Tirkkonen, Olav; Calderbank, Robert

Codebooks of Complex Lines Based on Binary Subspace Chirps

Published in:
2019 IEEE Information Theory Workshop, ITW 2019

DOI:
10.1109/ITW44776.2019.8989259

Published: 01/08/2019

Document Version
Peer reviewed version

Please cite the original version:
Tirkkonen, O., & Calderbank, R. (2019). Codebooks of Complex Lines Based on Binary Subspace Chirps. In *2019 IEEE Information Theory Workshop, ITW 2019* (pp. 639-643). [8989259] IEEE.
https://doi.org/10.1109/ITW44776.2019.8989259

Codebooks of Complex Lines Based on Binary Subspace Chirps

Olav Tirkkonen[1] and Robert Calderbank[2]
[1] Department of Communications and Networking, Aalto University, Finland
[2]Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina, USA
e-mail: olav.tirkkonen@aalto.fi, robert.calderbank@duke.edu

***Abstract*—Motivated by problems in machine-type wireless communications, we consider codebooks of complex Grassmannian lines in $N = 2^m$ dimensions. Binary Chirp (BC) codebooks of prior art are expanded to codebooks of Binary Subspace Chirps (BSSCs), where there is a binary chirp in a subset of the dimensions, while in the remaining dimensions there is a zero. BSSC codebooks have the same minimum distance as BC codebooks, while the cardinality is asymptotically 2.38 times larger. We discuss how BC codebooks can be understood in terms of a subset of the binary symplectic group $\mathrm{Sp}(2m, 2)$ in $2m$ dimensions; $\mathrm{Sp}(2m, 2)$ is isomorphic to a quotient group of the Clifford group acting on the codewords in N dimensions. The Bruhat decomposition of $\mathrm{Sp}(2m, 2)$ can be described in terms of binary subspaces in m dimensions, with ranks ranging from $r = 0$ to $r = m$. We provide a unique parameterization of the decomposition. The BCs arise directly from the full-rank part of the decomposition, while BSSCs are a group code arising from the action of the full group with generic r. The rank of the binary subspace is directly related to the number of zeros (sparsity) in the BSSC. We develop a reconstruction algorithm that finds the correct codeword with $\mathcal{O}(N \log^2 N)$ complexity, and present performance results in an additive white Gaussian noise scenario.**

I. Introduction

Massive Machine-type Communications (MTC) where multiple low-cost devices sporadically access communication resources, is of considerable current interest [1], [2]. Advanced random access methods have been investigated in this context, to lower the protocol burden on accessing devices. Both a *signature coding* principle [1], and an *unsourced random access* paradigm [2] are relevant.

Here we consider codes that can be used for random access, both from a signature coding, and an unsourced random access perspective. In addition to trading off cardinality against minimum distance, we are interested in low reconstruction/decoding complexity. In signature coding, each user has a unique signature, which is transmitted to initiate communication. It is assumed that the channel from a transmitter to a receiver is constant, but unknown, and that communication happens in a non-coherent manner. Accordingly coding happens in a *projective space*, where the overall phase of a codeword is irrelevant. Using conventional codes designed for linear spaces is thus suboptimal.

Binary Chirp sequences [3], [4] provide good signature codebooks, when the length of the codewords is a power of two, $N = 2^m$. Binary chirps come from a scaled fourth-root-of-unity alphabet $\{\pm 1, \pm i\}$, and there exists an $\mathcal{O}(N \log^2 N)$ decoding algorithm. The simple decoding is a consequence of the strong underlying algebraic structure, based on binary symplectic geometry.

Another motivation comes from virtual on-off duplexing for guaranteeing neighbor discovery in wireless networks [5]. In [6], it was observed that for neighbor discovery, it is beneficial to have a set of structured zeros in the transmission. Codebooks with entries from the set $\{\pm 1, 0\}$ were constructed, based on a *transformation* of binary chirp codewords.

Here, we construct codebooks with structured sets of vanishing entries, *expanding* the set of binary chirps. The underlying symplectic geometry allows larger codebooks, keeping the decoding complexity and distance properties fixed. By expanding the alphabet to include zero values, we construct binary subspace chirp codebooks. In these, the symplectic geometry not only dictates the algebra of the non-zero elements of the codebooks, but controls the on-off pattern by a mapping from sets of r-dimensional binary subspaces in m dimensions. Compared to binary chirps, there is more than twice as many codewords, at the same minimum distance.

This paper is organized as follows. In Section II, the concept of binary subspace chirps is introduced. Reconstruction algorithms are discussed in Section III, along with complexity and performance assessment. Some of the underlying algebraic machinery is summarized in the appendix.

II. Binary Subspace Chirps

A. Definition as $N = 2^m$-dimensional Vectors

Binary Chirps [3], [4] are a family of vectors in $N = 2^m$ dimensions with entries in $\frac{1}{\sqrt{N}}\{i^m\}_{m=0}^3$, which allow extremely simple decoder/reconstruction operations due to their inherent mathematical structure. Chirps can be defined as vectors with elements

$$w(\mathbf{a}) = \frac{1}{\sqrt{N}}(-i)^{\mathbf{a}^{\mathrm{T}}\mathbf{S}\mathbf{a} \,+\, 2*\mathbf{b}^{\mathrm{T}}\mathbf{a}} \tag{1}$$

where $\mathbf{a} \in \mathbb{F}_2^m$ is the index of the vector element in $N = 2^m$ dimensions in binary form, $\mathbf{S}$ is an $m \times m$ binary symmetric matrix, and $\mathbf{b} \in \mathbb{F}_2^m$ is a binary vector. The chirps are 2nd order Reed-Muller (RM) codes. Interesting subcodes of 2nd order RM give vectors with different minimum distances, related to sets of Kerdock, and Delsarte-Goethals vectors [7], [8]. The absolute value of the inner product of two distinct binary chirps is at most $1/\sqrt{2}$. Accordingly, binary chirps

can be considered a codebook $\mathcal{V}_{\rm chirp} \in \mathcal{G}(N,1,\mathbb{C})$ of Grassmannian lines in N-dimensional complex space. That is, they represent equivalence classes of N-dimensional complex vectors, up to phase rotations that are considered irrelevant for distance properties. Alternatively, $\mathcal{V}_{\rm chirp}$ can be understood as a collection of complex projective lines in $N+1$ dimensions, or a frame, i.e., an overcomplete basis, in $\mathbb{C}^N$. As there are $2^{m(m+1)/2}$ binary symmetric matrices, there are altogether

$$|\mathcal{V}_{\rm chirp}| = 2^{m(m+3)/2} = \sqrt{N}^{\ \log_2 N+3} \tag{2}$$

chirps. A chordal distance between two chirps, when considered as Grassmannian codewords, can be defined as

$$d(\mathbf{w}_1,\mathbf{w}_2) = \sqrt{1-|\mathbf{w}_1^{\rm H}\mathbf{w}_2|^2}\ , \tag{3}$$

and the minimum distance of $\mathcal{V}_{\rm chirp}$ is $d_{\min} = 1/\sqrt{2}$.

We now expand the set of binary chirps to binary subspace chirps. These are vectors that may take the value 0, in addition to integer powers of i. For this, take a rank r, and a binary r-dimensional subspace $\mathbf{H} \in \mathcal{G}(m,r,2)$. Then, take a binary symmetric $r\times r$ matrix $\mathbf{S}_r$, and a binary vector $\mathbf{b}\in\mathbb{F}_2^m$. The subspaces can be uniquely described in terms of Schubert cells $\mathcal{C}_{\mathcal{I}}$ as discussed in the appendix. These are indexed by ordered collections $\mathcal{I}$ of r elements from $\{1,2,\ldots,m\}$. For the rank of interest, a matrix $\mathbf{H}_{\mathcal{I}} \in \mathcal{C}_{\mathcal{I}}$ can be uniquely expanded to an invertible binary $m\times m$ matrix $\mathbf{P} = \left[\begin{array}{cc}\mathbf{H} & \mathbf{I}_{\widetilde{\mathcal{I}}}\end{array}\right]$, see the appendix. Here $\widetilde{\mathcal{I}}$ is the complement of $\mathcal{I}$. The $m-r$ dimensional subspace dual to $\mathbf{H}$ is $\widetilde{\mathbf{H}}$, and the inverse of $\mathbf{P}$ can be expressed in terms of $\widetilde{\mathbf{H}}$, see (22).

The subspace chirps can now be defined as the vectors $\mathbf{w}$ of sparsity determined by r, with elements

$$w(\mathbf{a}) = \frac{1}{\sqrt{2^r}}(-i)^{\mathbf{a}^{\rm T}\mathbf{P}^{-\rm T}\mathbf{S}\mathbf{P}^{-1}\mathbf{a}\ +\ 2\mathbf{b}^{\rm T}\mathbf{P}^{-1}\mathbf{a}}\ f(\mathbf{b},\mathbf{P}^{-1}\mathbf{a},r)\ , \tag{4}$$

where $\mathbf{S}$ is $\mathbf{S}_r$ expanded to an $m\times m$ symmetric matrix. The on-off pattern (which of the elements vanish) is determined by the binary polynomial

$$f(\mathbf{b},\mathbf{c},r) = \prod_{n=r+1}^{m}\ (1+b_n+c_n)\ , \tag{5}$$

which yields 1 iff the argument vectors $\mathbf{b}$ and $\mathbf{c}$ coincide in the last $m-r$ dimensions, and otherwise it is zero.

For full rank $r=m$, we have $\mathbf{P}=\mathbf{I}$. Thus $f=1$ for all $\mathbf{a}$, and one gets the binary chirp codewords (1). For $r<m$, using (21), we find that (4) is non-zero when

$$\widetilde{\mathbf{H}}_{\mathcal{I}}^{\rm T}\mathbf{a} = \mathbf{b}_{\tilde{r}}\ , \tag{6}$$

where $\mathbf{b}_{\tilde{r}}$ consists of the $m-r$ last elements in the parameter vector $\mathbf{b}$. As $\widetilde{\mathbf{H}}_{\mathcal{I}}$ has rank $m-r$, and its r-dimensional null space is given by $\mathbf{H}_{\mathcal{I}}$, all solutions of (6) can be written as

$$\mathbf{a} = \mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{\tilde{r}} + \mathbf{H}_{\mathcal{I}}\mathbf{x}\ , \tag{7}$$

where $\mathbf{x}$ is free in $\mathbb{F}_2^r$. This shows how $\mathbf{H}_{\mathcal{I}}$ yields the non-zero elements of the vector $\mathbf{w}$ in (4), and for rank r, there are precisely 2^r non-zero elements in $\mathbf{w}$. The binary subspace $\mathbf{H}_{\mathcal{I}}$ thus determines the *on-off pattern* of the codeword $\mathbf{w}$.

B. Grassmannian Line Codebook of Binary Subspace Chirps

The collection of binary subspace chirps $\mathbf{w}$ thus subsumes the set of binary chirps, with the alphabet enlarged to $\{\pm1,\pm i,0\}$, up to normalization. The interesting feature about the expanded set of vectors is that the minimum distance of the binary chirps is preserved. We have

Proposition 1: The set of binary subspace chirps, with all ranks $r\in\{0,1,\ldots,m\}$, and all binary subspaces $\mathbf{H}$ and binary symmetric matrices $\mathbf{S}_r$ of the given rank, and all vectors $\mathbf{b}$, provide a codebook $\mathcal{V}_{\rm BSSC}$ of Grassmannian lines in N dimensions with cardinality $|\mathcal{V}_{\rm BSSC}| = 2^m\prod_{k=1}^m\left(2^k+1\right)$, and minimum distance $d_{\min}=1/\sqrt{2}$.

Proof: If the ranks are different, $r'>r$, the inner product is non-zero in at most 2^r locations. The absolute values of the vector elements are $\sqrt{2}^{\ -r'}$ and $\sqrt{2}^{\ -r}$. The absolute value of the inner product is thus at most $2^r\sqrt{2}^{\ -r-r'} \le 1/\sqrt{2}$. The subspaces are described by invertible matrices $\mathbf{P}_1,\mathbf{P}_2$, and binary vectors $\mathbf{b}_1,\mathbf{b}_2$. For $r=r'$, (7) shows that the number of non-zero elements in the inner product is the number of pairs of binary r-dimensional vectors $\mathbf{x}_1,\mathbf{x}_2$ fulfilling

$$\mathbf{a} = \mathbf{P}_1\left[\begin{array}{c}\mathbf{x}_1\\ \mathbf{b}_{1,\tilde{r}}\end{array}\right] = \mathbf{P}_2\left[\begin{array}{c}\mathbf{x}_2\\ \mathbf{b}_{2,\tilde{r}}\end{array}\right]\ . \tag{8}$$

It is sufficient to investigate what restrictions the lower part of this equation poses on $\mathbf{x}_2$. Expanding as in (20) we find that $\mathbf{b}_{1,\tilde{r}} = \widetilde{\mathbf{H}}_1^{\rm T}\left[\begin{array}{cc}\mathbf{H}_2 & \mathbf{I}_{\widetilde{\mathcal{I}}}\end{array}\right]\left[\begin{array}{c}\mathbf{x}_2\\ \mathbf{b}_{2,\tilde{r}}\end{array}\right]$ has to be fulfilled. If the subspaces are not the same, the action of the dual space of one vector on the subspace of the other does not vanish, $\widetilde{\mathbf{H}}_1^{\rm T}\mathbf{H}_2 \neq \mathbf{0}$. Thus the space of solutions of (8) is at most $r-1$-dimensional, so that the vectors overlap in at most 2^{r-1} positions. The absolute value of the inner product is at most $2^{r-1}2^{-r}=1/2$. Finally, for the inner product of vectors with precisely the same non-zero subspace, one simply has the inner product of two binary chirps in 2^r dimensions, which is at most $1/\sqrt{2}$. ∎

The ratio of the cardinality of the binary chirp codebooks and the binary subspace chirp codebooks is $|\mathcal{V}_{\rm BSSC}|\,/\,|\mathcal{V}_{\rm chirp}| \approx 2.384$.

C. Connection to Binary Symplectic Group in $2m$ Dimensions

Recall that *stabilizer states* are defined as eigenvectors of commutative subgroups of the Pauli group. The cardinality of $\mathcal{V}_{\rm BSSC}$ is directly given by 2^m times the number of distinct maximal commutative subgroups of the Pauli group, thus $|\mathcal{V}_{\rm BSSC}|$ equals the number of stabilizer states. BSSCs are indeed directly related to stabilizer states, and for each BSSC, there is a maximal commutative set of Pauli matrices. Due to lack of space, we omit the discussion of this interesting connection. We shall use a diagonal reduction of this property when developing effective reconstruction algorithms. However, some details about the underlying symplectic geometry is needed.

The binary symplectic group $\mathrm{Sp}(2m,2)$, is the group of all binary $2m \times 2m$ matrices that fulfill $\mathbf{F}\mathbf{\Omega}\mathbf{F}^{\mathrm{T}} = \mathbf{\Omega}$, where

$$\mathbf{\Omega} = \begin{bmatrix} \mathbf{0}_m & \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{0}_m \end{bmatrix} . \tag{9}$$

The decomposition of $\mathrm{Sp}(2m,2)$ in terms of subgroups of block diagonal and upper triangular matrices has been discussed based on row echelon reduction in [9], and based on Bruhat decomposition in [10]. Consider the matrices

$$\mathbf{F}_D(\mathbf{P}) = \begin{bmatrix} \mathbf{P} & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{P}^{-\mathrm{T}} \end{bmatrix} , \ \mathbf{F}_U(\mathbf{S}) = \begin{bmatrix} \mathbf{I}_m & \mathbf{S} \\ \mathbf{0}_m & \mathbf{I}_m \end{bmatrix} , \tag{10}$$

where $\mathbf{P} \in \mathrm{GL}(m,2)$ is an invertible binary $m \times m$ matrix, $\mathbf{P}^{-\mathrm{T}}$ its inverse transpose, and $\mathbf{S} \in \mathrm{Sym}(m,2)$ a symmetric $m \times m$ matrix. Any symplectic matrix can be decomposed as a product of five matrices, two each of the form (10), and one of the form

$$\mathbf{F}_\Omega(r) = \begin{bmatrix} \mathbf{I}_{r-m} & \mathbf{I}_r \\ \mathbf{I}_r & \mathbf{I}_{r-m} \end{bmatrix} , \tag{11}$$

where $\mathbf{I}_r$ for $0 \leq r \leq m$ is the rank-deficient identity matrix with the first r diagonal elements 1, and $\mathbf{I}_{r-m} = \mathbf{I}_m - \mathbf{I}_r$. The matrices $\mathbf{F}_\Omega(r)$ interpolate between $\mathbf{I}_{2m}$ for $r = 0$, and $\mathbf{\Omega}$ for $r = m$. Products of elements of the form (10) form a subgroup

$$\mathcal{P} = \{\mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S}) \| \ \mathbf{P} \in \mathrm{GL}(m,2), \ \mathbf{S} \in \mathrm{Sym}(m,2)\} \tag{12}$$

which acts freely on the symplectic group both from right and left, and yields the Bruhat decomposition of $\mathrm{Sp}(2m,2)$. Here, we are interested in unique parametrization of cosets of $\mathcal{P}$. We have

Proposition 2: The cosets of the binary symplectic group $\mathrm{Sp}(2m,2)$ with respect to the upper triangular subgroup $\mathcal{P} \simeq \mathrm{GL}(m) \rtimes \mathrm{Sym}(m)$ are uniquely characterized by a rank $r = 0,\ldots,m$, a symmetric $r \times r$ matrix $\mathbf{S}_r$, and a rank r binary subspace $\mathbf{H}$ in m dimensions. A coset representative can be written as the product

$$\mathbf{F} = \mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})\mathbf{\Omega}(r) . \tag{13}$$

Here $\mathbf{P} \in \mathrm{GL}(m)$ is $\mathbf{H}$ complemented to an invertible matrix, as in (20), while $\mathbf{S}$ is an $m \times m$ symmetric binary matrix with $\mathbf{S}_r$ in the upper left corner, and otherwise filled with zeros.

Proof: The proof is left out due to lack of space. ∎

Consider the mapping (26) between the unitary representation of the Clifford group in N dimensions, and $\mathrm{Sp}(2m,2)$, discussed in the appendix. For each binary symplectic matrix in $2m$ dimensions, ϕ^{-1} gives a set of preimages, which are unitary matrices in N dimensions. This set can be generated from one unitary matrix by acting with the Pauli group, and the center of the Clifford group. Taking a representative of each of the unique cosets of $\mathrm{Sp}(2m,2)$ w.r.t. $\mathcal{P}$, as discussed in Proposition 2, and taking one of the unitary preimages, one gets a family of matrices parametrized by r, $\mathbf{H}$, and $\mathbf{S}$. The columns of these matrices correspond to the binary subspace chirps of (4), up to column rotations with i^k, thus the binary vector $\mathbf{b}$ is a *column index*. This structure is directly related to the natural interpretation of BSSCs as stabilizer states, which we leave out due to lack of space.

The binary chirps of (1) are a subset of BSSCs, related to the $\mathrm{Sp}(2m,2)$ cosets according to Proposition 2 with $r = m$, while BSSCs come from considering all values $r = 0,\ldots,m$. The underlying symplectic geometry is responsible for the distance properties of BSSCs and binary chirps, and the efficient yet simple reconstruction algorithm in [3]. Accordingly, expanding $\mathcal{V}_{\mathrm{chirp}}$ to $\mathcal{V}_{BSSC}$ corresponds to expanding from a set of cosets with $r = m$, to a set of cosets covering all of $\mathrm{Sp}(2m,2)$. This expansion of the chirp codebook is thus the largest that can be done preserving the underlying symplectic geometry. The symplectic structure can be used for efficient reconstruction of binary subspace chirps.

III. Reconstruction Algorithms

Given a noisy/corrupted version of a codeword, it is of interest ot understand how to efficiently reconstruct the original signal. Consider the signal model

$$\mathbf{y} = \mathbf{w} + \mathbf{n} , \tag{14}$$

where $\mathbf{n} \in \mathbb{C}^N$ represents noise. If the codewords were binary chirps, the efficient algorithm from [3], [4] could be used to identify $\mathbf{S}$ and $\mathbf{b}$, with $N\,(\log_2 N)^2$ complexity arising from computing $\mathcal{O}(\log_2 N)$ Walsh-Hadamard transforms.

When reconstructing a subspace chirp, one has to find the rank r, the subspace $\mathbf{H}$, the symmetric matrix $\mathbf{S}_r$, and the column index $\mathbf{b}$. If r and $\mathbf{H}$ were known, the algorithm from [3], [4] can be used to identify $\mathbf{S}_r$ and $\mathbf{b}$. To simplify reconstruction, we assume staged reconstruction, where r is found first, followed by finding $\mathbf{H}$.

A. Subspace Reconstruction

We first investigate some properties that follow from the BSSCs being stabilizer states. From (25) we have that the unitary matrix $\mathbf{G}_\mathbf{F}$, parametrized by the symplectic matrix $\mathbf{F}$, consists of eigenvectors of the Pauli operator $\mathbf{E}(\mathbf{c})$ precisely when the Pauli matrix $\mathbf{E}(\mathbf{c}^{\mathrm{T}}\mathbf{F})$ is diagonal. Recalling that the BSSCs $\mathbf{w}$ are columns of unitary matrices $\mathbf{G}_\mathbf{F}$, we thus have that $\mathbf{w}^{\mathrm{H}}\mathbf{E}(\mathbf{c})\mathbf{w} \neq 0$ iff $\mathbf{w}$ is an eigenvector of $\mathbf{E}(\mathbf{c})$. Moreover, the eigenvalues are ± 1. To identify the binary subspace of a BSSC, we concentrate on diagonal Pauli matrices $\mathbf{E}(0,\mathbf{b})$, for which $\mathbf{c} = \begin{bmatrix} 0 \\ \mathbf{b} \end{bmatrix}$.

From (25) we have that the unitary matrix $\mathbf{G}_\mathbf{F}$ corresponding to a symplectic matrix of the form (13) consists of eigenvectors of a diagonal Pauli matrix $\mathbf{E}(0,\mathbf{b})$, iff

$$\mathbf{b}^{\mathrm{T}}\mathbf{H}_\mathcal{I} = 0 . \tag{15}$$

As $\mathbf{H}_\mathcal{I}$ has rank r, there are precisely 2^{m-r} binary vectors $\mathbf{b}$ fulfilling (15), and precisely 2^{m-r} diagonal Pauli matrices which stabilize a rank r BSSC. These matrices are, by definition, commuting, and this set of matrices uniquely determines the binary subspace $\mathbf{H}_\mathcal{I}$, and thus the on-off pattern of the BSSC. All solutions of (15) can be written in terms of the dual subspace:

$$\mathbf{b} = \widetilde{\mathbf{H}}_\mathcal{I}\mathbf{x} , \tag{16}$$

where $\mathbf{x} \in \mathbb{F}_2^{m-r}$. To identify $\mathbf{H}_\mathcal{I}$ in the absence of noise, it is thus sufficient to find a set or $m-r$ linearly independent binary m-dimensional vectors $\mathbf{b}$ with

$$\mathbf{w}^{\mathrm{H}}\ \mathbf{E}(0,\mathbf{b})\ \mathbf{w} = \pm 1\ , \tag{17}$$

spanning the stabilizing diagonal Pauli matrices (16).

An efficient way to find the 2^{m-r} diagonal stabilizers is by Walsh-Hadamard transform. From (23) it follows that the diagonal Pauli matrices can by construction be written as $\mathbf{E}(0,\mathbf{b}) = \sum_{\mathbf{d}} (-1)^{\mathbf{d}^{\mathrm{T}}\mathbf{b}} \mathbf{e}_\mathbf{d}\mathbf{e}_\mathbf{d}^{\mathrm{T}}$, where $\mathbf{e}_\mathbf{d}$ is the 2^m-dimensional basis vector in the binary dimension $\mathbf{d} \in \mathbb{F}_2^m$. The needed inner products thus are

$$\mu(\mathbf{w},\mathbf{b}) = \mathbf{w}^{\mathrm{H}}\ \mathbf{E}(0,\mathbf{b})\ \mathbf{w} = \sum_{\mathbf{d}} (-1)^{\mathbf{d}^{\mathrm{T}}\mathbf{b}} |w_\mathbf{d}|^2\ . \tag{18}$$

Here, $w_\mathbf{d}$ is the element of $\mathbf{w}$ indexed by $\mathbf{d}$. In the right-hand side we recognize the binary description of the Walsh-Hadamard transform of the elementwise absolute vale of $\mathbf{w}$, i.e. the on-off pattern. The WH-transform of the on-off pattern is thus a *dual on-off pattern*, with 2^{m-r} non-zero elements, characterized by the dual $\widetilde{\mathbf{H}}$. A spanning set of $m-r$ positions $\mathbf{b}$ in the dual on-off pattern, together with their eigenvalues $\mu(\mathbf{w},\mathbf{b}) \in \{\pm 1\}$ fully determine the on-off pattern, i.e. the subspace where $\mathbf{w}$ is non-zero.

B. Reconstruction in the Presence of Noise

In the presence of noise, joint detection of rank r, subspace $\mathbf{H}$, and chirp content $\mathbf{S}, \mathbf{b}$ is optimal. Given a rank hypothesis $\hat{r}$, subspace detection of Section III-A can proceed with minor modifications. The WH-transform (18) of the on-off pattern yields arbitrary real values. We sort these in decreasing order, and find greedily the $m-\hat{r}$ largest elements with linearly independent $\mathbf{b}$, together with estimates of their eigenvalues $\mu(\mathbf{w},\mathbf{b}) \in \{\pm 1\}$. These yield an estimate of $\mathbf{H}_\mathcal{I}$, and an on-off pattern for the rank. An on-off pattern for all rank hypotheses can be computed with one Walsh-Hadamard transform only. Then, to reduce complexity, the inner product of the estimated rank-specific on-off patterns with the absolute value of the received signal are computed, and $K < m$ ranks with the largest inner products are selected. Chirp-reconstruction of [3] is performed in the candidate subspaces with different r, and the estimated codeword closest to the received signal is chosen.

C. Reconstruction Complexity

In detecting $\mathbf{S}_r$ and $\mathbf{b}$, using the algorithm of [3], the complexity is $\mathcal{O}(N \log^2 N)$, coming from a WH-transform. In the absence of noise, the subspace reconstruction algorithm of Section III-A is still dominated by WH and sorting complexity, where at most 2^{m-r} largest values should be found from N. Note that subspace decoding for all rank hypotheses can be performed once one WH-transform and sorting operation is done. Distance computation can be performed in $\mathcal{O}(N)$ operations. Thus if greedy subspace estimation is applied, even with an exhaustive search over rank hypotheses, the dominant complexity comes from applying the chirp reconstruction from [3], and is $\mathcal{O}(N \log^2 N)$.

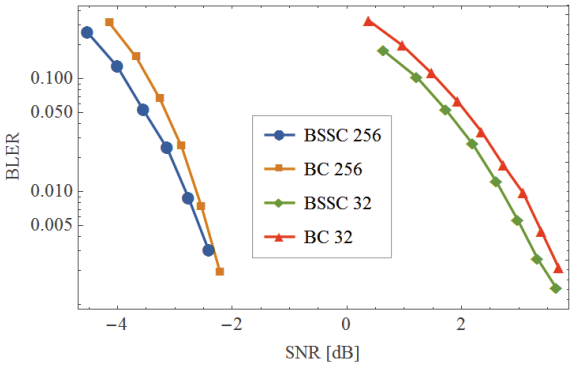

Fig. 1. Block error rate vs. SNR for BSSCs and binary chirps with $N = 32$ and $N = 256$.

D. Performance

We have performed Monte-Carlo simulations for BSSCs and BCs with $N = 32$ and $N = 256$, and receivers with $K = 3,\ 4$, respectively. For simplicity, we consider only an Additive White Gaussian Noise (AWGN) channel (14), not a random access scenario. One signature is chosen for transmission, and the receiver should identify the transmitted sequence. In Figure 1, the estimated detection error rate is reported against the average Signal-to-Noise power Ratio (SNR). It is remarkable that BSSCs perform slightly better than BCs, despite having higher cardinality. The reason is that while the codes have the same minimal distance, BSSC transmissions with lower rank have smaller number of neighboring codewords at the minimum distance, and accordingly a lower error probability than the full-rank transmissions. For BSSCs with $N = 256$, we observe performance degradation at high SNR due to the suboptimal receiver with $K = 4$.

IV. Conclusion

We have constructed families of Binary Subspace Chirps in $N = 2^m$ dimensions. These expand families of binary chirps to sequences where some elements may vanish. BSSCs have scaled fourth-root-of-unity elements in a non-zero subspace, characterized by an invertible binary $m \times m$ matrix. We have constructed a reconstruction algorithm BSSCs, based on an interpretation as stabilizer states. By Monte-Carlo simulation in an AWGN-channel, we have observed that BSSCs outperform Binary Chirps, despite the larger cardinality with the same minimum distance. In future work, we shall explore the underlying geometrical reasons for this, and address reconstruction in a multiple access scenario.

Appendix

A. Schubert Cells

Binary subspaces can be described in terms of Schubert cells. Denote r-dimensional subspaces over $\mathbb{F}_2^m$ as $\mathbf{H} \in \mathcal{G}(m,r,2) = \mathrm{GL}(m,2)/\mathrm{GL}(r,2)$. All subspaces can be grouped into Schubert cells $\mathcal{C}_\mathcal{I}$. Here $\mathcal{I} \subset \{1,\ldots,r\}$ is an ordered set of r indices with $i_n < i_j$ if $n < j$. The Schubert cell can be represented as the set of $m \times r$ matrices

$$\mathbf{H}_\mathcal{I} = \left[\ \mathbf{h}_{i_1}\ \cdots\ \mathbf{h}_{i_r}\ \right]\ , \tag{19}$$

where the first non-zero element in $\mathbf{h}_i$ is the ith element, and all matrix elements $h_{i_n i_j} = 0$ for $i_j \neq i_n$. The other matrix elements are free. There are $\binom{m}{r}$ different Schubert cells, and in cell $\mathcal{C}_\mathcal{I}$, the number of elements is $|\mathcal{C}_\mathcal{I}| = 2^{\sum_{n=1}^{r} i_n - n}$.

For each r-dimensional subspace $\mathbf{H}_\mathcal{I}$, there is a dual $m-r$-dimensional subspace $\widetilde{\mathbf{H}}_\mathcal{I}$, for which $\mathbf{H}^{\mathrm{T}}\widetilde{\mathbf{H}} = 0$, and similarly, for each Schubert cell $\mathcal{C}_\mathcal{I} \subset \mathcal{G}(m,r,2)$ there is a dual cell $\widetilde{\mathcal{C}}_\mathcal{I} \in \mathcal{G}(m,m-r,2)$ which consists of these dual subspaces. There is a one-to-one mapping between the set of dual Schubert cells $\{\widetilde{\mathcal{C}}_\mathcal{I}\}_{|\mathcal{I}|=r}$ and the set of $m-r$ dimensional Schubert cells $\{\mathcal{C}_\mathcal{I}\}_{|\mathcal{I}|=m-r}$. This mapping is realized by inverting the order of rows and columns in $\widetilde{\mathbf{H}}$.

We denote $\mathbf{I}_\mathcal{A}$ as the $m \times |\mathcal{A}|$ matrix with the columns of the $m \times m$ identity matrix indexed by the ordered set $\mathcal{A}$.

B. Invertible Matrices Representing Subspaces

An $m \times r$ matrix $\mathbf{H}_\mathcal{I} \in \mathcal{C}_\mathcal{I}$ can be complemented to an $m \times m$ invertible matrix

$$\mathbf{P}_\mathcal{I} = \left[\begin{array}{cc} \mathbf{H}_\mathcal{I} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{array} \right] . \tag{20}$$

Note that the $\mathbf{P}$-matrices are unique for a given rank r, but some $\mathbf{P}$ may represent subspaces of several ranks.

The inverse of $\mathbf{P}$ can directly be written in terms of the dual matrix. For the transpose of the inverse we have

$$\mathbf{P}^{-\mathrm{T}} = \left[\begin{array}{cc} \mathbf{I}_\mathcal{I} & \widetilde{\mathbf{H}}_\mathcal{I} \end{array} \right] . \tag{21}$$

Conjugate action with the anti-diagonal matrix $\mathbf{P}_{\mathrm{ad}}$ maps $\mathbf{P}^{-\mathrm{T}}$ to a matrix representing the dual cell:

$$\widetilde{\mathbf{P}} = \mathbf{P}_{\mathrm{ad}}\mathbf{P}^{-\mathrm{T}}\mathbf{P}_{\mathrm{ad}} = \left[\begin{array}{cc} \mathbf{H}_{\widetilde{\mathcal{I}}} & \mathbf{I}_\mathcal{I} \end{array} \right] , \tag{22}$$

where $\mathbf{H}_{\widetilde{\mathcal{I}}} = \mathbf{P}_{\mathrm{ad}}\widetilde{\mathbf{H}}_\mathcal{I}\mathbf{P}_{\mathrm{ad},m-r}$ is the unique element in $\mathcal{C}_{\widetilde{\mathcal{I}}}$ equivalent to the dual $\widetilde{\mathbf{H}}_\mathcal{I}$. The anti-dagonal matrices in the respective dimensions inverts the row and column orders.

C. Pauli Group

The Pauli (Heisenberg-Weyl) group in $N = 2^m$ dimensions can be represented by the semidirect product of the N^2 unitary matrices

$$\mathbf{E}(\mathbf{a},\mathbf{b}) = \mathrm{i}^{-\mathbf{a}^{\mathrm{T}}\mathbf{b}}\sigma_x^{a_1}\sigma_y^{b_1} \otimes \ldots \otimes \sigma_x^{a_m}\sigma_y^{b_m} \equiv \mathbf{E}(\mathbf{c}) , \tag{23}$$

and the center i^k. Here $\sigma_x, \sigma_y, \sigma_z$ are the 2D Pauli matrices, and

$$\mathbf{c} = \left[\begin{array}{c} \mathbf{a} \\ \mathbf{b} \end{array} \right] , \quad \mathbf{a} \in \mathbb{F}_2^m , \quad \mathbf{b} \in \mathbb{F}_2^m . \tag{24}$$

D. Mapping Between Symplectic and Clifford Groups

The binary symplectic group $\mathrm{Sp}(2m,2)$ is isomorphic to the outer automorphism group of the Pauli group:

$$\mathbf{G}_\mathbf{F}^{\mathrm{H}}\ \mathbf{E}(\mathbf{c})\ \mathbf{G}_\mathbf{F} = \pm\mathbf{E}\left(\mathbf{c}^{\mathrm{T}}\mathbf{F}\right) , \tag{25}$$

i.e. for each symplectic binary matrix $\mathbf{F}$ there exists a unitary transform $\mathbf{G}_\mathbf{F}$ in $N = 2^m$ dimensions which takes the Pauli group element corresponding to binary vector $\mathbf{c}$ to the element corresponding to $\mathbf{c}^{\mathrm{T}}\mathbf{F}$, up to a sign. For details, see [9].

The full automorphism group of the Pauli group can be created as the semidirect product of the matrices (25) representing $\mathrm{Sp}(2m,2)$ a and the Pauli group itself. Expanding with a center, one gets the Clifford group acting in N dimensions. We thus have a group homomorphism

$$\phi : \mathrm{Cliff}_N \mapsto \mathrm{Sp}(2m,2) , \tag{26}$$

where the preimage of each element of $\mathrm{Sp}(2m,2)$ is defined up to the Pauli group times some additional central elements. We shall be interested in the inverse images $\mathbf{G} = \phi^{-1}(\mathbf{F})$ of certain subgroups of symplectic matrices. This mapping of symplectic matrices to unitary matrices was discussed in [9]. Block diagonal matrices of the form (10), parameterized by an invertible matrix $\mathbf{P}$ correspond to the unitary permutations

$$\mathbf{G}_D(\mathbf{P}) : \mathbf{e}_\mathbf{v} \mapsto \mathbf{e}_{\mathbf{vP}} . \tag{27}$$

The upper triangular symplectic matrices $\mathbf{F}_U(\mathbf{S})$ in (10) map to unitary diagonal matrices with fourth-root of unity entries,

$$\mathbf{G}_U(\mathbf{S}) = \mathrm{diag}\left(\mathrm{i}^{\mathbf{vSv}^{\mathrm{T}} \bmod 4}\right) . \tag{28}$$

Finally, symplectic group elements of the form (11) correspond to r-fold tensor powers of 2×2 Walsh-Hadamard matrices $\mathbf{H}$,

$$\mathbf{G}_\Omega(r) \quad = \quad \mathbf{H}^{\otimes r} \ \otimes \ \mathbf{I}_{2^{m-r}} , \tag{29}$$

ACKNOWLEDGMENT

This work was funded in part by the Academy of Finland (grant 299916). We thank Andrew Thompson and Tefjol Pllaha for discussions on the subject matter.

REFERENCES

[1] Z. Utkovski, T. Eftimov, and P. Popovski, "Random access protocols with collision resolution in a noncoherent setting," *IEEE Wireless Comm. Lett.*, vol. 4, no. 4, pp. 445–448, Aug. 2015.

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

[3] 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*, Mar. 2008, pp. 11–15.

[4] L. Applebaum, S. D. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: Deterministic compressed sensing measurements for fast recovery," *Appl. Comput. Harmon. Anal.*, vol. 26, 2009.

[5] D. Guo and L. Zhang, "Virtual full-duplex wireless communication via rapid on-off-division duplex," in *Allerton Conference on Communication, Control, and Computing*, Sep. 2010, pp. 412–419.

[6] A. Thompson and R. Calderbank, "Compressed neighbour discovery using sparse kerdock matrices," in *Proc. IEEE ISIT*, Jun. 2018, pp. 2286–2290.

[7] A. Kerdock, "A class of low-rate nonlinear binary codes," *Information and Control*, vol. 20, no. 2, pp. 182–187, Mar. 1972.

[8] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The z_4-linearity of kerdock, preparata, goethals, and related codes," *IEEE Trans. Inf. Th.*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[9] T. Can, "An algorithm to generate a unitary transformation from logarithmically many random bits," Research Independent Study Report, Duke University, May 2017.

[10] D. Maslov and M. Roetteler, "Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations," *IEEE Trans. Inf. Th.*, 2018, in press.