{w}_{\mathbf{S},\mathbf{b}} = \frac{1}{\sqrt{N}}\left[i^{\mathbf{v^T S v}+\mathbf{2b^T v}}\right]_{\mathbf{v}\in\mathbb{F}_2^m}, \tag{7}$$

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

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 $\mathbf{H}_N \triangleq \mathbf{H}_2^{\otimes m}$ is an $N \times N$ Walsh-Hadamard matrix. According to the definition, $\mathbf{H}_2 = \frac{1}{\sqrt{2}}(\mathbf{I} - \mathbf{XZ})$, and then using the distributivity of the tensor product, we have

$$\mathbf{H}_N = \bigotimes_{1=1}^{m}\mathbf{H}_2 = \bigotimes_{i=1}^{m}\frac{1}{\sqrt{2}}(\mathbf{I}-\mathbf{XZ}) = \frac{1}{\sqrt{N}}\sum_{\mathbf{a}\in\mathbb{F}_2^m}(-1)^{w(\mathbf{a})}\mathbf{D}(\mathbf{a},\mathbf{a}) = \frac{1}{\sqrt{N}}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\mathbf{D}(\mathbf{0},\mathbf{a})\mathbf{D}(\mathbf{a},\mathbf{0}). \tag{8}$$

This is the version of the Walsh-Hadamard matrix where its diagonal elements are all one. Also, We have the ”naturally” ordered Walsh-Hadamard matrix defined as $\mathbf{H}_2^{nat} = \begin{bmatrix}1 & 1 \\ 1 & -1\end{bmatrix}^{\otimes m}$ and $\mathbf{H}_N^{nat} = \mathbf{H}_2^{nat\otimes m}$. We can switch between the different versions by multiplying $\mathbf{H}_N^{nat} = \mathbf{H}_N \mathbf{X}^{\otimes m}$ i.e., reversing the order of the columns. There is a neat sum form for the naturally ordered Walsh-Hadamard:

$$\mathbf{H}_N^{\text{nat}} = \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} \mathbf{D}(\mathbf{0}, \mathbf{a}) \mathbf{D}(\overline{\mathbf{a}}, \mathbf{0})$$

where $\overline{\mathbf{a}}$ is a bitwise complement of $\mathbf{a}$. Also, we can rewrite $\mathbf{H}_N^{\text{nat}}$ as follows

$$\mathbf{H}_N^{\text{nat}} = \frac{1}{\sqrt{N}} \sum_{\mathbf{u}, \mathbf{v} \in \mathbf{F}_2^m} (-1)^{\mathbf{u}\mathbf{v}^T} \left|\mathbf{u}\right\rangle\left\langle\mathbf{v}\right| \tag{9}$$

In the sequel, we denote the "all ones diagonal" version of the $N \times N$ Walsh-Hadamard matrix simply by $\mathbf{H}$. Walsh-Hadamard matrix belongs to the Clifford group as it permutes the Pauli group and it corresponds to the symplectic matrix $\mathbf{F} = \begin{bmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{bmatrix}$. This means that if we conjugate $\mathbf{E}(\mathbf{a}, \mathbf{b})$ with the Walsh-Hadamard matrix $\mathbf{H}$, the places of $\mathbf{a}$ and $\mathbf{b}$ will be swapped: $\mathbf{H}^H \mathbf{E}(\mathbf{a}, \mathbf{b}) \mathbf{H} = \pm \mathbf{E}([\mathbf{a}, \mathbf{b}]\, \mathbf{F}) = \pm \mathbf{E}(\mathbf{b}, \mathbf{a})$.

Consider the maximal commuting subgroup of Pauli group by $\mathcal{X}$-group: $\mathcal{X} = \{\mathbf{E}(\mathbf{a}, \mathbf{0}) \mid \mathbf{a} \in \mathbb{F}_2^m\}$, and $\mathcal{Z}$-group: $\mathcal{Z} = \{\mathbf{E}(\mathbf{0}, \mathbf{b}) \mid \mathbf{b} \in \mathbb{F}_2^m\}$. It can be seen that the Walsh-Hadamard matrix gives an isomorphism between the $\mathcal{X}$ and $\mathcal{Z}$ groups, since $\mathbf{H}^H \mathcal{X} \mathbf{H} = \mathcal{Z}$.

III. System Model

In this section, we first explain the system model considered in the paper, then discuss the Howard algorithm introduced in [5], and finally, show how the Howard algorithm is working.

A. Received Signal

We consider the transmission of the BCs over the additive white Gaussian noise channel for our analysis, and hence the received signal can be represented as follows

$$\mathbf{y} = \mathbf{w}_{\mathbf{S}, \mathbf{b}} + \mathbf{n}, \tag{10}$$

where $\mathbf{y} \in \mathbb{C}^N$ is the received signal, $\mathbf{n} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_N\right)$ denotes the noise of the system, and $\mathbf{w}_{\mathbf{S}, \mathbf{b}}$ is the BC given by Eq. (7). It can be seen that the BC codebooks represent the complex Grassmannian lines living in $\mathcal{G}_{\mathbb{C}}\left(N, 1\right)$. The chordal distance is considered as a metric in $\mathcal{G}_{\mathbb{C}}\left(N, 1\right)$, which is defined as

$$d_c\left(\mathbf{w}_1, \mathbf{w}_2\right) = \sqrt{1 - \left|\mathbf{w}_1^H \mathbf{w}_2\right|}, \tag{11}$$

and the minimum chordal distance is defined by

$$d_c\left(\mathcal{C}\right) = \min_{\substack{\mathbf{w}_1, \mathbf{w}_2 \in \mathcal{C} \\ \mathbf{w}_1 \neq \mathbf{w}_2}} d_c\left(\mathbf{w}_1, \mathbf{w}_2\right), \tag{12}$$

as a measure of the quality of the Grassmannian codebook. For the BC codewords, the minimum chordal distance has been found as

$$d_c\left(\mathbf{w}_1, \mathbf{w}_2\right) \geq \sqrt{1 - 2^{-\mathrm{R}/2}}, \tag{13}$$

where $\mathrm{R} = \mathrm{Rank}\left(\mathbf{S}_1 - \mathbf{S}_2\right)$, in which results in $d_c(\mathcal{C}) = \frac{1}{\sqrt{2}}$.

B. Howard Algorithm

A simple low-complex algorithm for decoding the BC has been proposed in [5] which contains the following steps:

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

In the sequel, we try to make it clear why this algorithm works. To do so, we consider two different coordinate-free representations for the BC given in Eq. (7) as follows

$$\mathbf{W_1} = \mathbf{g}\mathbf{H} \tag{14}$$

$$\mathbf{W_2} = \mathbf{g}\mathbf{H}\mathbf{g}^H, \tag{15}$$

where $\mathbf{g} = \text{diag}\left(i^{\mathbf{a}\mathbf{S}\mathbf{a}^T}\right), \mathbf{a}\in\mathbb{F}_2^m$. Before investigating the Howard algorithm, it is instructive to consider the two following lemmas.

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

Proof. Note that

$$\left(\mathbf{A}\otimes\mathbf{B}\right)\odot\left(\mathbf{C}\otimes\mathbf{D}\right) = \left(\mathbf{A}\odot\mathbf{C}\right)\otimes\left(\mathbf{B}\odot\mathbf{D}\right), \tag{16}$$

then, we have

$$\mathbf{D}(\mathbf{a},\mathbf{c})\odot\mathbf{D}(\mathbf{b},\mathbf{d}) = \left(\mathbf{x}^{a_1}\mathbf{z}^{c_1}\odot\mathbf{x}^{b_1}\mathbf{z}^{d_1}\right)\otimes ... \otimes\left(\mathbf{x}^{a_m}\mathbf{z}^{c_m}\odot\mathbf{x}^{b_m}\mathbf{z}^{d_m}\right). \tag{17}$$

As can be seen from (4), the $\mathbf{x}$ Pauli matrix changes the position of diagonal to anti-diagonal elements. As a result, 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, we have*

$$\mathbf{D}\left(\mathbf{a},\mathbf{b}+\mathbf{c}\right)\odot\mathbf{D}\left(\mathbf{a},\mathbf{b}\right) = \mathbf{D}\left(\mathbf{a},\mathbf{c}\right). \tag{18}$$

Proof. Consider Eq. (4), we have

$$\begin{aligned}\mathbf{D}\left(\mathbf{a},\mathbf{b}+\mathbf{c}\right)\mathbf{D}\left(\mathbf{a},\mathbf{b}\right) &= \sum_{\mathbf{v}\in\mathbb{F}_2^m}\left(-1\right)^{(\mathbf{b}+\mathbf{c})\mathbf{v}^T}|\mathbf{v}+\mathbf{a}\rangle\langle\mathbf{v}|\odot\sum_{\mathbf{u}\in\mathbb{F}_2^m}\left(-1\right)^{\mathbf{b}\mathbf{u}^T}|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}| \\ &\overset{(a)}{=}\sum_{\mathbf{u}\in\mathbb{F}_2^m}\left(-1\right)^{\mathbf{b}\mathbf{u}^T}|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}| = \mathbf{D}\left(\mathbf{a},\mathbf{c}\right)\end{aligned} \tag{19}$$

where (a) comes from the fact that $|\mathbf{v}+\mathbf{a}\rangle\langle\mathbf{v}|\odot|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}|$ is non-zero if $\mathbf{u}=\mathbf{v}$, since $\mathbf{u}$ and $\mathbf{v}$ are the standard basis vectors in $\mathbb{C}^N$. □

Also, note that

$$E(\mathbf{a},\mathbf{b}\oplus\mathbf{c})\odot E(\mathbf{a},\mathbf{b}) = i^{\mathbf{a}(\mathbf{b}\oplus\mathbf{c})^T}i^{\mathbf{a}\mathbf{b}^T}D(\mathbf{a},\mathbf{b}+\mathbf{c})\odot D(\mathbf{a},\mathbf{b}) = (-1)^{(\mathbf{b}+\mathbf{b}*\mathbf{c})\mathbf{a}^T}E(\mathbf{a},\mathbf{c}),$$

where $*$ denotes the element-wise product, and the final result comes from the fact that $\mathbf{a} \oplus \mathbf{b} = \mathbf{a} + \mathbf{b} - 2\mathbf{a} * \mathbf{b}$. Hence it is better to use $\mathbf{D}(.,.)$ instead of its counterpart $\mathbf{E}(.,.)$.

The following theorem clarifies how the Howard algorithm works.

Theorem 1. *Considering the coordinate-free representation of the BCs described in Eq.* (14) *and* (15)*, the output of the Howard algorithm for the jth shift can be written as*

$$\mathbf{H}\left(\overline{\mathbf{W}_i\left(\mathbf{a}\right)} \odot \mathbf{W}_i\left(\mathbf{a}+\mathbf{e}_j\right)\right) = \frac{-i^{\mathbf{e}_j \mathbf{S} \mathbf{e}_j^T}}{\sqrt{N}} \sum_{\mathbf{x} \in \mathbf{F}_2^m} (-1)^{\mathbf{e}_j \mathbf{S} \mathbf{x}^T} |\mathbf{S}_j\rangle\langle \mathbf{x}| \tag{20}$$

for $i \in \{1,2\}$, where $\mathbf{S}_j$ denotes the jth row of $\mathbf{S}$.

Proof. Starting with the first case, i.e., $\mathbf{W}_1 = \mathbf{g}\mathbf{H}$, using the definition we have

$$\mathbf{W}_1 = \mathbf{g}\mathbf{H} = \frac{1}{\sqrt{N}}\mathbf{g}\left(\sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}(\mathbf{a},\mathbf{a})\right) = \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{g}\mathbf{E}(\mathbf{a},\mathbf{a}) \tag{21}$$

$$\overline{\mathbf{W}_1} = \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{-w(\mathbf{a})}(-1)^{w(\mathbf{a})}\overline{\mathbf{g}}\mathbf{E}(\mathbf{a},\mathbf{a}) = \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}\overline{\mathbf{g}}\mathbf{E}(\mathbf{a},\mathbf{a}), \tag{22}$$

where $\overline{\mathbf{W}}_1$ denotes the elementwise complex conjugate of the matrix $\mathbf{W}_1$. Considering Eq. (21), we have

$$\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{W}_1 = \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{g}\mathbf{E}(\mathbf{a},\mathbf{a}), \tag{23}$$

then for calculating $\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{g}\mathbf{E}(\mathbf{a},\mathbf{a})$, we can perform as

$$\begin{aligned}
\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{g}\mathbf{E}(\mathbf{a},\mathbf{a}) &= i^{w(\mathbf{a})} \sum_{\mathbf{v} \in \mathbb{F}_2^m} |\mathbf{v}+\mathbf{e}_j\rangle\langle \mathbf{v}| \sum_{\mathbf{u} \in \mathbb{F}_2^m} i^{\mathbf{u}\mathbf{S}\mathbf{u}^T}|\mathbf{u}\rangle\langle \mathbf{u}| \sum_{\mathbf{x} \in \mathbb{F}_2^m} (-1)^{\mathbf{x}\mathbf{a}^T}|\mathbf{x}+\mathbf{a}\rangle\langle \mathbf{x}| \\
&= i^{w(\mathbf{a})} \sum_{\mathbf{v} \in \mathbb{F}_2^m} |\mathbf{v}+\mathbf{e}_j\rangle\langle \mathbf{v}| \sum_{\mathbf{u} \in \mathbb{F}_2^m} i^{\mathbf{u}\mathbf{S}\mathbf{u}^T}|\mathbf{u}\rangle\langle \mathbf{u}|(-1)^{(\mathbf{u}+\mathbf{a})\mathbf{a}^T}|\mathbf{u}\rangle\langle \mathbf{u}+\mathbf{a}| \\
&= i^{w(\mathbf{a})} \sum_{\mathbf{v} \in \mathbb{F}_2^m} i^{\mathbf{v}\mathbf{S}\mathbf{v}^T}(-1)^{(\mathbf{v}+\mathbf{a})\mathbf{a}^T}|\mathbf{v}+\mathbf{e}_j\rangle\langle \mathbf{v}+\mathbf{a}| \\
&= i^{w(\mathbf{a})} \sum_{\mathbf{v} \in \mathbb{F}_2^m} i^{(\mathbf{v}+\mathbf{a})\mathbf{S}(\mathbf{v}+\mathbf{a})^T}(-1)^{\mathbf{v}\mathbf{a}^T}|\mathbf{v}+\mathbf{a}+\mathbf{e}_j\rangle\langle \mathbf{v}|.
\end{aligned}$$

Replacing the result into Eq. (23), we get

$$\begin{aligned}
\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{W}_1 &= \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} \sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{w(\mathbf{a})} i^{(\mathbf{v}+\mathbf{a})\mathbf{S}(\mathbf{v}+\mathbf{a})^T}(-1)^{\mathbf{v}\mathbf{a}^T}|\mathbf{v}+\mathbf{a}+\mathbf{e}_j\rangle\langle \mathbf{v}| \\
&= \frac{1}{\sqrt{N}} \sum_{\mathbf{a} \in \mathbb{F}_2^m} \sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{w(\mathbf{a})} i^{\mathbf{a}\mathbf{S}\mathbf{a}^T}(-1)^{\mathbf{v}\mathbf{a}^T}|\mathbf{a}+\mathbf{e}_j\rangle\langle \mathbf{v}|.
\end{aligned} \tag{24}$$

where at the last equality, we replaced $\mathbf{a}$ with $\mathbf{a}+\mathbf{v}$. Hence, considering Eq. (24) and (22), one can proceed as follows

$$\begin{aligned}
\overline{\mathbf{W}_1} \odot \mathbf{E}(\mathbf{e}_j,0)\mathbf{W}_1 &= \frac{1}{N} \sum_{\mathbf{a} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}\overline{\mathbf{g}}\mathbf{E}(\mathbf{a},\mathbf{a}) \odot \sum_{\mathbf{b} \in \mathbb{F}_2^m} \sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{w(\mathbf{b})} i^{\mathbf{b}\mathbf{S}\mathbf{b}^T}(-1)^{\mathbf{v}\mathbf{b}^T}|\mathbf{b}+\mathbf{e}_j\rangle\langle \mathbf{v}| \\
&= \frac{1}{N} \sum_{\mathbf{a} \in \mathbb{F}_2^m} \sum_{\mathbf{b} \in \mathbb{F}_2^m} \sum_{\mathbf{v} \in \mathbb{F}_2^m} i^{w(\mathbf{a})}(-1)^{(\mathbf{b}+\mathbf{v})\mathbf{b}^T} i^{\mathbf{b}\mathbf{S}\mathbf{b}^T}(\overline{\mathbf{g}}\mathbf{E}(\mathbf{a},\mathbf{a})) \odot (|\mathbf{b}+\mathbf{e}_j\rangle\langle \mathbf{v}|),
\end{aligned} \tag{25}$$

where the term $(\overline{\mathbf{g}}\mathbf{E}\left(\mathbf{a},\mathbf{a}\right)) \odot (|\mathbf{b}+\mathbf{e}_j\rangle\langle\mathbf{v}|)$ can be written as

$$\begin{aligned}\overline{\mathbf{g}}\mathbf{E}(\mathbf{a},\mathbf{a}) &= i^{w(\mathbf{a})}\sum_{\mathbf{u}\in\mathbb{F}_2^m} i^{-\mathbf{u}\mathbf{S}\mathbf{u}^T}|\mathbf{u}\rangle\langle\mathbf{u}|\sum_{\mathbf{x}\in\mathbb{F}_2^m}(-1)^{\mathbf{x}\mathbf{a}^T}|\mathbf{x}+\mathbf{a}\rangle\langle\mathbf{x}| \\ &= i^{-w(\mathbf{a})}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\mathbf{u}\mathbf{a}^T} i^{-\mathbf{u}\mathbf{S}\mathbf{u}^T}|\mathbf{u}\rangle\langle\mathbf{u}+\mathbf{a}|. \qquad (26)\end{aligned}$$

Finally, replacing Eq. (26) into (25), we have

$$\begin{aligned}\overline{\mathbf{W}_1}\odot\mathbf{E}(\mathbf{e}_n,0)\mathbf{W}_1 &= \frac{1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\sum_{\mathbf{b}\in\mathbb{F}_2^m}\sum_{\mathbf{v}\in\mathbb{F}_2^m}(-1)^{(\mathbf{b}+\mathbf{v})\mathbf{b}^T} i^{\mathbf{b}\mathbf{S}\mathbf{b}^T}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\mathbf{u}\mathbf{a}^T} i^{-\mathbf{u}\mathbf{S}\mathbf{u}^T}|\mathbf{u}\rangle\langle\mathbf{u}+\mathbf{a}|\odot(|\mathbf{b}+\mathbf{e}_j\rangle\langle\mathbf{v}|) \\ &\overset{(a)}{=} \frac{1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{\mathbf{b}\mathbf{S}\mathbf{b}^T-(\mathbf{b}+\mathbf{e}_j)\mathbf{S}(\mathbf{b}+\mathbf{e}_j)^T}(-1)^{(2\mathbf{b}+\mathbf{a}+\mathbf{e}_j)\mathbf{b}^T+(\mathbf{b}+\mathbf{e}_j)\mathbf{a}^T}|\mathbf{b}+\mathbf{e}_j\rangle\langle\mathbf{a}+\mathbf{b}+\mathbf{e}_j| \\ &= \frac{1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{-2\mathbf{b}\mathbf{S}\mathbf{e}_j^T-\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}(-1)^{(\mathbf{a}+\mathbf{b})\mathbf{e}_j^T}|\mathbf{b}+\mathbf{e}_j\rangle\langle\mathbf{a}+\mathbf{b}+\mathbf{e}_j| \\ &= \frac{1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{-2(\mathbf{a}+\mathbf{b})\mathbf{S}\mathbf{e}_j^T+\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}(-1)^{(\mathbf{b}+\mathbf{e}_j)\mathbf{e}_j^T}|\mathbf{a}+\mathbf{b}\rangle\langle\mathbf{b}| \\ &= \frac{-1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{-2\mathbf{a}\mathbf{S}\mathbf{e}_j^T+\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}(-1)^{(\mathbf{e}_j+\mathbf{e}_j\mathbf{S})\mathbf{b}^T}|\mathbf{b}+\mathbf{a}\rangle\langle\mathbf{b}| \\ &= \frac{-1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{-2\mathbf{a}\mathbf{S}\mathbf{e}_j^T+\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}\mathbf{D}(\mathbf{a},\mathbf{e}_j+\mathbf{e}_j\mathbf{S}) \\ &= \frac{-i^{\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}}{N}\left(\sum_{\mathbf{a}\in\mathbb{F}_2^m}(-1)^{\mathbf{a}\mathbf{S}\mathbf{e}_j^T}\mathbf{D}(\mathbf{a},\mathbf{0})\right)\mathbf{D}(\mathbf{0},\mathbf{e}_j+\mathbf{e}_j\mathbf{S}), \qquad (27)\end{aligned}$$

where (a) comes from the fact that $|\mathbf{u}\rangle\langle\mathbf{u}+\mathbf{a}|\odot|\mathbf{b}+\mathbf{e}_j\rangle\langle\mathbf{v}| = 1$ iff $\mathbf{u}=\mathbf{b}+\mathbf{e}_j, \mathbf{u}+\mathbf{a}=\mathbf{v}$, thus $\mathbf{u}=\mathbf{b}+\mathbf{e}_j$ and $\mathbf{v}=\mathbf{a}+\mathbf{b}+\mathbf{e}_j$ is considered for proceeding.

Multiplying the Walsh-Hadamard, Eq. (9), with Eq. (27), and ignoring the last term, results in

$$\begin{aligned}\mathbf{H}_N^{\text{nat}}\sum_{\mathbf{a}\in\mathbb{F}_2^m}(-1)^{\mathbf{a}\mathbf{S}\mathbf{e}_j^T}\mathbf{D}(\mathbf{a},\mathbf{0}) &= \frac{1}{\sqrt{N}}\sum_{\mathbf{u},\mathbf{v}\in\mathbf{F}_2^m}(-1)^{\mathbf{u}\mathbf{v}^T}|\mathbf{u}\rangle\langle\mathbf{v}|\sum_{\mathbf{a},\mathbf{x}\in\mathbf{F}_2^m}(-1)^{\mathbf{S}_j\mathbf{a}^T}|\mathbf{x}+\mathbf{a}\rangle\langle\mathbf{x}| \\ &= \frac{1}{\sqrt{N}}\sum_{\mathbf{u},\mathbf{x},\mathbf{a}\in\mathbf{F}_2^m}(-1)^{(\mathbf{x}+\mathbf{a})\mathbf{u}^T}(-1)^{\mathbf{S}_j\mathbf{a}^T}|\mathbf{u}\rangle\langle\mathbf{x}| \\ &= \frac{1}{\sqrt{N}}\sum_{\mathbf{u},\mathbf{x}\in\mathbf{F}_2^m}(-1)^{\mathbf{u}\mathbf{x}^T}\sum_{\mathbf{a}\in\mathbf{F}_2^m}(-1)^{(\mathbf{u}+\mathbf{S}_j)\mathbf{a}^T}|\mathbf{u}\rangle\langle\mathbf{x}| \\ &= \sqrt{N}\sum_{\mathbf{x}\in\mathbf{F}_2^m}(-1)^{\mathbf{S}_j\mathbf{x}^T}|\mathbf{S}_j\rangle\langle\mathbf{x}| \qquad (28)\end{aligned}$$

where the last equality come from the fact that

$$\sum_{\mathbf{a}\in\mathbf{F}_2^m}(-1)^{(\mathbf{u}+\mathbf{S}_j)\mathbf{a}^T} = \begin{cases}0 & \mathbf{u}\neq\mathbf{S}_j \\ N & \mathbf{u}=\mathbf{S}_j\end{cases}. \qquad (29)$$

Finally, considering (27) and (28), we get

$$\mathbf{H}_N^{\text{nat}}\overline{\mathbf{W}_1}\odot\mathbf{E}(\mathbf{e}_n,0)\mathbf{W}_1 = \frac{-i^{\mathbf{e}_j\mathbf{S}\mathbf{e}_j^T}}{\sqrt{N}}\sum_{\mathbf{x}\in\mathbf{F}_2^m}(-1)^{\mathbf{e}_j\mathbf{S}\mathbf{x}^T}|\mathbf{S}_j\rangle\langle\mathbf{x}|, \qquad (30)$$

which is equivalent with Eq. (20).

In the sequel, we consider the second representation, i.e., $\mathbf{W}_2 = \mathbf{g}\mathbf{H}\mathbf{g}^H$. Using the definition, we have

$$\mathbf{W}_2 = \frac{1}{\sqrt{N}}\mathbf{g}\left(\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}\left(\mathbf{a},\mathbf{a}\right)\right)\mathbf{g}^H = \frac{1}{\sqrt{N}}\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}\left(\mathbf{a},\mathbf{a}+\mathbf{aS}\right) \tag{31}$$

$$\overline{\mathbf{W}_2} = \frac{1}{\sqrt{N}}\sum_{a} i^{-w(\mathbf{a})}(-1)^{\mathbf{a}(\mathbf{aS}+\mathbf{a})^T}\mathbf{E}\left(\mathbf{a},\mathbf{a}+\mathbf{aS}\right), \tag{32}$$

where in Eq. (31), we used the fact that $\mathbf{gE}(\mathbf{a},\mathbf{a})\mathbf{g}^H = +\mathbf{E}(\mathbf{a},\mathbf{a}+\mathbf{aS})$. It can be proven as follow

$$\begin{aligned}
\mathbf{gE}(\mathbf{a},\mathbf{a})\mathbf{g}^H &= \sum_{\mathbf{v}\in\mathbb{F}_2^m} i^{\mathbf{vSv^T}}|\mathbf{v}\rangle\langle\mathbf{v}| i^{\mathbf{aa}^T}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\mathbf{au}^T}|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}|\sum_{\mathbf{z}\in\mathbb{F}_2^m} i^{-\mathbf{zSz^T}}|\mathbf{z}\rangle\langle\mathbf{z}| \\
&= i^{\mathbf{aa}^T}\sum_{\mathbf{u}\in\mathbb{F}_2^m} i^{(\mathbf{u}+\mathbf{a})\mathbf{S}(\mathbf{u}+\mathbf{a})^T}(-1)^{\mathbf{au}^T} i^{-\mathbf{uSu}^T}|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}| \\
&= i^{(\mathbf{a}+\mathbf{aS})\mathbf{a}^T}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{(\mathbf{a}+\mathbf{aS})\mathbf{u}^T}|\mathbf{u}+\mathbf{a}\rangle\langle\mathbf{u}| = i^{(\mathbf{a}+\mathbf{aS})\mathbf{a}^T}\mathbf{D}(\mathbf{a},\mathbf{a}+\mathbf{aS}) = \mathbf{E}(\mathbf{a},\mathbf{a}+\mathbf{aS}).
\end{aligned}$$

Also, Eq. (32) resulted from using Eq. (31) and, considering the fact that $\mathbf{D}^T\left(\mathbf{a},\mathbf{b}\right) = (-1)^{\mathbf{ab}^T}\mathbf{D}\left(\mathbf{a},\mathbf{b}\right)$. Using Eq. (31), the shifted version of the codeword can be written as

$$\begin{aligned}
\mathbf{E}\left(\mathbf{e}_j,\mathbf{0}\right)\mathbf{W}_2 =& \frac{1}{\sqrt{N}}\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})}\mathbf{E}(\mathbf{e}_j,\mathbf{0})\mathbf{E}\left(\mathbf{a},\mathbf{aS}+\mathbf{a}\right) \\
=& \frac{1}{\sqrt{N}}\sum_{\mathbf{a}\in\mathbb{F}_2^m} i^{w(\mathbf{a})-\mathbf{a}(\mathbf{S}+\mathbf{I})\mathbf{e}_j^T}\mathbf{E}\left(\mathbf{a}+\mathbf{e}_j,\mathbf{aS}+\mathbf{a}\right)
\end{aligned} \tag{33}$$

Using Eq. (32) and (33), we get

$$\begin{aligned}
\overline{\mathbf{W}_2}\odot\mathbf{E}\left(\mathbf{e}_j,\mathbf{0}\right)\mathbf{W}_2 &= \frac{1}{N}\sum_{a} i^{-w(\mathbf{a})}(-1)^{\mathbf{a}(\mathbf{aS}+\mathbf{a})^T}\mathbf{E}\left(\mathbf{a},\mathbf{a}\left(\mathbf{S}+\mathbf{I}\right)\right)\odot\sum_{b} i^{w(\mathbf{b})-\mathbf{b}(\mathbf{S}+\mathbf{I})\mathbf{e}_j^T}\mathbf{E}\left(\mathbf{b}+\mathbf{e}_j,\mathbf{b}(\mathbf{S}+\mathbf{I})\right) \\
&= \frac{1}{N}\sum_{\mathbf{a}\in\mathbb{F}_2^m}(-1)^{\mathbf{a}(\mathbf{aS}+\mathbf{a})^T} i^{-w(\mathbf{a})}E\left(\mathbf{a},\mathbf{a}\left(\mathbf{S}+\mathbf{I}\right)\right)\odot\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{w(\mathbf{b})-\mathbf{b}(\mathbf{S}+\mathbf{I})\mathbf{e}_j^T}E\left(\mathbf{b}+\mathbf{e}_j,\mathbf{b}\left(\mathbf{S}+\mathbf{I}\right)\right) \\
&= \frac{1}{N}\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^m}\delta_{\mathbf{a},\mathbf{b}+\mathbf{e}_j}(-1)^{w(\mathbf{b})-w(\mathbf{a})} i^{\mathbf{bSb}^T-\mathbf{aSa}^T}D\left(\mathbf{a},\mathbf{a}\left(\mathbf{S}+\mathbf{I}\right)\right)\odot D\left(\mathbf{b}+\mathbf{e}_j,\mathbf{b}\left(\mathbf{S}+\mathbf{I}\right)\right) \\
&\overset{(a)}{=} \frac{1}{N}\sum_{\mathbf{b}\in\mathbb{F}_2^m}(-1)^{w(\mathbf{b})-w(\mathbf{b}\oplus\mathbf{e}_j)} i^{\mathbf{bSb}^T-(\mathbf{b}\oplus\mathbf{e_j})\mathbf{S}(\mathbf{b}\oplus\mathbf{e}_j)^T}\times \\
&\quad D\left(\mathbf{b}+\mathbf{e}_j,\mathbf{b}\left(\mathbf{S}+\mathbf{I}\right)+\mathbf{e}_j\left(\mathbf{S}+\mathbf{I}\right)\right)\odot D\left(\mathbf{b}+\mathbf{e}_j,\mathbf{b}\left(\mathbf{S}+\mathbf{I}\right)\right) \\
&\overset{(b)}{=} \frac{-1}{N}\sum_{\mathbf{b}\in\mathbb{F}_2^m} i^{\mathbf{bSb}^T-(\mathbf{b}\oplus\mathbf{e_j})\mathbf{S}(\mathbf{b}\oplus\mathbf{e}_j)^T}D\left(\mathbf{b}+\mathbf{e}_j,\mathbf{e}_j\left(\mathbf{S}+\mathbf{I}\right)\right) \\
&= \frac{-i^{-\mathbf{e}_j\mathbf{S}\mathbf{e}_j}}{N}\sum_{\mathbf{b}\in\mathbb{F}_2^m}(-1)^{\mathbf{bSe}_j^T}D\left(\mathbf{b}+\mathbf{e}_j,\mathbf{e}_j\left(\mathbf{S}+\mathbf{I}\right)\right),
\end{aligned} \tag{34}$$

where (a) and (b) are achieved using lemma 1 and 2, respectively. Also, the last term is equal to Eq. (27), and therefore applying the Hadamard transform, we get the same result. □

Remark 1. *We note that Theorem 1 reveals the location of the non-zero elements. In fact, $|\mathbf{S}_j\rangle$ is a map between the jth row of $\mathbf{S}$ and the basis vectors in 2^m and it has a non-zero element at the location of decimal mapping of the jth row of $\mathbf{S}$. Then, This theorem emphasizes that, at the output of the algorithm, non-zero elements are located at the row indexed by $\mathbf{S}_j$.*

Also, it is mentioned in [5] that instead of using $\mathbf{e}_j$, it is better to use $\mathbf{e}_j + \mathbf{e}_{j-1}$ (also it has been used in [6]). The main idea behind this approach is the multiple BCs scenario. Consider the case of two BCs received at the receiver, having the same jth row. It can happen that the next row of each of them can't be found using the Howard algorithm. In the following proposition, we provide proof of this statement.

Proposition 1. *In the multiple-BC transmit/receive scenarios, using shift by $\mathbf{e}_j$ may fail row recovery in the Howard algorithm, and it is better to use $\mathbf{e}_j + \mathbf{e}_{j-1}$.*

Proof. Consider the case that at the receiver two BCs have been received with parameters $\mathbf{S}, \mathbf{b}$ and $\mathbf{S}', \mathbf{b}'$, such that $\mathbf{S}_j = \mathbf{S}'_j$. Applying the procedure mentioned in theorem 1 for finding $\mathbf{S}_j$, results in

$$\mathbf{H}_N^{nat}\left(\overline{\mathbf{y}\left(\mathbf{a}\right)}\mathbf{y}\left(\mathbf{a}+\mathbf{e}_j\right)\right) = \left((-1)^{\mathbf{b}_1\mathbf{e}_j^T} + (-1)^{\mathbf{b}'\mathbf{e}_j^T}\right)|\mathbf{S}_j\rangle, \tag{35}$$

where it can be seen that if $\mathbf{b}_j \neq \mathbf{b}'_j$, results in cancellation. However, using $\mathbf{e}_j + \mathbf{e}_{j-1}$, if $\mathbf{S}_{j-1} \neq \mathbf{S}'_{j-1}$, then the non-zero location at the output of the algorithm for each of the BCs will be different and both can survive. □

C. List Decoding for Binary Chirp

In this section, using the algebraic features of the BC, we introduce a new algorithm that outperforms the original Howard. Considering a binary symmetric matrix $\mathbf{S}$, a maximal commutative subgroup of $\mathcal{HW}_N$ can be defined as

$$\mathcal{S}_{\mathbf{S}} = \left\{\mathbf{E}\left(\mathbf{x}, \mathbf{xS}\right) \mid \mathbf{x} \in \mathbb{F}_2^m\right\}. \tag{36}$$

Using m Pauli matrices $\mathbf{E}\left(\mathbf{e}_j, \mathbf{S}_j\right), r = 1, ..., m$, the subgroup $\mathcal{S}_{\mathbf{S}}$ can be generated. Also, it can be seen that a BC with parameters $\mathbf{S}, \mathbf{b}$ is a simultaneous eigenvector of $\mathcal{S}_{\mathbf{S}}$ and indeed of m Pauli matrices, i.e., $\mathbf{E}\left(\mathbf{e}_j, \mathbf{S}_j\right)$. This is the main property that enables an efficient low-complex decoding algorithm.

The BC defined in Eq. (7), can be decoded by finding a maximum set of commuting Pauli $\mathbf{E}$, such that the received signal is close to a common eigenvector of them. Following lemma clarifies this fact.

Lemma 3. *The BC, defined in Eq. (7), is a eigenvector of $\mathbf{E}\left(\mathbf{x}, \mathbf{xS}\right)$, i.e.,*

$$\mathbf{E}\left(\mathbf{x}, \mathbf{xS}\right)\mathbf{w}_{\mathbf{S},\mathbf{b}} = (-1)^{\mathbf{xb}^T}\mathbf{w}_{\mathbf{S},\mathbf{b}}. \tag{37}$$

Proof. According to the definition, we can perform as follows

$$\begin{aligned}\mathbf{E}\left(\mathbf{x}, \mathbf{xS}\right)\mathbf{w}_{\mathbf{S},\mathbf{b}} &= \frac{i^{\mathbf{xSx}^T}}{\sqrt{N}}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\mathbf{xSu}^T} i^{\mathbf{uSu}^T+2\mathbf{ub}^T}|\mathbf{u}+\mathbf{x}\rangle \\ &= \frac{i^{\mathbf{xSx}^T}}{\sqrt{N}}\sum_{\mathbf{v}\in\mathbb{F}_2^m}(-1)^{\mathbf{xS}(\mathbf{v}+\mathbf{x})^T} i^{(\mathbf{v}+\mathbf{x})\mathbf{S}(\mathbf{v}+\mathbf{x})^T+2(\mathbf{v}+\mathbf{x})\mathbf{b}^T}|\mathbf{v}\rangle \\ &= (-1)^{\mathbf{xb}^T}\mathbf{w}_{\mathbf{S},\mathbf{b}}. \end{aligned} \tag{38}$$

□

Therefore, similar to the Howard algorithm, one row of $\mathbf{S}$ at a time can be estimated [5]. For estimating the jth row of $\mathbf{S}$, $\mathbf{x} = \mathbf{e}_j$ is set. However, since $\mathbf{S}$ is a symmetric matrix, we need to consider the previously found rows. Define $\mathcal{R}$ as a set of previously determined rows, and $\widehat{\mathbf{S}}$ the partial symmetric matrix determined by the rows in $\mathcal{R}$. Consequently, the search space for $\mathbf{E}\left(\mathbf{e}_j, \mathbf{z}\right)$ is restricted to

$$\mathcal{Z}_j = \left\{\mathbf{z} \in \mathbb{F}_2^m \mid z_i = \widehat{s}_{j,i} \text{ for all } i \in \mathcal{R}\right\} \tag{39}$$

proportional to $\widehat{\mathbf{S}}$. In fact, for estimating the jth row of $\mathbf{S}$, we need to search for a Pauli $\mathbf{E} = \mathbf{E}\left(\mathbf{e}_j, \mathbf{z}\right); \ \mathbf{z} \in \mathcal{Z}$ such that $\mathbf{E}\mathbf{w}_{\mathbf{S},\mathbf{b}} = \pm\mathbf{w}_{\mathbf{S},\mathbf{b}}$. Also, for improving the estimation of the next rows, a projection operator can be used. The following lemma illuminates this fact.

Lemma 4. *Using the projection operator*

$$\prod\nolimits_{j,\epsilon} \triangleq \frac{\mathbf{I}_N + (-1)^{\epsilon}\mathbf{E}\left(\mathbf{e}_j, \mathbf{s}_j\right)}{2}, \tag{40}$$

for estimating the parameters of the BC, could result in degradation of the noise power.

Proof. Note that by considering lemma 3, we have

$$\prod\nolimits_{j,\epsilon}\mathbf{w}_{\mathbf{S},\mathbf{b}} = \begin{cases} \mathbf{w}_{\mathbf{S},\mathbf{b}}, & \text{if} \quad \epsilon = \mathbf{b}_j \\ \mathbf{0}, & \text{if} \quad \epsilon \neq \mathbf{b}_j \end{cases}. \tag{41}$$

In fact this operator project the received signal to an $N/2$-dimensional subspace. Hence, multiplying the received signal with this projection results in

$$\prod\nolimits_{j,\epsilon}\mathbf{y} = \mathbf{w}_{\mathbf{S},\mathbf{b}} + \prod\nolimits_{j,\epsilon}\mathbf{n}. \tag{42}$$

Assuming that the noise is circularly symmetric and i.i.d, then $p\left(\mathbf{n}\right) = p\left(\mathbf{U}\mathbf{n}\right)$, where $p\left(\mathbf{n}\right)$ denotes the probability distribution of the noise. This assumption holds for the considered system model, i.e., AWGN. Then the power of noise is halved by using this projection as follows

$$\begin{aligned} E\left\{\left\|\prod\nolimits_{j,\epsilon}\mathbf{n}\right\|^2\right\} &= \int p\left(\mathbf{n}\right)\mathbf{n}^H \prod\nolimits_{j,\epsilon} \mathbf{n} \, d\mathbf{n}d\mathbf{n}^* \\ &= \int p(\mathbf{n})\mathbf{n}^H\mathbf{U}^H\mathbf{I}_{N/2,N}\mathbf{U} \, \mathbf{n} \, d\mathbf{n}d\mathbf{n}^* \\ &= \frac{1}{2}E\left\{\left\|\mathbf{n}\right\|^2\right\}, \end{aligned} \tag{43}$$

where $\mathbf{I}_{N/2,N}$ is the identity with half-diagonal elements equal to zero. □

Another potential improvement in the decoding process is the selection of starting row. That means it is better to start with the row that is less corrupted by the noise. Algorithm 1 summarizes the procedure. Also, the low-complexity algorithm, based on the mentioned lemmas, for decoding each row is outlined in Algorithm 2. Finally, the proposed low-complex algorithm is given by Algorithm 3, which is based on keeping alive the multiple candidates to improve the decoding accuracy.

Algorithm 1 Decoding order selection.

```
Input: Received signal $\mathbf{y}$.
Output: Decoding order $\mathcal{O}$.
for $j = 1, ..., m$ do
    Compute $f_j(\mathbf{a}) = \mathbf{H}\left(\overline{\mathbf{y}(\mathbf{a})} \odot \mathbf{y}\left(\mathbf{a} + \mathbf{e}_j\right)\right)$.
    $\mu\left(j\right) = \max f_j\left(\mathbf{a}\right)$.
end for
Output decoding order is the order resulting from sorting $\mu$ in descending order.
```

IV. Extended Binary Chirps

In this section, first, we discuss the extended BC used in [7] and show that it lives at the 3rd level of the Hierarchy. Then, we introduce a new extended BC that lives at the nth level of the Hierarchy. Then, for the proposed higher-level BCs, we find the minimum distance, and finally, we propose simplified decoding.

Algorithm 2 Decoding jth row of $\mathbf{S}$

```
Input: Input signal $\mathbf{y}$, number of output candidates $K$, partial estimate $\widehat{\mathbf{S}}, \widehat{\mathbf{b}}$, estimated rows $\mathcal{R}$, Index of desired row to be estimated, $j$.
Output: List of $K$ partial candidates $\widehat{\mathbf{S}}_j$, metrics $\mu_k$, $\widehat{\mathbf{b}}$.
Compute $f_j(\mathbf{a}) = \mathbf{H}\left(\overline{\mathbf{y}(\mathbf{a})} \odot \mathbf{y}\left(\mathbf{a}+\mathbf{e}_j\right)\right)$.
Find search set $\mathcal{Z}_j \subset \mathbb{F}_2^m$ from $\mathcal{R}, \widehat{\mathbf{S}}$, and $j$ using (39).
Select $\mathbf{z}_k \in \mathcal{Z}_j, k = 1, ..., K$ according to $K$ largest $|f_j(\mathbf{a})|$.
Define $\mu = \|\mathbf{y}\|$.
for $k = 1, ..., K$ do
    Estimated $\widehat{\mathbf{S}}_k$ is $\widehat{\mathbf{S}}$ with $\widehat{\mathbf{S}}_j = \mathbf{z}_k$.
    $\sigma_k = \text{sign } f_j(\mathbf{z}_k)$.
    $\mu_k =$
    $\widehat{b}_j = \frac{1+\sigma_k}{2}$.
    $\mathbf{z}_k = \frac{1}{2}\left(\mathbf{I} + \sigma_k \mathbf{E}\left(\mathbf{e}_j, \mathbf{z}_k\right)\right)\mathbf{z}$.
end for
```

Algorithm 3 List decoding approach for decoding BCs

```
Input: Received signal $\mathbf{y}$, decoding order $\mathcal{O}$.
Output: Estimated $\widehat{\mathbf{S}}, \widehat{\mathbf{b}}$.
Initialize: Set $\mathcal{R} = \varnothing$ and candidate set $\mathcal{C} = \{(\mathbf{y}, K, \mathbf{0}_{m\times m}, \mathbf{0}_{m\times 1}, \varnothing, 0)\}$
for $j = 1, ..., m$ do
    Consider row $r = \mathcal{O}(j)$ to be estimated.
    Initialize candidate list $\mathcal{N} = \varnothing$.
    Number of branches $K' = \min\left(K, 2^{m-i+1}\right)$.
    for each $\left(\mathbf{z}_k, K', \widehat{\mathbf{S}}_k, \widehat{\mathbf{b}}, \mathcal{R}, r\right) \in \mathcal{C}$ do
        compute new candidates $\mathcal{N}_c = $ Algorithm 2 $\left(\mathbf{y}_k, K', \widehat{\mathbf{S}}_k, \widehat{\mathbf{b}}_k, \mathcal{R}, r\right)$.
        $\mathcal{N} = \mathcal{N} \cup \mathcal{N}_c$
    end for
    if $j < m$ then
        $\mathcal{C}$ is $\min\left(K, \text{size}\left(\mathcal{N}\right)\right)$ subset of $\mathcal{N}$ with largest $\mu_k$.
        Update decoded rows $\mathcal{R} = \mathcal{R} \cup \{r\}$.
    else
        Find elements correspond to maximum $\mu_k$ in $\mathcal{N}$.
    end if
end for
```

A. Extended Binary Chirp at the 3rd Level of the Hierarchy

An extension to the BCs has been considered in [7], where they assumed $\mathbf{S} = \overline{\mathbf{S}} + \frac{1}{2}\widetilde{\mathbf{S}}$ in Eq. (7), in which $\widetilde{\mathbf{S}}$ is an alternating matrix, i.e., symmetric with all zero diagonal elements. Using this extension, for $m = 2$, it can be seen that the number of codewords doubled. However, the maximum coherence increases from $\frac{1}{\sqrt{2}}$ to $\sqrt{\frac{5}{8}}$. As we know, the original BC is an element of Cliff_N and lives in the 2nd level of the hierarchy. Nevertheless, in the following lemma, we show that the extended BC considered in [7] belongs to 3rd level of the Hierarchy.

Lemma 5. *The extended BC described by*

$$\mathbf{w}_{Ext} = \frac{1}{\sqrt{N}}\left[i^{\mathbf{v}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{v}^T + 2\mathbf{b}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m}, \tag{44}$$

where $\widetilde{\mathbf{S}}$ is alternating matrix, belongs to 3rd level of the Hierarchy.

Proof. Consider $\mathbf{w}_{\text{Ext}}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\mathbf{w}_{\text{Ext}}^{H}$ for finding the level of the Hierarchy as follows

$$\begin{aligned}
\mathbf{w}_{\text{Ext}}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\mathbf{w}_{\text{Ext}}^{H} &= i^{\mathbf{a}\mathbf{b}^T}\sum_{\mathbf{v}\in\mathbf{F}_2^m} i^{(\mathbf{v}\oplus\mathbf{a})\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)(\mathbf{v}\oplus\mathbf{a})^T-\mathbf{v}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{v}^T}(-1)^{\mathbf{v}\mathbf{b}^T}|\mathbf{v}+\mathbf{a}><\mathbf{v}|\\
&\overset{(a)}{=} i^{\mathbf{a}\mathbf{b}^T}\sum_{\mathbf{v}\in\mathbf{F}_2^m} i^{(\mathbf{v}+\mathbf{a}-2\mathbf{v}\mathbf{D}_\mathbf{a})\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)(\mathbf{v}+\mathbf{a}-2\mathbf{v}\mathbf{D}_\mathbf{a})^T-\mathbf{v}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{v}^T}(-1)^{\mathbf{v}\mathbf{b}^T}|\mathbf{v}+\mathbf{a}><\mathbf{v}|\\
&\overset{(b)}{=} i^{\mathbf{a}\mathbf{b}^T+\mathbf{a}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{a}^T}\sum_{\mathbf{v}\in\mathbf{F}_2^m} i^{2\mathbf{v}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{a}^T-2(\mathbf{v}+\mathbf{a})\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}\mathbf{v}^T+2\mathbf{v}\mathbf{D}_\mathbf{a}\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}\mathbf{v}^T}(-1)^{\mathbf{v}\mathbf{b}^T}|\mathbf{v}+\mathbf{a}><\mathbf{v}|\\
&\overset{(c)}{=} i^{\mathbf{a}\mathbf{b}^T+\mathbf{a}\left(\overline{\mathbf{S}}+\frac{1}{2}\widetilde{\mathbf{S}}\right)\mathbf{a}^T}\sum_{\mathbf{v}\in\mathbf{F}_2^m} i^{\mathbf{v}\widetilde{\mathbf{S}}\mathbf{a}^T-2\mathbf{v}\mathbf{D}_{\overline{\mathbf{a}}}\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}\mathbf{v}^T}(-1)^{\mathbf{v}\left(\mathbf{b}+\mathbf{a}\overline{\mathbf{S}}+\mathbf{a}\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}\right)^T}|\mathbf{v}+\mathbf{a}><\mathbf{v}|\\
&\overset{(d)}{=} i^{\frac{1}{2}\mathbf{a}\widetilde{\mathbf{S}}\mathbf{a}^T}\mathbf{E}\left(\mathbf{a},\mathbf{b}+\mathbf{a}\overline{\mathbf{S}}+\mathbf{a}\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}\right)\operatorname{diag}\left(i^{\mathbf{v}\mathbf{S}'\mathbf{v}^T}\right) \qquad (45)
\end{aligned}$$

where (a) comes from the fact that for binary vectors $\mathbf{a}$ and $\mathbf{b}$, we have $\mathbf{a}\oplus\mathbf{v}=\mathbf{a}+\mathbf{v}-2\mathbf{a}*\mathbf{v}$, $\mathbf{D}_\mathbf{a}$ is a diagonal matrix where it has $\mathbf{a}$ as its diagonal elements and $\mathbf{v}*\mathbf{a}=\mathbf{v}\mathbf{D}_\mathbf{a}$. (b) is resulted from the symmetric property of $\overline{\mathbf{S}}$ and $\widetilde{\mathbf{S}}$, and in (c), $\mathbf{D}_{\overline{\mathbf{a}}}$ is a diagonal matrix with $\overline{\mathbf{a}}=\mathbf{I}\oplus\mathbf{a}$ as diagonal elements. Finally, (d) comes from the definition and $\mathbf{S}'=\mathbf{D}_{\mathbf{a}\widetilde{\mathbf{S}}}-2\mathbf{D}_{\overline{\mathbf{a}}}\widetilde{\mathbf{S}}\mathbf{D}_\mathbf{a}$. As a well-known fact, diag $\left(i^{\mathbf{v}\mathbf{S}'\mathbf{v}^T}\right)$ belongs to the Clifford group and since the element of Pauli group does not effect the Hierarchy level, we conclude that $\mathbf{w}\in\mathcal{C}_3$. □

Remark 2. *We note that if* $\widetilde{\mathbf{S}}=\mathbf{0}$ *at Eq.* (45)*, the result will be* $\mathbf{E}\left(\mathbf{a},\mathbf{b}+\mathbf{a}\widetilde{\mathbf{S}}\right)$ *which is consistent with [8]. Then it can be seen that extending the BC using* $\overline{\mathbf{S}}$*, increases the level of the Hierarchy.*

B. Extended Binary Chirp at the Level n

Motivated by this observation, we generalize the extended BC to nth level as follows.

Definition 1. *Define an extended BC as*

$$\tau_k\left(\mathbf{R}\right)=diag\left(\zeta_k^{\mathbf{v}\mathbf{R}\mathbf{v}^T \mod 2^k}\right), \qquad (46)$$

where $\zeta_k=e^{\frac{2\pi i}{2^k}}$*, and* $\mathbf{R}\in\mathbf{Z}_{2^k}$ *is a symmetric matrix, in which its anti-diagonal elements are in* $\mathbf{Z}_{2^{k-1}}$.

Using binary decomposition, $\mathbf{R}$ can be written in terms of binary symmetric matrices, i.e., $\mathbf{R}=\mathbf{S}_1+2\mathbf{S}_2+...+2^{k-1}\mathbf{S}_k=\sum_{i=1}^{k}2^{i-1}\mathbf{S}_i$. A symmetric matrix, $\mathbf{S}_i,\ i=1,2,...,k-1$ can be written as $\mathbf{S}_i=\mathbf{D}_i+\mathbf{A}_i+\mathbf{A}_i^T$, where $\mathbf{D}_i$ and $\mathbf{A}_i$ are diagonal and anti-diagonal matrices, respectively. However, for $\mathbf{S}_k=\mathbf{D}_k$, according to the definition of the BC, if $\mathbf{S}_k$ contains anti-diagonal elements, we have $2^{k-1}\mathbf{v}\left(\mathbf{A}_k+\mathbf{A}_k^T\right)\mathbf{v}^T \mod 2^k=2^k\mathbf{v}\mathbf{A}_k\mathbf{v} \mod 2^k=0$. In fact, $\mathbf{D}_k$ plays the Hadamard multiplication role in this extension as we have

$$\tau_k\left(\mathbf{R}\right)=\sum_{\mathbf{v}\in\mathbb{F}_2^m}\zeta_k^{\mathbf{v}\sum_{i=1}^{k-1}2^{i-1}\mathbf{S}_i\mathbf{v}^T}(-1)^{\mathbf{v}\mathbf{d}_k^T}, \qquad (47)$$

where $\mathbf{d}_k$ is a vector consisting of diagonal elements of $\mathbf{D}_k$. The following theorem, indicates that this extension lives in level k of the Hierarchy.

Theorem 2. *The extended BC defined in Def. 1 lives in the kth level of the Hierarchy and generates at most* $(k-1)\,2^{\frac{m(m+3)}{2}}$ *codewords.*

Proof. First, we prove that

$$\tau_k\left(\mathbf{R}\right)\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_k^H\left(\mathbf{R}\right)=\zeta_k^{\mathbf{aRa}^T}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_{k-1}\left(\widetilde{\mathbf{R}}\right) \tag{48}$$

as follows

$$\begin{aligned}
\tau_k\mathbf{E}\left([\mathbf{a},\mathbf{b}]\right)\tau_k^H &= i^{\mathbf{ab}^T}\sum_{\mathbf{v}\in\mathbf{F}_2^m}\zeta_k^{\mathbf{vRv}^T}|\mathbf{v}><\mathbf{v}|\sum_{\mathbf{u}\in\mathbf{F}_2^m}(-1)^{\mathbf{ub}^T}|\mathbf{u}+\mathbf{a}><\mathbf{u}|\sum_{\mathbf{x}\in\mathbf{F}_2^m}\zeta_k^{-\mathbf{xRx}^T}|\mathbf{x}><\mathbf{x}| \\
&= i^{\mathbf{ab}^T}\sum_{\mathbf{u}\in\mathbf{F}_2^m}\zeta_k^{(\mathbf{u}\oplus\mathbf{a})\mathbf{R}(\mathbf{u}\oplus\mathbf{a})^T-\mathbf{uRu}^T}(-1)^{\mathbf{ub}^T}|\mathbf{u}+\mathbf{a}><\mathbf{u}| \\
&= i^{\mathbf{ab}^T}\sum_{\mathbf{u}\in\mathbf{F}_2^m}\zeta_k^{(\mathbf{u}+\mathbf{a}-2\mathbf{u}*\mathbf{a})\mathbf{R}(\mathbf{u}+\mathbf{a}-2\mathbf{u}*\mathbf{a})^T-\mathbf{uRu}^T}(-1)^{\mathbf{ub}^T}|\mathbf{u}+\mathbf{a}><\mathbf{u}| \\
&\overset{(a)}{=} i^{\mathbf{ab}^T}\zeta_k^{\mathbf{aRa}^T}\sum_{\mathbf{u}\in\mathbf{F}_2^m}\zeta_k^{2\mathbf{aRu}^T-4(\mathbf{uD}_{\overline{\mathbf{a}}}+\mathbf{a})\mathbf{RD}_{\mathbf{a}}\mathbf{u}^T}(-1)^{\mathbf{ub}^T}|\mathbf{u}+\mathbf{a}><\mathbf{u}| \\
&\overset{(b)}{=} i^{\mathbf{ab}^T}\zeta_k^{\mathbf{aRa}^T}\sum_{\mathbf{u}\in\mathbf{F}_2^n}\zeta_{k-1}^{\mathbf{u}\left(\mathbf{D}_{\mathbf{G}}-2\mathbf{D}_{\overline{\mathbf{a}}}\mathbf{R}^{'}\mathbf{D}_{\mathbf{a}}\right)\mathbf{u}^T}(-1)^{\mathbf{ub}^T}|\mathbf{u}><\mathbf{u}| \\
&= \zeta_k^{\mathbf{aRa}^T}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_{k-1}\left(\widetilde{\mathbf{R}}\right),
\end{aligned} \tag{49}$$

where (a) results from the definition and $\mathbf{D}_{\overline{\mathbf{a}}}\triangleq\mathbf{I}-\mathbf{D}_{\mathbf{a}}$, in (b), $\mathbf{G}\triangleq\mathbf{aR}^{''}-2\mathbf{aR}'\mathbf{D}_{\mathbf{a}}$, where $\mathbf{R}'=\mathbf{S}_1+2\mathbf{S}_2+...+2^{k-3}\mathbf{S}_{k-2}$ and $\mathbf{R}^{''}=\mathbf{S}_1+2\mathbf{S}_2+...+2^{k-2}\mathbf{S}_{k-1}$, and finally $\widetilde{\mathbf{R}}=\mathbf{D}_{\mathbf{G}}-2\mathbf{D}_{\overline{\mathbf{a}}}\mathbf{R}^{'}\mathbf{D}_{\mathbf{a}}$. Thus using lemma 5, we know that τ_3 lives in 3rd level, and hence using Eq. (48) and definition of the Hierarchy level, $\tau_4\in\mathcal{C}_3$. Continuing this approach it can be seen that $\tau_k\in\mathcal{C}_k$.

Also, considering the binary representation of the $\mathbf{R}$, we have $k-1$ complete binary symmetric matrix in which each of them can generate $2^{\frac{m(m+1)}{2}}$ codewords, and finally $\mathbf{D}_k$ can generate 2^m different codewords.

Another approach: Using induction. Let's assume that $\tau_k\left(\mathbf{R}_k\right)\in\mathcal{C}_k$, then we need to prove that $\tau_k\left(\mathbf{R}_{k+1}\right)$ belongs to $\mathcal{C}_{k+1}$. Using the binary representation, $\mathbf{R}_{k+1}=\mathbf{S}_1+2\mathbf{S}_2+...+2^{k-1}\mathbf{S}_k+2^k\mathbf{D}_{k+1}$, we have $\tau_{k+1}=\tau_k(\mathbf{R}_k')\text{diag}\left(\zeta_{k+1}^{\mathbf{vS}_1\mathbf{v}^T}\right)$. Then $\tau_{k+1}(\mathbf{R}_{k+1})\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_{k+1}^H(\mathbf{R}_{k+1})=\tau_k\left(\mathbf{R}_k'\right)\text{diag}\left(\zeta_{k+1}^{\mathbf{vS}_1\mathbf{v}^T}\right)\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\text{diag}\left(\zeta_{k+1}^{-\mathbf{vS}_1\mathbf{v}^T}\right)\tau_k^H\left(\mathbf{R}_k'\right)$. Using a similar approach as lemma 5, we have

$$\text{diag}\left(\zeta_{k+1}^{\mathbf{vS}_1\mathbf{v}^T}\right)\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\text{diag}\left(\zeta_{k+1}^{-\mathbf{vS}_1\mathbf{v}^T}\right)=\zeta_{k+1}^{\mathbf{aS}_1\mathbf{a}^T}\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_k\left(\widetilde{\mathbf{R}}\right),$$

where $\widetilde{\mathbf{R}}=\mathbf{D}_{\mathbf{a}}+2\mathbf{D}_{\overline{\mathbf{a}}}\mathbf{S}_1\mathbf{D}_{\mathbf{a}}$. Thus, this results in $\zeta_{k+1}^{\mathbf{aS}_1\mathbf{a}^T}\tau_k\left(\mathbf{R}_k'\right)\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_k\left(\widetilde{\mathbf{R}}\right)\tau_k^H\left(\mathbf{R}_k'\right)=\zeta_{k+1}^{\mathbf{aS}_1\mathbf{a}^T}\tau_k\left(\mathbf{R}_k'\right)\mathbf{E}\left(\mathbf{a},\mathbf{b}\right)\tau_k\left(\widetilde{\mathbf{R}}-\mathbf{R}_k'\right)$, in which similarly using the approach in lemma 5, we have $\zeta_{k+1}^{\mathbf{aR}_3\mathbf{a}^T}\tau_k\left(\mathbf{R}_4\right)\in\mathcal{C}_k$. Since Pauli matrices do not affect the Hierarchy level, we can conclude that $\tau_{k+1}\left(\mathbf{R}_{k+1}\right)\in\mathcal{C}_{k+1}$. □

Through the analysis of the Hierarchy, one can find out that there exists a connection between the binary representation of the symmetric matrix used in the extended BC and the levels. The most significant matrix, i.e., $\mathbf{D}_k$, results in the first level, the second most significant i.e., $\mathbf{S}_{k-1}$, results in the second level, and so on.

C. Minimum Distance

What is the effect of this extension on the minimum distance of the BC? We expect a decrease in the minimum distance since the number of codewords has been increased. The following theorem shed light on the maximum coherence or worst-case coherence.

Theorem 3. *Maximum coherence between the codewords defined by the extended BC in Def. 1, independent of m, is*

$$\max_{i\neq j} \left|\mathbf{w}_i^H \mathbf{w}_j\right| = \cos\left(\frac{\phi_k}{2}\right), \tag{50}$$

where $\phi_k = \frac{2\pi}{2^k}$.

Proof. Considering the definition of the extended BC, we need to find

$$\max \frac{1}{N} \sum_{v\in\mathbb{F}_2^m} \zeta_k^{\mathbf{v}(\mathbf{R}_1-\mathbf{R}_2)\mathbf{v}^T} \tag{51}$$

where $\mathbf{R}_1$ and $\mathbf{R}_2$ correspond to codewords $\mathbf{w}_j$ and $\mathbf{w}_i$, respectively. For simplicity of analysis, set $\mathbf{R} = \mathbf{R}_1 - \mathbf{R}_2$, and therefore term in the exponential can be written as $\mathbf{vRv}^T = \sum_{i=1}^m r_{ii}v_i + 2\sum_{i<j} r_{ij}v_iv_j$. In fact, for calculating the summation, vector of 2^m different powers of ζ_k need to be considered, i.e., ζ_k to the power of the following vector

$$\mathbf{r} = \left(0, r_{11}, ..., r_{mm}, r_{11} + r_{22} + 2r_{12}, ..., r_{(m-1)(m-1)} + r_{mm} + 2r_{m(m-1)}, ..., \sum_{i=1}^m r_{ii} + \sum_{i<j} r_{ij}\right), \tag{52}$$

where first element is result of $v_i = 0, i = 1, ..., m$, second term is results of $v_1 = 1, v_i = 0, i = 2, .., m$, and so on. It is obvious that maximum value for $S = \sum_{\mathbf{v}\in\mathbb{F}_2^m} \zeta_k^{\mathbf{vRv}^T} = \sum_{i=1}^{2^m} \zeta_k^{a_i}$ for different values of $(a_1, ..., a_{2^m})$ is $2^m\zeta_k^c$ and achieved when all terms are equal i.e., $a_1 = a_2 = ... = a_{2^m} = c$. However, for calculating the summation in Eq. (51), as seen from Eq. (52), we can not set all of the terms to be equal, since the first term is 0, and setting other terms to be zero means all zero vector that leads to trivial case $\mathbf{R}_1 = \mathbf{R}_2$. Can we set other elements to be the same? The answer is no! For example setting $r_{11} = 1, r_{ij} = 0$, affects 2^{m-1} other positions and the result of absolute value of the sum will be $2^{m-1}\left|(1 + \zeta_k)\right| = 2^m \cos\left(\frac{\phi_k}{2}\right)$.

It can be seen that if we set $r_{11} = \ell, 1 \leq \ell \leq 2^k - 1$ and $r_{ij} = 0, \forall i, j = 2, ..., m$, results in $2^m \cos\left(\ell\frac{\phi_k}{2}\right) < \cos\left(\frac{\phi_k}{2}\right)$. Another case that needs to check is the case that $r_{12} = 1$ and zero otherwise. In this case only non-zero power appears when $v_1 = v_2 = 1$, which results in ζ_k^2 in 2^{m-2} cases, and for the rest of them, we have all zeros in Eq. (52). Hence, in this case, $|S| = \left|2^{m-2}\left(3 + \zeta_k^2\right)\right| < 2^m \cos\left(\frac{\phi_k}{2}\right)$. Another case worth investigating is the case where $r_{11} = r_{12} = 1$ and other elements are zero.

In this case 4 different situations exist: $(v_1, v_2) = (0, 0)$, $(v_1, v_2) = (1, 0)$, $(v_1, v_2) = (0, 1)$, and $(v_1, v_2) = (1, 1)$, which result in ζ_k^0, ζ_k^1, ζ_k^2, and ζ_k^3, respectively. Therefore, $|S| = 2^{m-2}\left|1 + \zeta_k + \zeta_k^2 + \zeta_k^3\right| < 2^m \cos\left(\frac{\phi_k}{2}\right)$, since the summation is over four different directions rather than two directions. Also, one can consider the case that all elements are zero, except $r_{12} = r_{23} = 1$. In this case using similar reasoning $|S| = 2^{m-3}\left|5 + 2\zeta_k^2 + \zeta_k^4\right| < 2^m \cos\left(\frac{\phi_k}{2}\right)$ (needs considering 5 different cases concentrating on $v_2 = 0$ and $v_2 = 1$). Also, another possible candidate for generating the maximum value of $|S|$ is considering the case $r_{12} = r_{34} = 1$ and other elements to be zero, which results in $|S| = 2^{m-4}\left|7 + 4\zeta_k^2 + \zeta_k^4\right| < 2^m \cos\left(\frac{\phi_k}{2}\right)$.

Hence, we can see that by adding more non-zero elements to $\mathbf{R}$, we get lower values for $|S|$, since the summation is over more different and also larger phases in these cases. Hence, we conclude that $\max\frac{1}{N}|S| = \cos\left(\frac{\phi_k}{2}\right)$. □

Considering $k = 2$, one could get $\max\frac{1}{N}|S| = \cos\left(\frac{\pi}{4}\right)$, which results in $d_c = \frac{1}{\sqrt{2}}$ which is consistent with result in [9], [10]. Also, the following proposition points out the minimum distance for extended BC considered in [7] (Eq. 44).

Proposition 2. *For the extended BC defined in Eq.* (44)*, the maximum coherence between codewrods is $\sqrt{\frac{5}{8}}$ and hence the minimum chordal distance is $\sqrt{\frac{3}{8}}$.*

Proof. Using similar approach as in theorem 3, consider $\mathbf{R} = 2\overline{\mathbf{S}} + \widetilde{\mathbf{S}}$ and $S = \frac{1}{N}\sum_{v\in\mathbb{F}_2^m} i^{\frac{1}{2}\left(\mathbf{vRv}^T\right)}$. One candidate is $\overline{s}_{11} = 1$ and zero otherwise, where results in $\frac{1}{N}\left|S\right| = \frac{2^{m-1}}{N}\left|1+i\right| = \frac{1}{\sqrt{2}}$. Another candidate is $\overline{s}_{12} = 1$ in which results in $\frac{1}{N}\left|S\right| = \frac{2^{m-2}}{N}\left|3+i^2\right| = \frac{1}{2}$. The case that $\widetilde{s}_{12} = 1$ and other elements are zero results in $\frac{1}{N}\left|S\right| = \frac{2^{m-2}}{N}\left|3+i\right| = \sqrt{\frac{5}{8}}$ which is the maximum coherence. Considering other options always result in smaller coherence values using same reasoning as in theorem 3. □

D. Simplified Extended Binary Chirp Decoder

In this subsection, we propose a low complexity algorithm to decode the extended BC. In [7], the authors proposed an exhaustive search approach for recovering the extended BC, defined in Eq. (44). To find $\widetilde{\mathbf{S}}$, they multiplied all the candidates by the received signal, then applied the Howard algorithm to recover the relevant $\overline{\mathbf{S}}$. Finally, among all the options, the best candidate is selected. However, this approach isn't suitable for the large values of m, e.g., $m = 10$ needs to test $2^{\frac{10\times 9}{2}} = 2^{45}$ different candidates.

Instead, we propose at first to consider the element-wise power 2 of the received signal, i.e., $\mathbf{y}^2$. Then apply the Howard algorithm to find $\widetilde{\mathbf{S}}$, and by using the selected candidate, reduce it from the received signal. Finally, apply the Howard algorithm to find $\widetilde{\mathbf{S}}$. The idea behind this approach is that, in the non-noisy condition, we have

$$\mathbf{y}^2 = \frac{1}{N}\left[i^{\mathbf{v}\left(2\overline{\mathbf{S}}+\widetilde{\mathbf{S}}\right)\mathbf{v}^T+4\mathbf{b}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m} = \frac{1}{N}\left[i^{\mathbf{v}\widetilde{\mathbf{S}}\mathbf{v}^T+2\mathbf{d_s}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m}, \tag{53}$$

where $\mathbf{d_s}$ denotes the diagonal elements of $\overline{\mathbf{S}}$. Hence, after considering the element-wise power 2, the received signal is a BC with $\mathbf{S} = \widetilde{\mathbf{S}}$ and $\mathbf{b} = \mathbf{d_s}$. Therefore, the Howard algorithm can be applied directly to find these parameters. After finding $\widetilde{\mathbf{S}}$, we can perform

$$\mathbf{y}\odot\left[i^{-\frac{1}{2}\mathbf{v}\widetilde{\mathbf{S}}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m} = \left[i^{\mathbf{v}\overline{\mathbf{S}}\mathbf{v}^T+2\mathbf{b}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m}, \tag{54}$$

where $\overline{\mathbf{S}}$, and $\mathbf{b}$, can be found using the Howard algorithm. Algorithm 4 summarizes this approach for more general extended BC defined in def. 1.

Algorithm 4 Simplified decoding algorithm for extended BC defined in Eq. 44

```
Input: Input signal $\mathbf{y}$, $m$.
Output: Estimated $\overline{\mathbf{S}}, \widetilde{\mathbf{S}}$, and $\mathbf{b}$.
Compute $\mathbf{y}_2 = \mathbf{y}\odot\mathbf{y}$.
Apply Howard algorithm to $\mathbf{y}_2$ in order to find $\widetilde{\mathbf{S}}$.
Compute $\mathbf{y}_3 = \mathbf{y}\odot\left[i^{-\frac{1}{2}\mathbf{v}\widetilde{\mathbf{S}}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m}$.
Apply Howard algorithm to find $\overline{\mathbf{S}}$ and $\mathbf{b}$.
```

However, the received signal usually suffers from noise. Hence, using this approach, the power of the noise will be increased, and using a simple Howard algorithm could result in significant performance degradation. Instead, we propose using Algorithm 3. In this algorithm for each $\mathbf{S}_i, i = 1, ..., k-1$, using the proposed Algorithm 3, K candidates can be found. Then for each candidate, by removing the previously founded $\mathbf{S}_{i-1}$, we apply Algorithm 3 and select the K best candidates among them. At the output of the Howard algorithm in the final state, one can treat estimated $\mathbf{b}$ as $\mathbf{D}_k$. Algorithm 5 describes this approach, where through numerical results, we show that the performance gap between the proposed and the exhaustive search approach is minor. However, one can apply the proposed low complexity approach for higher values of m.

Algorithm 5 Simplified decoding algorithm for extended BC defined in def. 1

```
Input: Input signal $\mathbf{y}$, $m$, $k$, and $K$.
Output: Estimated $\mathbf{S}_i, i = 1, ..., k-1$, and $\mathbf{D}_k$.
Initialize candidate list $\mathcal{N} = \left\{\widetilde{\mathbf{y}}_j, = \mathbf{y}, \widehat{\mathbf{S}}_j^i = \mathbf{0}\right\}_{j=1}^{K}, i = 1, ..., k-1$.
for i=1:k-1 do
    for each Candidate do
        Compute $\mathbf{y}_2^j = \underbrace{\widehat{\mathbf{y}}_j \odot ... \odot \widehat{\mathbf{y}}_j}_{2^{k-i-1}\text{ times}}$.
        Find $K$ candidate for $\widehat{\mathbf{S}}_j$ using Algorithm 3 based on $\mathbf{y}_2^j$
    end for
    Consider best $K$ candidtes and update $\mathcal{N}$.
    Update $\widetilde{\mathbf{y}}_j = \widetilde{\mathbf{y}}_j \odot \left[i^{-\frac{1}{2}\mathbf{v}\widetilde{\mathbf{S}}\mathbf{v}^T}\right]_{\mathbf{v}\in\mathbb{F}_2^m}$
end for
Select the best candidates among $K$ estimated parameters.
```

V. Numerical Results

VI. Conclusion

Future Works

It is interesting to consider an approach for extending the binary chirps to higher levels without reducing the minimum distance. Even if it isn't possible, it is worth investigating a new extension with a higher minimum distance than the proposed extended binary chirps. To do so, one can consider the Ungerboeck partitioning for 8-PSK. Also, there exist Dolsarle-Goethals (DG) codes, defined as

$$\text{DG}\left(m, r\right) = \left\{\mathbf{S} \middle| \text{rank}\left(\mathbf{S}_1 - \mathbf{S}_2\right) \geq 2r\right\}. \tag{55}$$

Thus at each level of the Hierarchy, the codebooks of the extended binary chirps need to be designed carefully. It is obvious that using the power two decoding approach, always less significant in terms of binary decomposition, is the worst one to achieve, i.e., $\mathbf{R}_0$ in $\mathbf{R} = \mathbf{R}_0 + 2\mathbf{R}_2 + ... + 2^{K-1}\mathbf{R}_{K-1}$.

Also, we need to reconsider the decoder in this case since the Howard algorithm only works on symmetric matrices without any constraints on them. However, considering a restriction on the codewords, it is interesting to find out a decoding approach that achieves a better result with lower complexity.

References

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

[2] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, 1999.

[3] N. Rengaswamy, R. Calderbank, and H. D. Pfister, "Unifying the clifford hierarchy via symmetric matrices over rings," *Physical Review A*, 2019.

[4] O. Tirkkonen and R. Calderbank, "Codebooks of complex lines based on binary subspace chirps," in *2019 IEEE Information Theory Workshop (ITW)*, 2019, pp. 1–5.

[5] 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 *2008 42nd Annual Conference on Information Sciences and Systems*, 2008, pp. 11–15.

[6] R. Calderbank and A. Thompson, "CHIRRUP: a practical algorithm for unsourced multiple access," *Information and Inference: A Journal of the IMA*, vol. 9, no. 4, pp. 875–897, 12 2019.

[7] R.-A. Pitaval and Y. Qin, "Chirp reconstruction algorithm for generalized second-order reed-muller frames," in *2021 IEEE Information Theory Workshop (ITW)*, 2021, pp. 1–6.

[8] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Logical clifford synthesis for stabilizer codes," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–17, 2020.

[9] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 358–374, 2010.

[10] R.-A. Pitaval and Y. Qin, "Grassmannian frames in composite dimensions by exponentiating quadratic forms," in *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 13–18.