Binary Subspace Chirps

Tefjol Pllaha, Olav Tirkkonen, *Senior Member, IEEE*, and Robert Calderbank, *Life Fellow, IEEE*

***Abstract*— We describe in detail the interplay between binary symplectic geometry and notions from quantum computation, with the ultimate goal of constructing highly structured codebooks. The Binary Chirps (BCs) are Complex Grassmannian Lines in $N = 2^m$ dimensions used in deterministic compressed sensing and random/unsourced multiple access in wireless networks. Their entries are fourth roots of unity and can be described in terms of second order Reed-Muller codes. The Binary Subspace Chirps (BSSCs) are a unique collection of BCs of *ranks* ranging from $r = 0$ to $r = m$, embedded in N dimensions according to an on-off pattern determined by a rank r binary subspace. This yields a codebook that is asymptotically 2.38 times larger than the codebook of BCs, has the same minimum chordal distance as the codebook of BCs, and the alphabet is minimally extended from $\{\pm 1, \pm i\}$ to $\{\pm 1, \pm i, 0\}$. Equivalently, we show that BSSCs are stabilizer states, and we characterize them as columns of a well-controlled collection of Clifford matrices. By construction, the BSSCs inherit all the properties of BCs, which in turn makes them good candidates for a variety of applications. For applications in wireless communication, we use the rich algebraic structure of BSSCs to construct a low complexity decoding algorithm that is reliable against Gaussian noise. In simulations, BSSCs exhibit an error probability comparable or slightly lower than BCs, both for single-user and multi-user transmissions.**

***Index Terms*— Massive random access, Grassmannian codes, Clifford matrices, stabilizer states, symplectic geometry.**

I. Introduction

CODEBOOKS of complex projective (Grassmannian) lines, or tight frames, have found application in multiple problems of interest for communications and information processing, such as code division multiple access sequence design [2], precoding for multi-antenna transmissions [3] and network coding [4]. Contemporary interest in such codes arise, e.g., from deterministic compressed sensing [5]–[9], virtual full-duplex communication [10], mmWave communication [11], and random access [12].

Manuscript received 23 February 2021; revised 14 December 2021; accepted 12 June 2022. Date of publication 29 June 2022; date of current version 22 November 2022. The work of Tefjol Pllaha and Olav Tirkkonen was supported in part by the Academy of Finland under Grant 319484 and Grant 334539. The work of Robert Calderbank was supported in part by the Air Force Office of Scientific Research under Grant FA 8750-20-2-0504. An earlier version of this paper was presented at the 2020 IEEE International Symposium on Information Theory [DOI: 10.1109/ISIT44484.2020.9174412]. *(Corresponding author: Tefjol Pllaha.)*

Tefjol Pllaha is with the Department of Mathematics, University of Nebraska, Lincoln, NE 68588 USA (e-mail: tefjol.pllaha@unl.edu).

Olav Tirkkonen is with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland.

Robert Calderbank is with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708 USA (e-mail: robert.calderbank@duke.edu).

Communicated by P. K. Sarvepalli, Associate Editor for Quantum.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2022.3186872.

Digital Object Identifier 10.1109/TIT.2022.3186872

One of the challenges/promises of 5G wireless communication is to enable massive machine-type communications (mMTC) in the Internet of Things (IoT), in which a massive number of low-cost devices sporadically and randomly access the network [13]. In this scenario, users are assigned a unique *signature* sequence which they transmit whenever active [14]. A complementary use-case is unsourced multiple access, where a large number of messages is transmitted infrequently. Polyanskiy [13] proposed a framework in which communication occurs in blocks of N channel uses, and the task of a receiver is to identify correctly L active users (messages) out of 2^B, with one regime of interest being $N = 30,000, L = 250$, and $B = 100$. Ever since its introduction, there have been several follow-up works [12], [15]–[18], extensions to a massive MIMO scenario [19] where the base station has a very large number of antennas, and a discussion on the fundamental limits on what is possible [20].

Given the massive number of users/messages to-be-supported, the design criteria are fundamentally different from classical multiple-access channel, and solutions have to be sought for from novel directions. For instance, interference is unavoidable due to the high number of users. Moreover, due to the randomness in channel access, the level of interference varies from instance to instance. As the transmissions are of initial access type, phase coherence or instantaneous power control cannot be assumed. Thus, the challenge becomes to design highly structured codebooks of large cardinality, subject to invariance with respect to absolute phase and amplitude, along with a reliable and low-complexity multi-user decoding algorithm.

Codebooks of Binary Chirps (BCs) [6], [21] provide such highly structured Grassmannian line codebook in $N = 2^m$ dimensions with additional desirable properties. All entries come from a small alphabet, being a fourth root of unity, and can be described in terms of second order Reed-Muller (RM) codes. RM codes have the fascinating property that a Walsh-Hadamard measurement cuts the solution space in half. This yields a single-user decoding complexity of $\mathcal{O}(N \log^2 N)$, coming from the Walsh-Hadamard transform and number of required measurements. Additionally, the number of codewords is reasonably large, growing as $2^{m(m+3)/2} = \sqrt{N}^{3+\log_2 N}$, while the minimum *chordal distance* is $1/\sqrt{2}$.

In this paper, we expand the BC codebook to the codebook of Binary Subspace Chirps (BSSCs) in $N = 2^m$ dimensions by collectively considering all BCs in $S = 2^r$ dimensions for $r = 0, \ldots, m$. That is, given a BC in $S = 2^r$ dimensions, we embed it in $N = 2^m$ dimensions via a unique *on-off pattern* determined by a rank r binary subspace. Thus, a BSSC is characterized by a *sparsity* r, a BC part parametrized by a binary symmetric matrix $\mathbf{S}_r \in \mathrm{Sym}(r; 2)$ and a binary vector

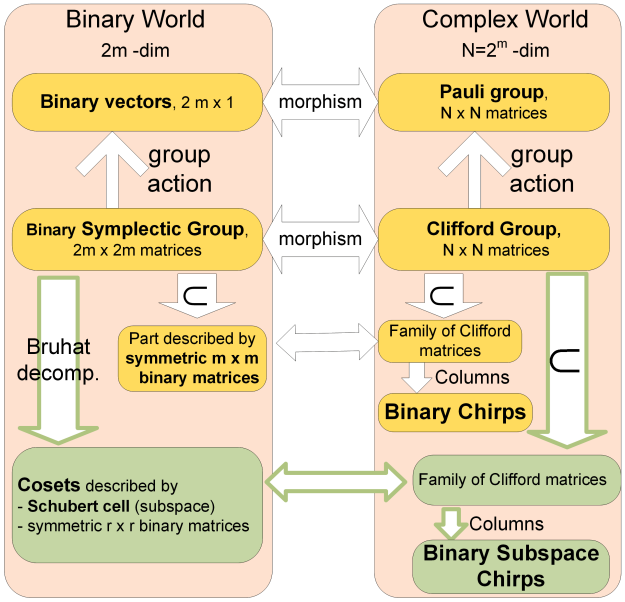

Fig. 1. Interplay of binary world and complex world. The interplay detailed in this paper, which is then used in the low-complexity decoding algorithm of BSSCs, is depicted in green.

$\mathbf{b} \in \mathbb{F}_2^m$, and a unique on-off pattern parametrized by a rank r binary subspace $H \in \mathcal{G}(m, r; 2)$. Thus, an active device with a rank r signature will transmit $\alpha/\sqrt{2^r}$, $\alpha \in \{\pm 1, \pm i\}$ during time slots determined by the rank r subspace H, and it will be silent otherwise. This resembles the model of [10], in which active devices can also be used (to listen) as receivers during the off-slots. The codebook of BSSCs inherits all the desirable properties of BCs, and in addition, it has asymptotically about 2.384 more codewords.

Given the structure of BSSCs, a unified rank, on-off pattern, and BCs part (in this order) estimation technique is needed. In [22], a reliable on-off pattern detection was proposed, which made use of a Weyl-type transform [23] on m qubit diagonal Pauli matrices. The algorithm can be described with the common language of symplectic geometry and quantum computation. We show that BSSCs are common eigenvectors of maximal sets of commuting Pauli matrices, commonly referred in literature as *stabilizer groups*. In this way BSSCs constitute nothing else but a parametrization of *stabilizer states*. While there are other known parametrizations, e.g. [24], the parametrization of this paper is derived in such a way that it can be leveraged to a low-complexity decoding algorithm. The key insight will be to decode a BSSC by estimating the corresponding unique maximal stabilizer that stabilizes it. In particular, we show that each BSSC is a column of a *unique* Clifford matrix (99), which itself is the common eigenspace of a unique stabilizer group (110); see also Theorem 3. The interplay between the binary world and the complex world is depicted in Figure 1.

Making use of these structural results, the on-off pattern detection of [22] can be generalized to recover the BC part of the BSSC, this time by using the Weyl-type transform on the off-diagonal part of the corresponding stabilizer group. This yields a single-user BSSC reconstruction as described in Algorithm 2. In [1], we added Orthogonal Matching Pursuit (OMP) to obtain a multi-user BSSCs reconstruction (see Algorithm 3) with reliable performance when there is a small number of active users. As the number of active users increases, so does the interference, which has a quite destructive effect on the on-off pattern. However, state-of-the-art solutions for BCs [9], [18], [25] such as slotting and patching, can be used to reduce the interference. Preliminary simulations show that BSSCs exhibit a lower error probability than BCs. This is because BSSCs have fewer closest neighbors on average than BCs. In addition, BSSCs are uniformly distributed over the sphere, which makes them optimal when dealing with Gaussian noise.

Throughout, the decoding complexity is kept at bay by exploiting the underlying symplectic geometry. The sparsity, the BC part, and the on-off pattern of a BSSC can be described in terms of the Bruhat decomposition (31) of a symplectic matrix. Indeed, the unique Clifford matrix (99) of which a BSSC is a column, is parametrized by a coset representative (33) as described in Lemma 1. In turn, such coset representative determines a unique stabilizer group (110). We use this interplay to reconstruct a BSSC *by reconstructing the stabilizer group that stabilizes the given BSSC*. This alone reduces the complexity from $\mathcal{O}(N^2)$ to $\mathcal{O}(N \log_2 N)$.

The paper is organized as follows. In Section II we formulate the problem and motivate the solution approach. In Section III we review the basics of binary symplectic geometry and quantum computation. In order to obtain a unique parametrization of BSSCs, we use Schubert cells and the Bruhat decomposition of the symplectic group. In Section III-D we lift the Bruhat decomposition of the symplectic group to obtain a decomposition of the Clifford group. Additionally, we parametrize those Clifford matrices whose columns are BSSCs. In Section IV we give the formal definition of BSSCs, along with their algebraic and geometric properties. In Sections V and VI we present reliable low complexity decoding algorithms, and discuss simulation results. We end the paper with some conclusions and directions future research.

A. Main Contributions

We have extended the codebook of binary chirps to the codebook of binary subspace chirps which is asymptotically 2.38 times bigger and has the same minimum chordal distance as stated in Theorem 1. In Corollary 1 we show that binary subspace chirps are precisely the collection of stabilizers states, which in turn immediately makes them a non-Abelian group code with a faithful representation in N dimensions. Of prime interest is the corresponding unique maximal stabilizer as described in Theorem 3. We use the underlying group structure to generalize the algorithm of [6] to a BSSC setting without significantly increasing the complexity. We argue that binary subspace chirps constitute good candidates in a variety of IoT applications such as random access, unsourced access, and neighbor discovery.

B. Conventions

All vectors, binary or complex, will be columns. $\mathbb{F}_2$ denotes the binary field, $\mathrm{GL}(m; 2)$ denotes the group of binary $m \times m$

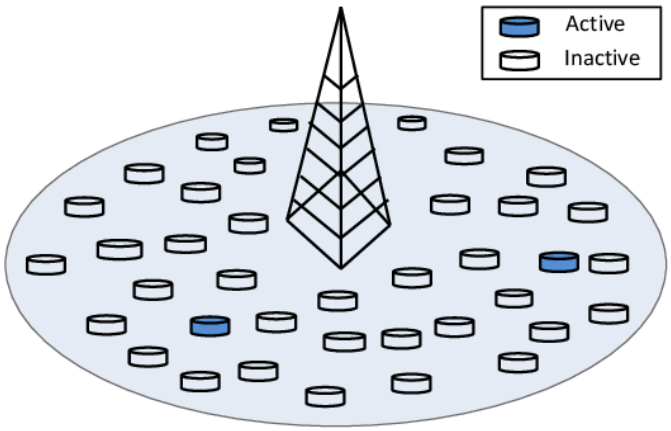

Fig. 2. Massive random access.

invertible matrices, and $\mathrm{Sym}(m;2)$ denotes the group of binary $m \times m$ symmetric matrices. We will denote matrices (resp., vectors) with upper case (resp., lower case) bold letters. $\mathbf{A}^{\mathsf{T}}$ will denote the transpose and $\mathbf{A}^{-\mathsf{T}}$ will denote the inverse transposed. $\mathrm{cs}\,(\mathbf{A})$ and $\mathrm{rs}\,(\mathbf{A})$ will denote the column space and the row space of $\mathbf{A}$ respectively. Since all our vectors are columns, we will typically deal with column spaces, except when we work with notions from quantum computation, where row spaces are customary. $\mathbf{I}_m$ will denote the $m \times m$ matrix (complex or binary). $\mathcal{G}(m,r;2) \cong \mathrm{GL}(m;2)/\mathrm{GL}(r;2)$ denotes the binary Grassmannian, that is, the set of all r-dimensional subspaces of $\mathbb{F}_2^m$. $\mathbb{U}(N)$ denotes the set of unitary $N \times N$ complex matrices and $\dagger$ will denote the conjugate transpose of a matrix.

II. Problem Formulation and Solution Approach

A. System Model

We consider a dense network of M single antenna low-cost sensors/users spread out in a cell covered by a base station. Each sensor becomes active randomly and sporadically, during which it transmits its *signature*, or an information carrying message, to the base station in blocks of N channel uses. We assume that the users are synchronized to the base station, and that the channels are frequency flat. The overall number of users is massive; $M \gg N$. Whenever active, user u will transmit its signature $\mathbf{s}_u \in \mathbb{C}^N$. During a given communication event, a random selection of L users is simultaneously active, with signatures or messages indexed by $u_\ell,\ \ell = 1,\ldots,L$. The base station then receives

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} c_\ell \mathbf{s}_{u_\ell}\right) + \mathbf{n}, \quad c_\ell \in \mathbb{C}, \mathbf{n} \in \mathbb{C}^N, \tag{1}$$

where c_ℓ denotes the complex channel coefficient between user u_ℓ and the base station, $\mathbf{n}$ is Additive White Gaussian Noise (AWGN) and each user obeys the power constraint $\|\mathbf{s}_u\| = 1$. Two related problems can be formulated as follows.

Problem 1: Determine the set of active users/their messages $\{u_1,\ldots,u_L\}$ given $\mathbf{s}$.

Problem 2: Design a codebook $\mathcal{C} = \{\mathbf{s}_1,\ldots,\mathbf{s}_M\} \subset \mathbb{C}^N$ that reliably solves Problem 1 with low complexity.

In simulations we assume to know the number L of active users at any given time, and the error probability of single user transmission is estimated as

$$p_u = 1 - \frac{\text{number of users decoded correctly}}{\text{total number of active users}}. \tag{2}$$

The performance of a codebook $\mathcal{C} = \{\mathbf{s}_i\}_{i=1}^M \subset \mathbb{C}^N$ is governed by the *worst-case coherence* $\mu(\mathcal{C}) = \max_{i\neq j} |\mathbf{s}_i^\dagger \mathbf{s}_j|$, or equivalently by the *minimum chordal distance* $\delta_c(\mathcal{C}) = \sqrt{1-\mu^2(\mathcal{C})}$. Thus, we are seeking for a very large number of unit vectors in $\mathbb{C}^N$ that are sufficiently separated. As the users are not phase coherent, codewords are not separated by phase, and thus we are interested in equivalence classes of unit vectors, up to $\mathbb{U}(1)$ rotations, i.e. complex projective lines in $\mathbb{CP}^{N-1}$, or equivalently, Grassmannian lines in $\mathcal{G}_{\mathbb{C}}(N,1)$. Given the very large number of total users M that we would want to support, the codebook $\mathcal{C}$ of signatures must be highly structured, so that low-complexity decoding algorithms are feasible. One such codebook, shown to be successful in theory and practice, is the codebook of Binary Chirps (BCs) [6], [21], defined as follows. Fix a natural number m and put $N = 2^m$. For a binary vector $\mathbf{b} \in \mathbb{F}_2^m$ and binary symmetric matrix $\mathbf{S} \in \mathrm{Sym}(m;2)$ define

$$\mathcal{C}^{(m)} = \{\mathbf{w}_{\mathbf{b},\mathbf{S}}\}_{\mathbf{b},\mathbf{S}}, \quad \mathbf{w}_{\mathbf{b},\mathbf{S}}(\mathbf{a}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathsf{T}}\mathbf{S}\mathbf{a}+2\mathbf{b}^{\mathsf{T}}\mathbf{a} \bmod 4}. \tag{3}$$

A time-slot $n \in \{1,\ldots,N\}$ is indexed as a binary vector $\mathbf{a}^{(n)} \in \mathbb{F}_2^m$ of length m. Thus, during time-slot n, an active user will transmit the corresponding symbol $\mathbf{w}_{\mathbf{b},\mathbf{S}}(\mathbf{a}^{(n)})$ of its signature $\mathbf{w}_{\mathbf{b},\mathbf{S}}$. To simplify the notation, we will drop the superscript. The number of signatures/codewords is

$$|\mathcal{C}^{(m)}| = 2^m \cdot 2^{m(m+1)/2} = \sqrt{N}^{3+\log_2 N}, \tag{4}$$

while the minimum chordal distance is $1/\sqrt{2}$; see (9). In [6], the authors leverage the structure of BCs to construct a low-complexity decoding algorithm. They use the so-called *shift and multiply* technique in conjunction with the Walsh-Hadamard transform.

B. Generalizing BCs to BSSCs

We aim to further leverage the structure of BCs, by extending them to a larger codebook, while preserving the main algebraic and geometric features so that a low-complexity algorithm for the extended codebook remains feasible. For this, we use the guiding principles of [10], in which an active user transmits only on $K \leq N$ time-slots. This creates an *on-off pattern* of time-slots. We assume that the on-pattern forms a binary subspace of $\mathbb{F}_2^m$ of dimension/rank $0 \leq r \leq m$, that is, an active user transmits only during time-slots indexed by a binary subspace. Given the power constrain of each user, the dimension of the on-pattern, can also be used to prioritize users based on their distance from the base station. Now, given an on-pattern, characterized by a binary subspace $H \in \mathcal{G}(m,r;2)$ of dimension r, an active user will transmit a 2^r-dimensional

binary chirp characterized by $\widetilde{\mathbf{b}} \in \mathbb{F}_2^r$, $\widetilde{\mathbf{S}} \in \mathrm{Sym}(r;2)$. This strategy creates a codebook $\mathcal{C}^{(r)} = \{\mathbf{w}_{\widetilde{\mathbf{b}},\widetilde{\mathbf{S}}}\}$ of 2^r-dimensional binary chirps to be distributed to users that, when active, transmit on time-slots indexed by H. As we will see, however, transmitting on a coset of H is just as good as transmitting on H itself. Since there are 2^{m-r} different cosets of H, we can keep track of every single option with a vector $\widehat{\mathbf{b}} \in \mathbb{F}_2^{m-r}$. This suggest to think of a vector $\mathbf{b} \in \mathbb{F}_2^m$ as $\mathbf{b} = \begin{bmatrix} \widetilde{\mathbf{b}} \\ \widehat{\mathbf{b}} \end{bmatrix} \in \mathbb{F}_2^r \times \mathbb{F}_2^{m-r}$, the first r bits of which are used to define a 2^r-dimensional binary chirp and the last $m-r$ bits of which are used to keep track of the coset of H. The concise method for keeping track of cosets will use Schubert Cells as described in Section III-A, and will be detailed in Section IV. Note that, since cosets are disjoint, so are the 2^{m-r} on-patterns determined by H.[1] Thus, combining all together, we obtain a codebook $\mathcal{C}_H^{(r)} = \{\mathbf{w}_{\mathbf{b},\widetilde{\mathbf{S}}}\}$, for which $|\mathcal{C}_H^{(r)}| = 2^m \cdot 2^{r(r+1)/2}$. The codebook of *Binary Subspace Chirps* (BSSCs) is defined as

$$\mathcal{V}_{\mathrm{BSSC}} = \bigcup_{r=0}^{m} \bigcup_{H \in \mathcal{G}(m,r;2)} \mathcal{C}_H^{(r)}. \tag{5}$$

We will have a running example that illustrates all the structural the details. But first, to compute the size of the extended codebook, we recall that the size of the binary Grassmannian is given by the 2-binomial coefficient, that is

$$|\mathcal{G}(m,r;2)| = \binom{m}{r}_2 = \prod_{i=0}^{r-1} \frac{1-2^{m-i}}{1-2^{i+1}}, \tag{6}$$

and hence, the cardinality of our extended codebook is

$$|\mathcal{V}_{\mathrm{BSSC}}| = 2^m \cdot \sum_{r=0}^{m} 2^{r(r+1)/2} \cdot \left(\prod_{i=0}^{r-1} \frac{1-2^{m-i}}{1-2^{i+1}} \right) \tag{7}$$

$$= 2^m \cdot \prod_{r=1}^{m} (2^r + 1), \tag{8}$$

where the last equality is simply the 2-binomial theorem [26].

Recall Slepian's definition of group codes [27]; a group code is a code generated as the orbit of a generating vector $\mathbf{v}$ under the action of a finite group $\mathcal{G}$; $\mathcal{C} = \{\mathbf{w} = \mathbf{G}\mathbf{v} \mid \mathbf{G} \in \mathcal{G}\}$. Group codes are efficient for constructing tight frames/Grassmannian line codebooks [28].

The main coding-related characteristics of the extended codebook $\mathcal{V}_{\mathrm{BSSC}}$ are the following.

Theorem 1: We have $\delta_c(\mathcal{V}_{\mathrm{BSSC}}) = \delta_c(\mathcal{C}^{(m)}) = 1/\sqrt{2}$ and $|\mathcal{V}_{\mathrm{BSSC}}|/|\mathcal{C}^{(m)}| \approx 2.384$. Additionally, $\mathcal{V}_{\mathrm{BSSC}}$ is a group code of the Clifford group.

Proof: Fix a binary chirp $\mathbf{w}_1 \in \mathcal{V}_{\mathrm{BC}}$ parametrized by $\mathbf{S}_1 \in \mathrm{Sym}(m;2)$, and let $\mathbf{w}_2$ range among 2^m binary chirps parametrized by $\mathbf{S}_2 \in \mathrm{Sym}(m;2)$. Then [6], [29], [30]

$$|\mathbf{w}_1^\dagger \mathbf{w}_2|^2 = \begin{cases} 1/2^r, & 2^r \text{ times}, \\ 0, & 2^m - 2^r \text{ times}, \end{cases} \tag{9}$$

where $r = \mathrm{rank}\,(\mathbf{S}_1 - \mathbf{S}_2)$. It follows immediately that $|\mathbf{w}_1^\dagger \mathbf{w}_2| \leq 1/\sqrt{2}$, and thus $\delta_c(\mathcal{C}^{(m)}) = 1/\sqrt{2}$. Next, let $\mathbf{w}_1, \mathbf{w}_2 \in \mathcal{V}_{\mathrm{BSSC}}$. By Theorem 4 we have two cases: either (1) the on-patterns don't overlap in which case we have $|\mathbf{w}_1^\dagger \mathbf{w}_2| = 0$ and $\delta_c(\mathbf{w}_1, \mathbf{w}_2) = 1$, or (2) the on-patterns overlap in which case the overlap is again a binary chirp of some lower rank. In the latter case (9) still applies and $\delta_c(\mathcal{V}_{\mathrm{BSSC}}) = 1/\sqrt{2}$ follows. The statement relating the cardinalities is a combination of (4) and (8). Finally, by Corollary 1, $\mathcal{V}_{\mathrm{BSSC}}$ is the collection of all stabilizer states, which in turn is the orbit of $\mathbf{e}_0$ under the action of the Clifford group. ∎

BSSCs thus provide an appealing example of a non-Abelian group code with a faithful representation in N dimensions. As we shall see, the group structure enables low-complexity decoding.

1) Decoding BSSCs: While Theorem 1 points out a clear coding gain, as mentioned, for our specific use-case, a low complexity decoding algorithm is of prime interest. The extension of BCs to BSSCs is done in such a way that we can still leverage the decoding algorithm of [6]. Within this extended codebook, a decoding algorithm should be able to identify/reconstruct $\mathbf{b}_u \in \mathbb{F}_2^m, \mathbf{S}_u \in \mathrm{Sym}(r,2)$, and $H_u \in \mathcal{G}(m,r;2)$ for each active user u. The heavy task of the decoding algorithm is to identify the on-off pattern characterized by H_u, which we then tune-in with the BC decoding algorithm of [6] to identify $\mathbf{b}_u$ and $\mathbf{S}_u$. The case when there is a single active user at any given time was considered in [22].

As it turns out, even though our construction is purely motivated by a communication scenario, it leads to well-known notions in quantum computing. The first tell is that BCs are exactly the so-called *graph states*. The second tell is (8), which hints strong connections with *stabilizer states*, and in fact, as we will see, BSSCs are precisely stabilizer states. Our strategy is to decode a BSSC by identifying the maximal stabilizer group that stabilizes it. For this, one will need a well-behaved one-to-one correspondence[2] between stabilizer states and maximal stabilizers *that clearly separates the "chirp part" and the "on-off pattern part"*. To establish this one-to-one correspondence we use Schubert cells and cosets of the binary symplectic group $\mathrm{Sp}(m;2)$. We leverage this connection, and its underlying binary structure, to decode a BSSC by identifying the stabilizer group that stabilizes it.

III. Preliminaries

In this section we will introduce all preliminary notions needed for navigating the connection between the $2m$ dimensional binary world and the 2^m dimensional complex world, as depicted in Figure 1. The primary bridge used here is the well-known homomorphism (71) between the Clifford and symplectic binary groups, and the Bruhat decomposition of the symplectic group. We focus on cosets of the symplectic group modulo the semidirect product $\mathrm{GL}(m;2) \rtimes \mathrm{Sym}(m;2)$. In the complex world, this semidirect product corresponds to

[1] This important feature can be further leveraged by the network. Namely, a user can receive/listen during the off-pattern, and if neighboring users are assigned to have disjoint on-patterns, this can be used for neighbour discovery [9].

[2] A stabilizer state is stabilized by several maximal stabilizer groups, but because we are interested in decoding (complexity), a well-behaved canonical form is a must. See also the discussion proceeding Theorem 3.

column permutations and column rotations. We are interested in codebooks of Grassmannian lines, and we shall construct them from columns of Clifford group elements. Column permutations and rotations thus do not change the codebook, the cosets are sufficient for constructing all unique codewords.

The cosets are characterized by a rank $r = 0, \ldots, m$ and a binary subspace $H \in \mathcal{G}(m, r; 2)$, which we will think of as the column space of an $m \times r$ binary matrix in column reduced echelon form. We will use Schubert cells as a formal and systematic approach. This also provides a framework for describing well-known facts from binary symplectic geometry (e.g., Remark 4). Finally, Subsection III-C discusses common notions from quantum computation.

A. Schubert Cells

Here we discuss the Schubert decomposition of the Grassmannian $\mathcal{G}(m, r; 2)$ with the respect to the standard *flag*

$$\{\mathbf{0}\} = V_0 \subset V_1 \subset \cdots \subset V_m, \tag{10}$$

where $V_i = \operatorname{span}\{\mathbf{e}_1, \ldots, \mathbf{e}_i\}$ and $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ is the standard basis of $\mathbb{F}_2^m$. Fix a set of r indices $\mathcal{I} = \{i_1, \ldots, i_r\} \subset \{1, \ldots, m\}$, which, without loss of generality, we assume to be in increasing order. The *Schubert cell* $\mathcal{C}_\mathcal{I}$ is the set of all $m \times r$ matrices that have 1 in *leading* positions (i_j, j), 0 on the left, right, and above each leading position, and every other entry is free. This is simply the set of all binary matrices in *column reduced echelon form* with leading positions $\mathcal{I}$. By counting the number of free entries in each column one concludes that

$$\dim \mathcal{C}_\mathcal{I} = \sum_{j=1}^{r} (m - i_j) - (r - j). \tag{11}$$

Fix $H \in \mathcal{G}(m, r; 2)$, and think of it as the column space of a $m \times r$ matrix $\mathbf{H}$. After column operations, it will belong to some cell $\mathcal{C}_\mathcal{I}$. To emphasize this fact, we will denote it as $\mathbf{H}_\mathcal{I}$.

Schubert cells have a well-known duality theory which we outline next. Let $\widetilde{\mathbf{H}_\mathcal{I}}$ be such that $(\mathbf{H}_\mathcal{I})^\mathsf{T} \widetilde{\mathbf{H}_\mathcal{I}} = 0$. Of course $\operatorname{cs}(\widetilde{\mathbf{H}_\mathcal{I}}) \in \mathcal{G}(m, m - r; 2)$. Let $\widetilde{\mathcal{I}} := \{1, \ldots, m\} \setminus \mathcal{I}$ and put $\widetilde{\mathcal{C}_\mathcal{I}} := \{\widetilde{\mathbf{H}_\mathcal{I}} \mid \mathbf{H}_\mathcal{I} \in \mathcal{C}_\mathcal{I}\}$. There is a bijection between $\{\widetilde{\mathcal{C}_\mathcal{I}}\}_{|\mathcal{I}|=r}$ and $\{\mathcal{C}_{\widetilde{\mathcal{J}}}\}_{|\mathcal{J}|=r}$, realized by reverting the rows and columns of $\widetilde{\mathbf{H}_\mathcal{I}}$ and by identifying the set $\widetilde{\mathcal{J}} = \{i_1, \ldots, i_{m-r}\}$ with its image under the mapping $\mathcal{A} \to \widehat{\mathcal{A}} = \{m + 1 - a \mid a \in \mathcal{A}\}$. With this identification, we will denote $\mathbf{H}_{\widetilde{\mathcal{I}}}$ the unique element of cell $\mathcal{C}_{\widetilde{\mathcal{I}}}$ that is equivalent with $\widetilde{\mathbf{H}_\mathcal{I}}$, obtained by reverting the rows and columns of $\widetilde{\mathbf{H}_\mathcal{I}}$:

$$\mathbf{H}_{\widetilde{\mathcal{I}}} = \mathbf{P}_{\mathrm{ad},m} \widetilde{\mathbf{H}_\mathcal{I}} \mathbf{P}_{\mathrm{ad},m-r}, \tag{12}$$

where $\mathbf{P}_{\mathrm{ad}}$ is the antidiagonal matrix in respective dimensions.

Each cell has a distinguished element: $\mathbf{I}_\mathcal{I} \in \mathcal{C}_\mathcal{I}$ will denote the identity matrix $\mathbf{I}_m$ restricted to $\mathcal{I}$, that is, the unique element in $\mathcal{C}_\mathcal{I}$ that has all the free entries 0. Note that $\mathbf{I}_\mathcal{I}$ has as jth column the i_jth column of $\mathbf{I}_m$, and thus its non-zero rows form $\mathbf{I}_r$. In particular if $|\mathcal{I}| = m$ then $\mathbf{I}_\mathcal{I} = \mathbf{I}_m$. We also have $\mathbf{I}_{\widetilde{\mathcal{I}}} \in \mathcal{C}_{\widetilde{\mathcal{I}}}$. With this notation one easily verifies that

$$(\mathbf{I}_\mathcal{I})^\mathsf{T} \mathbf{H}_\mathcal{I} = \mathbf{I}_r, \quad (\mathbf{I}_\mathcal{I})^\mathsf{T} \mathbf{I}_{\widetilde{\mathcal{I}}} = 0, \quad (\widetilde{\mathbf{H}_\mathcal{I}})^\mathsf{T} \mathbf{I}_{\widetilde{\mathcal{I}}} = \mathbf{I}_{m-r}. \tag{13}$$

In addition, $\mathbf{H}_\mathcal{I}$ can be completed to an invertible matrix

$$\mathbf{P}_\mathcal{I} := \begin{bmatrix} \mathbf{H}_\mathcal{I} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix} \in \mathrm{GL}(m; 2). \tag{14}$$

Note that when $\mathbf{I}_\mathcal{I}$ is completed to an invertible matrix it gives rise to a permutation matrix. Next, (13) along with the default equality $(\mathbf{H}_\mathcal{I})^\mathsf{T} \widetilde{\mathbf{H}_\mathcal{I}} = 0$ implies that

$$\mathbf{P}_\mathcal{I}^{-\mathsf{T}} = \begin{bmatrix} \mathbf{I}_\mathcal{I} & \widetilde{\mathbf{H}_\mathcal{I}} \end{bmatrix}. \tag{15}$$

Let us describe this framework with an example.

Example 1: Let $m = 3$ and $r = 2$. Then

$$\mathcal{C}_{\{1,2\}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ u & v \end{bmatrix}, \quad \widetilde{\mathcal{C}_{\{1,2\}}} = \begin{bmatrix} u \\ v \\ 1 \end{bmatrix}, \quad \mathcal{C}_{\widehat{\{3\}}} \cong \mathcal{C}_{\{1\}} = \begin{bmatrix} 1 \\ v \\ u \end{bmatrix},$$

$$\mathcal{C}_{\{1,3\}} = \begin{bmatrix} 1 & 0 \\ u & 0 \\ 0 & 1 \end{bmatrix}, \quad \widetilde{\mathcal{C}_{\{1,3\}}} = \begin{bmatrix} u \\ 1 \\ 0 \end{bmatrix}, \quad \mathcal{C}_{\widehat{\{2\}}} \cong \mathcal{C}_{\{2\}} = \begin{bmatrix} 0 \\ 1 \\ u \end{bmatrix},$$

$$\mathcal{C}_{\{2,3\}} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \widetilde{\mathcal{C}_{\{2,3\}}} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathcal{C}_{\widehat{\{1\}}} \cong \mathcal{C}_{\{3\}} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Let us spell out $\mathcal{I} = \{1, 3\}$ in detail. The set $\mathcal{C}_\mathcal{I}$ is constructed directly by definition, that is, in column reduced echelon form with leading positions 1 and 3, while $\widetilde{\mathcal{C}_\mathcal{I}}$ is constructed so that $(\mathbf{H}_\mathcal{I})^\mathsf{T} \widetilde{\mathbf{H}_\mathcal{I}} = 0$. Then we revert the rows and columns (only rows in this case) to obtain the last object where we identify[3] $\{2\} = \widetilde{\{1, 3\}}$ with $\widehat{\{2\}} \equiv \{2\}$.

In this case, as we see from above, there is only one free bit. This yields two subspaces/matrices $\mathbf{H}_\mathcal{I}$, which when completed to an invertible matrix as in (14) yield

$$\mathbf{P}_{u=0} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{P}_{u=1} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{16}$$

Then one directly computes

$$\mathbf{P}_{u=0}^{-\mathsf{T}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{P}_{u=1}^{-\mathsf{T}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{17}$$

Compare (17) with (15); the first two columns are obviously $\mathbf{I}_\mathcal{I}$, whereas the last column is precisely $\mathcal{C}_{\widehat{\{2\}}} \equiv \mathcal{C}_{\{2\}}$ with rows reverted. Note here that when *all* the free bits are zero then the resulting $\mathbf{P}$ is simply a permutation matrix, and in this case $\mathbf{P}^{-\mathsf{T}} = \mathbf{P}$.

B. Bruhat Decomposition of the Symplectic Group

We first briefly describe the symplectic structure of $\mathbb{F}_2^{2m}$ via the symplectic bilinear form

$$\langle \mathbf{a}, \mathbf{b} \mid \mathbf{c}, \mathbf{d} \rangle_\mathrm{s} := \mathbf{b}^\mathsf{T} \mathbf{c} + \mathbf{a}^\mathsf{T} \mathbf{d}. \tag{18}$$

One is naturally interested in automorphisms that preserve such symplectic structure. It follows directly by the definition that a $2m \times 2m$ matrix $\mathbf{F}$ preserves $\langle \bullet \mid \bullet \rangle_\mathrm{s}$ iff $\mathbf{F} \boldsymbol{\Omega} \mathbf{F}^\mathsf{T} = \boldsymbol{\Omega}$ where

$$\boldsymbol{\Omega} = \begin{bmatrix} \mathbf{0}_m & \mathbf{I}_m \\ \mathbf{I}_m & \mathbf{0}_m \end{bmatrix}. \tag{19}$$

[3]In this specific case there is no need for identification, but this is only a coincidence. For different choices of $\mathcal{I}$ one needs a true identification.

We will denote the group of all such *symplectic matrices* $\mathbf{F}$ with $\mathrm{Sp}(2m;2)$. Equivalently,

$$\mathbf{F}=\begin{bmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{C} & \mathbf{D}\end{bmatrix}\in \mathrm{Sp}(2m;2) \tag{20}$$

iff $\mathbf{AB}^{\mathsf{T}},\mathbf{CD}^{\mathsf{T}}\in \mathrm{Sym}(m;2)$ and $\mathbf{AD}^{\mathsf{T}}+\mathbf{BC}^{\mathsf{T}}=\mathbf{I}_m$. It is well-known that

$$|\mathrm{Sp}(2m;2)|=2^{m^2}\prod_{i=1}^{m}(4^i-1). \tag{21}$$

Consider the row space $H:=\mathrm{rs}\,[\mathbf{A}\ \ \mathbf{B}]$ of the $m\times 2m$ upper half of a symplectic matrix $\mathbf{F}\in\mathrm{Sp}(2m;2)$. Because $\mathbf{AB}^{\mathsf{T}}$ is symmetric one has $[\mathbf{A}\ \ \mathbf{B}]\mathbf{\Omega}[\mathbf{A}\ \mathbf{B}]^{\mathsf{T}}=\mathbf{0}$ and thus $\langle\,\mathbf{x}\,|\,\mathbf{y}\,\rangle_{\mathrm{s}}=0$ for all $\mathbf{x},\mathbf{y}\in H$. We will denote $(\,\bullet\,)^{\perp_{\mathrm{s}}}$ the dual with respect to the symplectic inner product (18). It follows that $H\subseteq H^{\perp}$, that is, H is self-orthogonal or *totally isotropic*. Moreover, H is *maximal* totally isotropic because $\dim H=m$ and thus $H=H^{\perp}$. The set of all self-dual/maximal totally isotropic subspaces is commonly referred as the *Lagrangian Grassmannian* $\mathcal{L}(2m,m;2)\subset\mathcal{G}(2m,m;2)$. It is well-known that

$$|\mathcal{L}(2m,m)|=\prod_{i=1}^{m}(2^i+1). \tag{22}$$

For reasons that will become clear latter on we are interested in decomposing symplectic matrices into more elementary symplectic matrices, and we will do this via the *Bruhat decomposition* of $\mathrm{Sp}(2m;2)$. While the decomposition holds in a general group-theoretic setting [31], here we give a rather elementary approach; see also [32]. We start the decomposition by writing

$$\mathrm{Sp}(2m;2)=\bigcup_{r=0}^{m}\mathcal{C}_r, \tag{23}$$

where

$$\mathcal{C}_r=\left\{\mathbf{F}=\begin{bmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{C} & \mathbf{D}\end{bmatrix}\in\mathrm{Sp}(2m;2)\;\middle|\;\mathrm{rank}\,\mathbf{C}=r\right\}. \tag{24}$$

In $\mathrm{Sp}(2m;2)$ there are two distinguished subgroups:

$$S_D:=\left\{\mathbf{F}_D(\mathbf{P})=\begin{bmatrix}\mathbf{P} & \mathbf{0}\\ \mathbf{0} & \mathbf{P}^{-\mathsf{T}}\end{bmatrix}\;\middle|\;\mathbf{P}\in\mathrm{GL}(m;2)\right\}, \tag{25}$$

$$S_U:=\left\{\mathbf{F}_U(\mathbf{S})=\begin{bmatrix}\mathbf{I} & \mathbf{S}\\ \mathbf{0} & \mathbf{I}\end{bmatrix}\;\middle|\;\mathbf{S}\in\mathrm{Sym}(m;2)\right\}. \tag{26}$$

Let $\mathcal{P}$ be the semidirect product of S_D and S_U, that is,

$$\mathcal{P}=\{\mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})\mid\mathbf{P}\in\mathrm{GL}(m;2),\mathbf{S}\in\mathrm{Sym}(m;2)\}. \tag{27}$$

Note that the order of the multiplication doesn't matter since the semidirect product satisfies

$$\mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})=\mathbf{F}_U(\mathbf{PSP}^{\mathsf{T}})\mathbf{F}_D(\mathbf{P}), \tag{28}$$

and $\mathbf{PSP}^{\mathsf{T}}$ is again symmetric. It is straightforward to verify that $\mathcal{P}=\mathcal{C}_0$, and that in general

$$\mathcal{C}_r=\{\mathbf{F}_1\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_2\mid\mathbf{F}_1,\mathbf{F}_2\in\mathcal{P}\}, \tag{29}$$

where

$$\mathbf{F}_{\mathbf{\Omega}}(r)=\begin{bmatrix}\mathbf{I}_{m|-r} & \mathbf{I}_{m|r}\\ \mathbf{I}_{m|r} & \mathbf{I}_{m|-r}\end{bmatrix}, \tag{30}$$

with $\mathbf{I}_{m|r}$ being the block matrix with $\mathbf{I}_r$ in upper left corner and 0 else and $\mathbf{I}_{m|-r}=\mathbf{I}_m-\mathbf{I}_{m|r}$. Note here that $\mathbf{\Omega}=\mathbf{F}_{\mathbf{\Omega}}(m)$ and $\mathbf{\Omega}\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{\Omega}=\mathbf{F}_{\mathbf{\Omega}}(m-r)$. Then it follows by (29) (and by (28)) that every $\mathbf{F}\in\mathrm{Sp}(2m;2)$ can be written as

$$\mathbf{F}=\mathbf{F}_D(\mathbf{P}_1)\mathbf{F}_U(\mathbf{S}_1)\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\mathbf{S}_2)\mathbf{F}_D(\mathbf{P}_2). \tag{31}$$

The above constitutes the Bruhat decomposition of a symplectic matrix; see also [1], [33].

Remark 1: It was shown in [34] that a symplectic matrix $\mathbf{F}$ can be decomposed as

$$\mathbf{F}=\mathbf{F}_D(\mathbf{P}_1)\mathbf{F}_U^{\mathsf{T}}(\mathbf{S}_1)\mathbf{\Omega}\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\mathbf{S}_2)\mathbf{F}_D(\mathbf{P}_2). \tag{32}$$

If we, instead, decompose $\mathbf{\Omega}\mathbf{F}$ as in (32) and insert $\mathbf{\Omega}^2=\mathbf{I}_{2m}$ between $\mathbf{F}_D(\mathbf{P}_1)$ and $\mathbf{F}_U^{\mathsf{T}}(\mathbf{S}_1)$, we see that (32) is reduced to (31). This reduction from a seven-component decomposition to a five-component decomposition is beneficial in quantum circuits design [33], [35].

In what follows we will focus on the right action of $\mathcal{P}$ on $\mathrm{Sp}(2m;2)$, that is, the right cosets in the quotient group $\mathrm{Sp}(2m;2)/\mathcal{P}$. It is an immediate consequence of (31) and (28) that a coset representative will look like

$$\mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})\mathbf{F}_{\mathbf{\Omega}}(r), \tag{33}$$

for some rank r, invertible $\mathbf{P}$, and symmetric $\mathbf{S}$. However, two different invertibles $\mathbf{P}$ may yield representatives of the same coset. We make this precise below.

Lemma 1: A right coset in $\mathrm{Sp}(2m;2)/\mathcal{P}$ is uniquely characterized by a rank r, an $r\times r$ symmetric matrix $\mathbf{S}_r\in\mathrm{Sym}(r)$, and a r-dimensional subspace H in $\mathbb{F}_2^m$.

Proof: Write a coset representative $\mathbf{F}$ as in (33). This immediately determines r. Next, write $\mathbf{S}$ in a block form

$$\mathbf{S}=\begin{bmatrix}\mathbf{S}_r & \mathbf{X}\\ \mathbf{X}^{\mathsf{T}} & \mathbf{S}_{m-r}\end{bmatrix}, \tag{34}$$

where $\mathbf{S}_r,\mathbf{S}_{m-r}$ are symmetric. Denote $\widetilde{\mathbf{S}_r},\widehat{\mathbf{S}}_{m-r}\in\mathrm{Sym}(m;2)$ the matrices that have $\mathbf{S}_r$ and $\mathbf{S}_{m-r}$ in upper left and lower right corner respectively and 0 otherwise. Put also

$$\widetilde{\mathbf{X}}=\begin{bmatrix}\mathbf{I}_r & \mathbf{0}\\ \mathbf{X}^{\mathsf{T}} & \mathbf{I}_{m-r}\end{bmatrix}. \tag{35}$$

With this notation we have

$$\mathbf{F}_U(\mathbf{S})\mathbf{F}_{\mathbf{\Omega}}(r)=\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\widehat{\mathbf{S}}_{m-r})\mathbf{F}_D(\widetilde{\mathbf{X}}). \tag{36}$$

In other words $\mathbf{F}_U(\mathbf{S})\mathbf{F}_{\mathbf{\Omega}}(r)$ and $\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_{\mathbf{\Omega}}(r)$ belong to the same coset. Now consider an invertible

$$\widetilde{\mathbf{P}}=\begin{bmatrix}\mathbf{P}_r & \mathbf{0}\\ \mathbf{0} & \mathbf{P}_{m-r}\end{bmatrix}. \tag{37}$$

It is also straightforward to verify that

$$\begin{aligned}\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_D(\widetilde{\mathbf{P}})&=\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_D(\widehat{\mathbf{P}})\mathbf{F}_{\mathbf{\Omega}}(r)\\&=\mathbf{F}_D(\widehat{\mathbf{P}})\mathbf{F}_U(\widehat{\mathbf{P}}^{-1}\widetilde{\mathbf{S}_r}\widehat{\mathbf{P}}^{-\mathsf{T}})\mathbf{F}_{\mathbf{\Omega}}(r),\end{aligned}$$

where

$$\widehat{\mathbf{P}}=\begin{bmatrix}\mathbf{P}_r^{-\mathsf{T}} & \mathbf{0}\\ \mathbf{0} & \mathbf{P}_{m-r}\end{bmatrix}, \tag{38}$$

and the second equality follows by (28). Thus $\mathbf{F}_D(\mathbf{P}_1)\mathbf{F}_U(\mathbf{S}_1)\mathbf{F}_{\mathbf{\Omega}}(r)$, where

$$\mathbf{P}_1 := \mathbf{P}\widehat{\mathbf{P}},\ \mathbf{S}_1 := \widehat{\mathbf{P}}^{-1}\widetilde{\mathbf{S}_r}\widehat{\mathbf{P}}^{-\mathsf{T}} \tag{39}$$

represents the same coset. Note that the transformation (39) doesn't change the column space $\mathbf{C}$ (that is, the lower left corner of $\mathbf{F}$), which is an r-dimensional subspace in $\mathbb{F}_2^m$. ■

Next, using Schubert we cells will choose a canonical coset representative. We will use the same notation as in the above lemma. Let r and $\widetilde{\mathbf{S}_r}$ be as above. To choose $\mathbf{P}$, think of the r-dimensional subspace H from the above lemma as the column space of a matrix $\mathbf{H}$, which belongs to some Schubert cell $\mathcal{C}_{\mathcal{I}}$. We will use the coset representative

$$\mathbf{F}_O(\mathbf{P}_{\mathcal{I}}, \mathbf{S}_r) := \mathbf{F}_D(\mathbf{P}_{\mathcal{I}})\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_{\mathbf{\Omega}}(r), \tag{40}$$

where $\mathbf{P}_{\mathcal{I}}$ is as in (14).

Let $\mathbf{F} \in \mathrm{Sp}(2m;2)$ be in block from as in (20), and assume it is written as

$$\mathbf{F} = \mathbf{F}_D(\mathbf{P}^{-\mathsf{T}})\mathbf{F}_U(\widetilde{\mathbf{S}_r})\mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_D(\mathbf{M})\mathbf{F}_U(\mathbf{S}). \tag{41}$$

Multiplying both sides of (41) on the left with $\mathbf{F}_D(\mathbf{P}^{\mathsf{T}})$ and on the right with $\mathbf{F}_U(\mathbf{S})$, and then comparing respective blocks we obtain

$$\mathbf{P}^{\mathsf{T}}\mathbf{A} = (\widetilde{\mathbf{S}_r} + \mathbf{I}_{m|-r})\mathbf{M}, \tag{42}$$

$$\mathbf{P}^{\mathsf{T}}\mathbf{A}\mathbf{S} = \mathbf{P}^{\mathsf{T}}\mathbf{B} + \mathbf{I}_{m|r}\mathbf{M}^{-\mathsf{T}}, \tag{43}$$

$$\mathbf{P}^{-1}\mathbf{C} = \mathbf{I}_{m|r}\mathbf{M}, \tag{44}$$

$$\mathbf{P}^{-1}\mathbf{C}\mathbf{S} = \mathbf{P}^{-1}\mathbf{D} + \mathbf{I}_{m|-r}\mathbf{M}^{-\mathsf{T}}, \tag{45}$$

which we can solve for $\mathbf{M}, \widetilde{\mathbf{S}_r}$ and $\mathbf{S}$, while assuming that we know $\mathbf{F}$ (and implicitly $\mathbf{P}$ which can be determined by the column space of the lower-left block of $\mathbf{F}$). First we find $\mathbf{M}$. For this, recall that $\widetilde{\mathbf{S}_r}$ has nonzero entries only on the upper left $r\times r$ block. Thus, it follows by (42) that the last $m-r$ rows of $\mathbf{M}$ coincide with the last $m-r$ rows of $\mathbf{P}^{\mathsf{T}}\mathbf{A}$. Similarly, it follows from (44) that the first r rows of $\mathbf{M}$ coincide with the first r rows of $\mathbf{P}^{-1}\mathbf{C}$. With $\mathbf{M}$ in hand we have

$$\widetilde{\mathbf{S}_r} = \mathbf{P}^{\mathsf{T}}\mathbf{A}\mathbf{M}^{-1} + \mathbf{I}_{m|-r}. \tag{46}$$

By using (44) in (45) we see that the first r rows of $\mathbf{MS}$ coincide with first r rows of $\mathbf{P}^{-1}\mathbf{CS}$. Similarly, by using (42) in (43), we see that the last $m-r$ rows of $\mathbf{MS}$ coincide with the last $m-r$ rows of $\mathbf{P}^{\mathsf{T}}\mathbf{AS}$. Multiplication with $\mathbf{M}^{-1}$ yields $\mathbf{S}$. We collect everything in Algorithm 1, which gives not only the Bruhat decomposition but also a canonical coset representative.

We end this section with a few remarks.

Remark 2: One can follow an analogous path by considering left action of $\mathcal{P}$ on $\mathrm{Sp}(2m;2)$. This follows most directly by the observation that if $\mathbf{F} = \mathbf{F}_D(\mathbf{P})\mathbf{F}_U(\mathbf{S})\mathbf{F}_{\mathbf{\Omega}}(r)$ is a right coset representative then $\mathbf{F}^{-1} = \mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\mathbf{S})\mathbf{F}_D(\mathbf{P}^{-1})$ is a left coset representative.

Remark 3: Note that for the extremal case $r = m$, a coset representative as in (40) is completely determined by a symmetric matrix $\mathbf{S} \in \mathrm{Sym}(m;2)$, since in this case, as one would recall, $\mathbf{P}_{\mathcal{I}} = \mathbf{I}_{\mathcal{I}} = \mathbf{I}_m$.

Algorithm 1 Bruhat Decomposition of Symplectic Matrix

Input: A symplectic matrix $\mathbf{F}$.

1. Block decompose $\mathbf{F}$ to $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$ as in (20).
2. $r = \mathrm{rank}\,(\mathbf{C})$.
3. Find $\mathbf{P}$ as in (14) from $\mathrm{cs}\,(\mathbf{C})$.
4. $\mathbf{M}_{\mathrm{up}}$ is the first r rows of $\mathbf{P}^{-1}\mathbf{C}$.
5. $\mathbf{M}_{\mathrm{lo}}$ is the last $m-r$ rows of $\mathbf{P}^{\mathsf{T}}\mathbf{A}$.
6. $\mathbf{M} = \begin{bmatrix}\mathbf{M}_{\mathrm{up}} \\ \mathbf{M}_{\mathrm{lo}}\end{bmatrix}$.
7. $\widetilde{\mathbf{S}_r} = \mathbf{P}^{\mathsf{T}}\mathbf{A}\mathbf{M}^{-1} + \mathbf{I}_{m|-r}$.
8. $\mathbf{S}_r$ is the upper left $r \times r$ block of $\widetilde{\mathbf{S}_r}$.
9. $\mathbf{N}_{\mathrm{up}}$ is the first r rows of $\mathbf{P}^{-1}\mathbf{D} + \mathbf{I}_{m|-r}\mathbf{M}^{-\mathsf{T}}$.
10. $\mathbf{N}_{\mathrm{lo}}$ is the last $m-r$ rows of $\mathbf{P}^{\mathsf{T}}\mathbf{B} - \mathbf{I}_{m|r}\mathbf{M}^{-\mathsf{T}}$.
11. $\mathbf{S} = \mathbf{M}^{-1}\begin{bmatrix}\mathbf{N}_{\mathrm{up}} \\ \mathbf{N}_{\mathrm{lo}}\end{bmatrix}$.

Output: $r, \mathbf{P}, \mathbf{S}_r, \mathbf{M}, \mathbf{S}$

Remark 4: Directly from the definition we have

$$|\mathcal{P}| = |\mathrm{GL}(m;2)| \cdot |\mathrm{Sym}(m;2)| = 2^{m^2}\prod_{i=1}^{m}(2^i - 1), \tag{47}$$

which combined with (21) yields

$$|\mathrm{Sp}(2m;2)/\mathcal{P}| = \prod_{i=1}^{m}(2^i + 1) = |\mathcal{L}(2m,m)|. \tag{48}$$

The above is of course not a coincidence. Indeed, $\mathrm{Sp}(2m;2)$ acts transitively from the right on $\mathcal{L}(2m,m)$. Next, consider $\mathrm{rs}\begin{bmatrix}\mathbf{0}_m & \mathbf{I}_m\end{bmatrix} \in \mathcal{L}(2m,m)$. If a symplectic matrix $\mathbf{F}$ as in (20) fixes this space, then $\mathbf{C} = \mathbf{0}$ and $\mathbf{A}$ is invertible. Additionally, because $\mathbf{F}$ is symplectic to start with, we obtain $\mathbf{D} = \mathbf{A}^{-\mathsf{T}}$ and $\mathbf{A}\mathbf{B}^{\mathsf{T}} =: \mathbf{S}$ is symmetric. Thus $\mathbf{B} = \mathbf{S}\mathbf{A}^{\mathsf{T}}$, and $\mathbf{F} \in \mathcal{P}$. That is, $\mathcal{P}$ is the stabilizer (in a group action terminology) of $\mathrm{rs}\begin{bmatrix}\mathbf{0}_m & \mathbf{I}_m\end{bmatrix} \in \mathcal{L}(2m,m)$. The mapping $\mathrm{Sp}(2m;2)/\mathcal{P} \longrightarrow \mathcal{L}(2m,m)$, given by

$$\mathbf{F}_O(\mathbf{P}_{\mathcal{I}}, \mathbf{S}_r) \longmapsto \mathrm{rs}\begin{bmatrix}\mathbf{I}_{m|r}\mathbf{P}_{\mathcal{I}}{}^{\mathsf{T}} & (\mathbf{I}_{m|r}\widetilde{\mathbf{S}_r} + \mathbf{I}_{m|-r})\mathbf{P}_{\mathcal{I}}^{-1}\end{bmatrix} \tag{49}$$

is well-defined. This follows by the fact that the upper half of a symplectic matrix is maximal isotropic. It is also injective, and thus bijective due to cardinality reasons. Of course one can have many bijections but we choose this one due to Theorem 3.

C. The Heisenberg-Weyl Group

Fix $N = 2^m$, and let $\{\mathbf{e}_0, \mathbf{e}_1\}$ be the standard basis of $\mathbb{C}^2$, which is commonly referred as the *computational basis*. For $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{F}_2^m$ set $\mathbf{e}_{\mathbf{v}} := \mathbf{e}_{v_1} \otimes \cdots \otimes \mathbf{e}_{v_m}$. Then $\{\mathbf{e}_{\mathbf{v}} \mid \mathbf{v} \in \mathbb{F}_2^m\}$ is the standard basis of $\mathbb{C}^N \cong (\mathbb{C}^2)^{\otimes m}$. The *Pauli matrices* are

$$\mathbf{I}_2,\ \sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\ \sigma_y = i\sigma_x\sigma_z. \tag{50}$$

For $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$ put

$$\mathbf{D}(\mathbf{a}, \mathbf{b}) := \sigma_x^{a_1}\sigma_z^{b_1} \otimes \cdots \otimes \sigma_x^{a_m}\sigma_z^{b_m}. \tag{51}$$

Directly by definition we have

$$\mathbf{D}(\mathbf{a},\mathbf{0})\mathbf{e}_{\mathbf{v}} = \mathbf{e}_{\mathbf{v}+\mathbf{a}} \text{ and } \mathbf{D}(\mathbf{0},\mathbf{b})\mathbf{e}_{\mathbf{v}} = (-1)^{\mathbf{b}^{\mathsf{T}}\mathbf{v}}\mathbf{e}_{\mathbf{v}}, \tag{52}$$

and thus, the former is a permutation matrix whereas the latter is a diagonal matrix. Then

$$\mathbf{D}(\mathbf{a},\mathbf{b})\mathbf{D}(\mathbf{c},\mathbf{d}) = (-1)^{\mathbf{b}^{\mathsf{T}}\mathbf{c}}\mathbf{D}(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}). \tag{53}$$

Thanks to (53) we have

$$\mathbf{D}(\mathbf{a},\mathbf{b})\mathbf{D}(\mathbf{c},\mathbf{d}) = (-1)^{\mathbf{b}^{\mathsf{T}}\mathbf{c}+\mathbf{a}^{\mathsf{T}}\mathbf{d}}\mathbf{D}(\mathbf{c},\mathbf{d})\mathbf{D}(\mathbf{a},\mathbf{b}). \tag{54}$$

In turn, $\mathbf{D}(\mathbf{a},\mathbf{b})$ and $\mathbf{D}(\mathbf{c},\mathbf{d})$ commute iff

$$\langle\, \mathbf{a},\mathbf{b} \,|\, \mathbf{c},\mathbf{d} \,\rangle_{\mathrm{s}} := \mathbf{b}^{\mathsf{T}}\mathbf{c} + \mathbf{a}^{\mathsf{T}}\mathbf{d} = 0, \tag{55}$$

that is, iff $(\mathbf{a},\mathbf{b})$ and $(\mathbf{c},\mathbf{d})$ are orthogonal with respect to the symplectic inner product (18). Also thanks to (53), the set

$$\mathcal{HW}_N := \{i^k\mathbf{D}(\mathbf{a},\mathbf{b}) \mid \mathbf{a},\mathbf{b} \in \mathbb{F}_2^m, k = 0,1,2,3\} \tag{56}$$

is a subgroup of $\mathbb{U}(N)$ and is called the *Heisenberg-Weyl* group. We will also call its elements Pauli matrices as well. Directly from the definition, we have a surjective homomorphism of groups

$$\Psi_N : \mathcal{HW}_N \longrightarrow \mathbb{F}_2^{2m},\ i^k\mathbf{D}(\mathbf{a},\mathbf{b}) \longmapsto (\mathbf{a},\mathbf{b}). \tag{57}$$

Its kernel is $\ker\Psi_N = \{\pm\mathbf{I}_N, \pm i\mathbf{I}_N\} \cong \mathbb{Z}_4$. We will denote $\mathcal{HW}_N^* := \mathcal{HW}_N/\ker\Psi_N$ the *projective* Heisenberg-Weyl group, and the induced isomorphism Ψ_N^*.

Note that $\langle\, \bullet \mid \bullet \,\rangle_{\mathrm{s}}$ defines a nondegenerate bilinear form in $\mathbb{F}_2^{2m}$ that translates commutativity in $\mathcal{HW}_N$ to orthogonality in $\mathbb{F}_2^{2m}$. A commutative subgroup $\mathcal{S} \subset \mathcal{HW}_N$ is called a *stabilizer group* if $-\mathbf{I}_N \notin \mathcal{S}$. Thus, for a stabilizer $\mathcal{S}$, thanks to (55) we have $\Psi_N(\mathcal{S}) \subseteq \Psi_N(\mathcal{S})^{\perp_{\mathrm{s}}}$ [36], [37]. In addition, because Ψ_N restricted to a stabilizer is an isomorphism, we have that $|\mathcal{S}| = 2^r$ iff $\dim\Psi_N(\mathcal{S}) = r$. We will think of $\Psi_N(\mathcal{S})$ as the row space of a full rank matrix $[\mathbf{A}\ \ \mathbf{B}]$ where both $\mathbf{A}$ and $\mathbf{B}$ are $r \times m$ binary matrices. We will write

$$\mathbf{E}(\mathbf{A},\,\mathbf{B}) := \{\mathbf{E}(\mathbf{x}^{\mathsf{T}}\mathbf{A},\,\mathbf{x}^{\mathsf{T}}\mathbf{B}) \mid \mathbf{x} \in \mathbb{F}_2^r\}, \tag{58}$$

where $\mathbf{E}(\mathbf{a},\,\mathbf{b}) := i^{\mathbf{a}^{\mathsf{T}}\mathbf{b}}\mathbf{D}(\mathbf{a},\mathbf{b})$. Combining this with (52) and (53) we obtain

$$\mathbf{E}(\mathbf{a},\mathbf{b}) = i^{\mathbf{a}^{\mathsf{T}}\mathbf{b}} \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{b}^{\mathsf{T}}\mathbf{v}}\mathbf{e}_{\mathbf{v}+\mathbf{a}}\mathbf{e}_{\mathbf{v}}^{\mathsf{T}}. \tag{59}$$

Next, if $\mathrm{rs}\,[\mathbf{A}\ \ \mathbf{B}]$ is self-orthogonal in $\mathbb{F}_2^{2m}$ then $\mathbf{E}(\mathbf{A},\,\mathbf{B})$ is a stabilizer. Moreover, $\Psi_N(\mathbf{E}(\mathbf{A},\,\mathbf{B})) = \mathrm{rs}\,[\mathbf{A}\ \ \mathbf{B}]$, which yields a one-to-one correspondence between stabilizers in $\mathcal{HW}_N$ and self-orthogonal subspaces in $\mathbb{F}_2^{2m}$. It also follows that a maximal stabilizer must have 2^m elements. Thus there is a one-to-one correspondence between maximal stabilizers and Lagrangian Grassmannians $\mathcal{L}(2m,m) \subset \mathcal{G}(2m,m)$. Of particular interest are maximal stabilizers

$$\mathcal{X}_N := \mathbf{E}(\mathbf{I}_m,\mathbf{0}_m) = \{\mathbf{E}(\mathbf{a},\mathbf{0}) \mid \mathbf{a} \in \mathbb{F}_2^m\}, \tag{60}$$

$$\mathcal{Z}_N := \mathbf{E}(\mathbf{0}_m,\mathbf{I}_m) = \{\mathbf{E}(\mathbf{0},\mathbf{b}) \mid \mathbf{b} \in \mathbb{F}_2^m\}, \tag{61}$$

which we naturally identify with $X_N := \Psi_N(\mathcal{X}_N) = \mathrm{rs}\,[\mathbf{I}_m\ \ \mathbf{0}_m]$ and $Z_N := \Psi_N(\mathcal{Z}_N) = \mathrm{rs}\,[\mathbf{0}_m\ \ \mathbf{I}_m]$.

What follows holds in general for any stabilizer, but for our purposes, we need only focus on the maximal ones. Let $\mathcal{S} = \mathbf{E}(\mathbf{A},\,\mathbf{B}) \subset \mathcal{HW}_N$ be a maximal stabilizer and let $\{\mathbf{E}_1,\ldots,\mathbf{E}_m\}$ be an independent generating set of $\mathcal{S}$ (that is, $\mathrm{span}\{\Psi_N(\mathbf{E}_1),\ldots,\Psi_N(\mathbf{E}_m)\} = \Psi_N(\mathcal{S})$). Consider the complex vector space [38]

$$V(\mathcal{S}) := \{\mathbf{v} \in \mathbb{C}^N \mid \mathbf{E}_i\mathbf{v} = \mathbf{v}, i = 1,\ldots,m\}. \tag{62}$$

It is well-known (see, e.g., [39]) that $\dim V(\mathcal{S}) = 2^m/|\mathcal{S}| = 1$. A unit norm vector that generates it is called *stabilizer state*, and with a slight abuse of notation is also denoted by $V(\mathcal{S})$. Because we are disregarding scalars, it is beneficial to think of a stabilizer state as *Grassmannian line*, that is, $V(\mathcal{S}) \in \mathcal{G}(\mathbb{C}^N,1)$. Next,

$$\Pi_{\mathcal{S}} := \prod_{i=1}^{m} \frac{\mathbf{I}_N + \mathbf{E}_i}{2} = \frac{1}{N}\sum_{\mathbf{E}\in\mathcal{S}} \mathbf{E} \tag{63}$$

is a projection onto $V(\mathcal{S})$.

Given a stabilizer as above, for any $\mathbf{d} \in \mathbb{F}_2^m$, $\{(-1)^{d_1}\mathbf{E}_1,\ldots,(-1)^{d_m}\mathbf{E}_m\}$ also describes a stabilizer $\mathcal{S}_{\mathbf{d}}$. Similarly to (63) put

$$\begin{aligned}\Pi_{\mathcal{S}_{\mathbf{d}}} :=& \prod_{i=1}^{m} \frac{\mathbf{I}_N + (-1)^{d_i}\mathbf{E}_i}{2} \\ =& \frac{1}{N}\sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{\mathbf{d}^{\mathsf{T}}\mathbf{x}}\mathbf{E}(\mathbf{x}^{\mathsf{T}}\mathbf{A},\,\mathbf{x}^{\mathsf{T}}\mathbf{B}).\end{aligned} \tag{64}$$

It is readily verified that $\{\Pi_{\mathcal{S}_{\mathbf{d}}} \mid \mathbf{d} \in \mathbb{F}_2^m\}$ are pair-wise orthogonal, and a stabilizer group determines a resolution of the identity

$$\mathbf{I}_N = \sum_{\mathbf{d}\in\mathbb{F}_2^m} \Pi_{\mathcal{S}_{\mathbf{d}}}. \tag{65}$$

Thus every such projection determines a one-dimensional subspace which with another abuse of notation (see also Remark 5 below) we call a stabilizer state.

Remark 5: A stabilizer state as in (62) is the unit norm vector that is fixed by the stabilizer. Now for every $\mathbf{E} \in \mathcal{S} = \mathbf{E}(\mathbf{A},\,\mathbf{B})$ there exists a unique $\mathbf{x} \in \mathbb{F}_2^m$ such that $\mathbf{E} = \mathbf{E}(\mathbf{x}^{\mathsf{T}}\mathbf{A},\,\mathbf{x}^{\mathsf{T}}\mathbf{B})$. For $\mathbf{d} \in \mathbb{F}_2^m$, consider the map $\chi_{\mathbf{d}} : \mathbf{E}(\mathbf{x}^{\mathsf{T}}\mathbf{A},\,\mathbf{x}^{\mathsf{T}}\mathbf{B}) \longmapsto (-1)^{\mathbf{d}^{\mathsf{T}}\mathbf{x}}$. Then $\Pi_{\mathcal{S}_{\mathbf{d}}}$ projects onto

$$V(\mathcal{S}_{\mathbf{d}}) := \{\mathbf{v} \in \mathbb{C}^N \mid \mathbf{E}\mathbf{v} = \chi_{\mathbf{d}}(\mathbf{E})\mathbf{v} \text{ for all } \mathbf{E} \in \mathcal{S}_{\mathbf{d}}\}, \tag{66}$$

that is, the state that under the action of $\mathbf{E}$ is scaled by $\chi_{\mathbf{d}}(\mathbf{E})$. Then of course $V(\mathcal{S}_{\mathbf{0}}) = V(\mathcal{S})$ where $\mathbf{0} \in \mathbb{F}_2^m$. In addition, the map $\chi_{\mathbf{d}}$ is a linear character of $\mathcal{S}$, which has led to non-binary quantum stabilizer codes [40].

Remark 6: Let $\{\mathbf{E}_1,\ldots,\mathbf{E}_m\}$ be an independent generating set of a maximal stabilizer $\mathcal{S}$ and consider $\mathcal{S}_{\mathbf{d}}$. By [39, Prop. 10.4] it follows that for each $i = 1,\ldots,m$, there exists $\mathbf{G}_i \in \mathcal{HW}_N$ such that $\mathbf{G}_i^{\dagger}\mathbf{E}_i\mathbf{G}_i = -\mathbf{E}_i$ and $\mathbf{G}_i^{\dagger}\mathbf{E}_j\mathbf{G}_i = \mathbf{E}_j$ for $i \neq j$. Now put $\mathbf{G}_{\mathbf{d}} := \mathbf{G}_1^{d_1}\cdots\mathbf{G}_m^{d_m}$. Then

$$\mathbf{G}_{\mathbf{d}}^{\dagger}\Pi_{\mathcal{S}}\mathbf{G}_{\mathbf{d}} = \Pi_{\mathcal{S}_{\mathbf{d}}}. \tag{67}$$

It follows that $\{V(\mathcal{S}_{\mathbf{d}}) \mid \mathbf{d} \in \mathbb{F}_2^m\}$ is an orthonormal basis of $\mathbb{C}^N$. In [41] the authors used a similar insight to construct maximal sets of *mutually unbiased bases*.

D. Clifford Group

The Clifford group in N dimensions [42] is defined to be the normalizer of $\mathcal{HW}_N$ in $\mathbb{U}(N)$ modulo $\mathbb{U}(1)$:

$$\mathrm{Cliff}_N = \{\mathbf{G} \in \mathbb{U}(N) \mid \mathbf{G}\mathcal{HW}_N\mathbf{G}^\dagger = \mathcal{HW}_N\}/\mathbb{U}(1). \quad (68)$$

The reason one quotients out $\mathbb{U}(1) \cong \{\alpha\mathbf{I}_N \mid |\alpha| = 1\}$, is to obtain a finite group. In this case $\mathcal{HW}_N^*$ is a normal subgroup of Cliff_N.

Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_{2m}\}$ be the standard basis of $\mathbb{F}_2^{2m}$, and consider $\mathbf{G} \in \mathrm{Cliff}_N$. Let $\mathbf{c}_i \in \mathbb{F}_2^{2m}$ be such that

$$\mathbf{G}\mathbf{E}(\mathbf{e}_i)\mathbf{G}^\dagger = \pm\mathbf{E}(\mathbf{c}_i). \quad (69)$$

Then the matrix $\mathbf{F}_\mathbf{G}$ whose ith row is $\mathbf{c}_i$ is a symplectic matrix such that

$$\mathbf{G}\mathbf{E}(\mathbf{c})\mathbf{G}^\dagger = \pm\mathbf{E}(\mathbf{c}^\mathsf{T}\mathbf{F}_\mathbf{G}) \quad (70)$$

for all $\mathbf{c} \in \mathbb{F}_2^{2m}$. Based on (70) we obtain a group homomorphism

$$\Phi : \mathrm{Cliff}_N \longrightarrow \mathrm{Sp}(2m; 2), \quad \mathbf{G} \longmapsto \mathbf{F}_\mathbf{G}, \quad (71)$$

with kernel $\ker\Phi = \mathcal{HW}_N^*$ [35]. This map is also surjective; see Section III-D.1 where specific preimages are given. From (21) and (57) ($|\mathcal{HW}_N^*| = 2^{2m}$) follows that

$$|\mathrm{Cliff}_N| = 2^{m^2+2m}\prod_{i=1}^{m}(4^i - 1). \quad (72)$$

Remark 7: Since Φ is a homomorphism we have that $\Phi(\mathbf{G}^\dagger) = \mathbf{F}_\mathbf{G}^{-1}$ and as a consequence $\mathbf{G}^\dagger\mathbf{E}(\mathbf{c})\mathbf{G} = \pm\mathbf{E}(\mathbf{c}^\mathsf{T}\mathbf{F}_\mathbf{G}^{-1})$. We will make use of this simple observation later on to determine when a column of $\mathbf{G}$ is an eigenvector of $\mathbf{E}(\mathbf{c})$. This interplay with symplectic geometry provides an exponential complexity reduction in various applications. Here, we will focus on efficiently computing common eigenspaces of maximal stabilizers.

The *phase* and *Hadamard* matrices

$$\mathbf{G}_P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \text{ and } \mathbf{H}_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (73)$$

are easily seen to be in the Clifford group Cliff_2. Some authors also include $(\mathbf{G}_P\mathbf{H}_2)^3 = \exp(\pi i/4)\mathbf{I}_2$ [37], which in our case would disappear as a scalar quotient. Thus (72) differs by a factor of 1/8 of what is commonly considered as the cardinality of the Clifford group; see https://oeis.org/A003956. For our purposes the phases are irrelevant.

1) Decomposition of the Clifford Group: In this section we will make use of the Bruhat decomposition of $\mathrm{Sp}(2m; 2)$ to obtain a decomposition of Cliff_N. To do so we will use the surjectivity of Φ from (71) and determine preimages of coset representatives from (40). The preimages of symplectic matrices $\mathbf{F}_D(\mathbf{P}), \mathbf{F}_U(\mathbf{S})$, and $\mathbf{F}_\mathbf{\Omega}(r)$ under Φ are the unitary permutation matrix, a diagonal matrix, and a partial Hadamard matrix,

$$\mathbf{G}_D(\mathbf{P}) := \mathbf{e}_\mathbf{v} \longmapsto \mathbf{e}_{\mathbf{P}^\mathsf{T}\mathbf{v}}, \quad (74)$$

$$\mathbf{G}_U(\mathbf{S}) := \mathrm{diag}\left(i^{\mathbf{v}^\mathsf{T}\mathbf{S}\mathbf{v} \mod 4}\right)_{\mathbf{v}\in\mathbb{F}_2^m}, \quad (75)$$

$$\mathbf{G}_\mathbf{\Omega}(r) := (\mathbf{H}_2)^{\otimes r} \otimes \mathbf{I}_{2^{m-r}}, \quad (76)$$

respectively. We refer the reader to [35], [43] for details.

Remark 8: Note that directly by the definition of the Hadamard matrix we have

$$\mathbf{H}_N := \mathbf{G}_\mathbf{\Omega}(m) = \frac{1}{\sqrt{2^m}}[(-1)^{\mathbf{v}^\mathsf{T}\mathbf{w}}]_{\mathbf{v},\mathbf{w}\in\mathbb{F}_2^m}. \quad (77)$$

Whereas, for any $r = 1, \ldots, m$, one straightforwardly computes

$$\mathbf{G}_\mathbf{\Omega}(r)\cdot\mathbf{Z}(m, r) = [(-1)^{\mathbf{v}^\mathsf{T}\mathbf{w}} \cdot f(\mathbf{v}, \mathbf{w}, r)]_{\mathbf{v},\mathbf{w}\in\mathbb{F}_2^m}, \quad (78)$$

where $\mathbf{Z}(m, r) := \mathbf{I}_{2^r} \otimes \sigma_z^{\otimes m-r}$ is the diagonal Pauli that acts as σ_z on the last $m - r$ qubits, and

$$f(\mathbf{v}, \mathbf{w}, r) = \prod_{i=r+1}^{m}(1 + v_i + w_i). \quad (79)$$

Note that the value of f will be 1 precisely when $\mathbf{v}$ and $\mathbf{w}$ coincide in their last $m - r$ coordinates and 0 otherwise. It follows that f is identically 1 when $r = m$ and f is the Kronecker function $\delta_{\mathbf{v},\mathbf{w}}$ when $r = 0$. We will use f to determine the *sparsity* of a Clifford matrix/stabilizer state. Of course $r = m$ corresponds to *fully occupied* objects with only nonzero entries; see also Remarks 11 and 12 for the extreme cases of $r = 0, 1$.

Example 2 (Example 1 continued): Let us reconsider the invertible matrices from (16). Recall that there we had $m = 3, r = 2$. Here we will construct the Cliffords corresponding to the canonical coset representative (49), with $\mathbf{S}_r = \mathbf{0}_{2\times 2}$. For the case $u = 0$ one computes[4] $\mathbf{G}_D(\mathbf{P}_{u=0}^\mathsf{T})$ as in (74), and multiplies it (from the right) by $\mathbf{G}_\mathbf{\Omega}(2)$ as in (76) (we will omit $1/\sqrt{2^2}$) and then by $\mathbf{Z}(3, 2)$ to obtain

$$\mathbf{G}_{u=0} = \begin{bmatrix} + & 0 & + & 0 & + & 0 & + & 0 \\ + & 0 & - & 0 & + & 0 & - & 0 \\ 0 & - & 0 & - & 0 & - & 0 & - \\ 0 & - & 0 & + & 0 & - & 0 & + \\ + & 0 & + & 0 & - & 0 & - & 0 \\ + & 0 & - & 0 & - & 0 & + & 0 \\ 0 & - & 0 & - & 0 & + & 0 & + \\ 0 & - & 0 & + & 0 & + & 0 & - \end{bmatrix}. \quad (80)$$

As mentioned, (74) by definition yields a permutation matrix. Thus $\mathbf{G}_{u=0}$ is nothing else but $\mathbf{G}_\mathbf{\Omega}(2) = \mathbf{H}_2 \otimes \mathbf{H}_2 \otimes \mathbf{I}_2$, with its rows permuted accordingly, and a possible sign introduced to its columns by the diagonal matrix $\mathbf{Z}(3, 2) = \mathbf{I}_4 \otimes \sigma_z$. Similarly, for the case $u = 1$, one obtains

$$\mathbf{G}_{u=1} = \begin{bmatrix} + & 0 & + & 0 & + & 0 & + & 0 \\ + & 0 & - & 0 & + & 0 & - & 0 \\ 0 & - & 0 & - & 0 & - & 0 & - \\ 0 & - & 0 & + & 0 & - & 0 & + \\ 0 & - & 0 & - & 0 & + & 0 & + \\ 0 & - & 0 & + & 0 & + & 0 & - \\ + & 0 & + & 0 & - & 0 & - & 0 \\ + & 0 & - & 0 & - & 0 & + & 0 \end{bmatrix}. \quad (81)$$

We will discuss how the $\{+, -, 0\}$ patterns are correlated later on.

Let us now return to the Clifford group. The Bruhat decomposition (31) of $\mathrm{Sp}(2m; 2)$ already gives a decomposition of Cliff_N. However, in order to have a concise approach one has to be a bit careful. In this section we will write $\mathbf{G} = \Phi^{-1}(\mathbf{F})$,

[4] See Section IV-A for why we consider the transpose instead of $\mathbf{P}$ itself.

where the equality is taken modulo the center $\mathcal{HW}_N^* \ltimes \mathbb{Z}_8$. In other words, we will disregard the central part of $\Phi^{-1}(\mathbf{F})$ and consider only the Clifford part. The cyclic group $\mathbb{Z}_8$ of order 8 comes into play to accommodate 8th roots of unity coming out of products $\mathbf{G}_U(\mathbf{S})\mathbf{G}_{\mathbf{\Omega}}(r)$. This setup, yet again, confirms the importance of

$$\mathrm{Cliff}_N^* := \{\exp(i\pi k/4)\mathbf{G} \mid k \in \mathbb{Z}_8, \mathbf{G} \in \mathrm{Cliff}_N\}. \tag{82}$$

Let $\mathcal{G} = \{\mathbf{G}_D(\mathbf{P})\mathbf{G}_U(\mathbf{S}) \mid \mathbf{P} \in \mathrm{GL}(m;2), \mathbf{S} \in \mathrm{Sym}(m;2)\}$ be the preimage of $\mathcal{P}$ from (27). For obvious reasons, it is referred as the *Hadamard-free* group; see also [44]. As for the case of the symplectic group, this group acts from the right on matrices of the form

$$\mathbf{G}_D(\mathbf{P}_1)\mathbf{G}_U(\mathbf{S}_1)\mathbf{G}_{\mathbf{\Omega}}(r)\mathbf{G}_U(\mathbf{S}_2)\mathbf{G}_D(\mathbf{P}_2) \tag{83}$$

and thus, a coset representative would look like

$$\mathbf{G}_{\mathbf{F}} := \mathbf{G}_D(\mathbf{P}_1)\mathbf{G}_U(\mathbf{S}_1)\mathbf{G}_{\mathbf{\Omega}}(r)\,. \tag{84}$$

For Grassmannian line codebooks, one is interested on coset representatives, the right action of $\mathbf{G}_U(\mathbf{S}_1)\mathbf{G}_{\mathbf{\Omega}}(r)$ has been divided out, i.e., column rotations and permutations.

The coset representatives can be understood in terms of the preimage of generators of $\mathrm{GL}(m;2)$ and $\mathrm{Sym}(m;2)$. Let us start with the former, which can be generated by two elements [45]. Namely, it can be generated $\mathbf{P} := \mathbf{I}_m + \mathbf{E}_{12}$ where $\mathbf{E}_{12}$ is the elementary (binary) matrix with 1 in position $(1,2)$ and 0 elsewhere, together with the cyclic permutation matrix Π_{cycl} acting as the permutation $(12\cdots m)$. A larger set of generators is also of interest. Let $\Pi_{i,j}$ be a transposition matrix. Then of course $\mathbf{P}$ along with all the $\Pi_{i,j}$ generate $\mathrm{GL}(m;2)$. While $\Pi_{i,j}$ swaps dimensions i and j in $\mathbb{F}_2^m$, it is easily seen that $\Phi^{-1}(\mathbf{F}_D(\Pi_{i,j}))$ swaps the tensor dimensions i and j in $(\mathbb{C}^2)^{\otimes m}$. Moreover

$$\Phi^{-1}(\mathbf{F}_D(\mathbf{P})) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \otimes \mathbf{I}_{N-4}. \tag{85}$$

The above 4×4 matrix is known in quantum computation as the controlled-NOT (CNOT) quantum gate. In itself, the CNOT gate is of form $\mathbf{G}_D(\mathbf{P})$ where

$$\mathbf{P} = \mathbf{P}^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{86}$$

For $\mathrm{Sym}(m;2)$ we consider matrices $\mathbf{S}_{\mathbf{v}} := \mathbf{v}^{\mathsf{T}}\mathbf{v}$ where $\mathbf{v} \in \mathbb{F}_2^m$ is a vector with at most two non-zero entries. Then

$$\Phi^{-1}(\mathbf{F}_U(\mathbf{S}_{\mathbf{v}})) = \frac{1}{\sqrt{2}}(\mathbf{I}_N + i\mathbf{E}(\mathbf{0},\mathbf{v})). \tag{87}$$

Note that when $\mathbf{v}$ has exactly one non-zero entry in position j, the jth tensor dimension will contain the phase matrix $\mathbf{G}_P = \exp(-i\pi/4)(\mathbf{I}_2 + i\sigma_z)$ form (73). On the other hand, when $\mathbf{v}$ has exactly two non-zero entries (87) gives rise to $\mathbf{G}_{CZ}(\mathbf{G}_P \otimes \mathbf{G}_P)$ in tensor dimensions i and j, where $\mathbf{G}_{CZ} = \mathrm{diag}(1,1,1,-1)$. The latter is known in quantum computation as the controlled-Z (CZ) quantum gate, and it is of form $\mathbf{G}_U(\mathbf{I}_2)$.

In conclusion, the Bruhat decomposition of $\mathrm{Sp}(2m;2)$ directly yields some fundamental quantum gates as described above. Similar ideas were used in [33] where the *depth* of *stabilizer circuits* was considered. Classically, there exist several decompositions of the symplectic group, which in principle would yield a decomposition of the Clifford group.

IV. Binary Subspace Chirps

Let us recall the definition of Binary Subspace Chirps from (5). A BSSC $\mathbf{w}$ is a unit complex vector in $N = 2^m$ dimensions characterized by a rank $0 \le r \le m$, a "binary chirp part", and an "on-off pattern part". Namely, given a binary subspace $H \in \mathcal{G}(m,r;2)$ of rank $0 \le r \le m$, we have $\mathbf{w}(\mathbf{a}) = 0$ for $\mathbf{a} \notin H$, whereas the collection of dimensions indexed by H, $\{\mathbf{w}(\mathbf{a}) \mid \mathbf{a} \in H\}$, will form a binary chirp in 2^r dimensions. As in Section III-A, we will think of the subspace H as the column space of a full-rank $m \times r$ matrix $\mathbf{H}_{\mathcal{I}}$, for which $\mathbf{a} \in H$ iff $\mathbf{a} = \mathbf{H}_{\mathcal{I}}\mathbf{x}$ for some *unique* $\mathbf{x} \in \mathbb{F}_2^r$. Additionally, the "BC part", in turn, is characterized by $\mathbf{S}_r \in \mathrm{Sym}(r;2)$ and $\mathbf{b}_r \in \mathbb{F}_2^r$. As mentioned in Section II-B, working with a coset of H is just as good, and since there 2^{m-r} different cosets, we can keep track of them with a vector $\mathbf{b}_{m-r} \in \mathbb{F}_2^{m-r}$. Namely, for $\mathbf{b}_{m-r} \in \mathbb{F}_2^{m-r}$, the BC part, will be located in dimensions indexed by the coset $\{\mathbf{a} = \mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} + \mathbf{H}_{\mathcal{I}}\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_2^r\}$, with $\mathbf{I}_{\widetilde{\mathcal{I}}}$ as in Section III-A. With this notation, we recover the subspace H for $\mathbf{b}_{m-r} = \mathbf{0}$. Thus, for a general vector $\mathbf{b}^{\mathsf{T}} = [\mathbf{b}_r^{\mathsf{T}} \;\; \mathbf{b}_{m-r}^{\mathsf{T}}] \in \mathbb{F}_2^m$ we have

$$\mathbf{w}^H_{\mathbf{b},\mathbf{S_r}}(\mathbf{a}) = \begin{cases} \frac{1}{\sqrt{2^r}} i^{\mathbf{x}^{\mathsf{T}}\mathbf{S}_r\mathbf{x} + 2\mathbf{b}_r^{\mathsf{T}}\mathbf{x}}, & \text{if } \mathbf{a} = \mathbf{H}_{\mathcal{I}}\mathbf{x} + \mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r}, \\ 0, & \text{otherwise.} \end{cases} \tag{88}$$

Before procceding with further understanding (88), we point out that BCs are indeed a special case of BSSC. Indeed, for $r = m$ we have $H = \mathbb{F}_2^m$ and $\mathbf{S}_{r=m} \in \mathrm{Sym}(m,2)$ and (88) has only non-zero entries and exactly matches (3). The next step, is to better understand (88) by further leveraging Schubert Cells. Note first that

$$\mathbf{a} = \mathbf{H}_{\mathcal{I}}\mathbf{x} + \mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ \mathbf{b}_{m-r} \end{bmatrix} = \mathbf{P} \begin{bmatrix} \mathbf{x} \\ \mathbf{b}_{m-r} \end{bmatrix}, \tag{89}$$

where $\mathbf{P}$ is the unique invertible matrix (14) associated to the subspace H. Making use of (15), we obtain

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{b}_{m-r} \end{bmatrix} = \mathbf{P}^{-1}\mathbf{a} = \begin{bmatrix} (\mathbf{I}_{\mathcal{I}})^{\mathsf{T}}\mathbf{a} \\ \widetilde{\mathbf{H}_{\mathcal{I}}}^{\mathsf{T}}\mathbf{a} \end{bmatrix}, \tag{90}$$

which, in particular, tells us that the coset $\{\mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} + \mathbf{H}_{\mathcal{I}}\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_2^r\}$ is precisely the solution set of the equation

$$\widetilde{\mathbf{H}_{\mathcal{I}}}^{\mathsf{T}}\mathbf{a} = \mathbf{b}_{m-r}. \tag{91}$$

Next, recall the function $f(\mathbf{v},\mathbf{w},r)$ from (79). Recall also that, by the very definition, its value is 1 precisely when $\mathbf{v},\mathbf{w}$ coincide in their last $m-r$ coordinates. We thus conclude that

$$f(\mathbf{b},\mathbf{P}^{-1}\mathbf{a},r) = \begin{cases} 1, & \text{if } \mathbf{a} = \mathbf{H}_{\mathcal{I}}\mathbf{x} + \mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r}, \\ 0, & \text{otherwise,} \end{cases} \tag{92}$$

for any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m$. We will use this to keep track of the on-off pattern of the corresponding BSSC. We point out here that Remark 8 already hints a close relationship with the partial Hadamard matrix $\mathbf{G}_{\mathbf{\Omega}}(r) = (\mathbf{H}_2)^{\otimes r} \otimes \mathbf{I}_{2^{m-r}}$. Next, as already hinted in the proof of Lemma 1, it is beneficial to embed $\mathbf{S}_r \in \mathrm{Sym}(r;2)$ as the upper-left block of $\mathbf{S} \in \mathrm{Sym}(m;2)$, and set the rest of $\mathbf{S}$ to zero. Then, for $\mathbf{a} \in \mathbb{F}_2^m$ satisfying (91) (that is, nonzero locations of the BSSC), (90) implies $\mathbf{a}^\mathsf{T}\mathbf{P}^{-\mathsf{T}}\mathbf{S}\mathbf{P}^{-1}\mathbf{a} = \mathbf{x}^\mathsf{T}\mathbf{S}_r\mathbf{x}$. Combining everything together, (88) reads as

$$\mathbf{w}_{\mathbf{b}}^{H,\mathbf{S}_r}(\mathbf{a}) = \frac{(-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}}{\sqrt{2^r}} i^{\mathbf{a}^\mathsf{T}\mathbf{P}^{-\mathsf{T}}\mathbf{S}\mathbf{P}^{-1}\mathbf{a}+2\mathbf{b}^\mathsf{T}\mathbf{P}^{-1}\mathbf{a}} f(\mathbf{b}, \mathbf{P}^{-1}\mathbf{a}, r). \tag{93}$$

Above, the function $\mathrm{wt}(\bullet)$ is just the Hamming weight which counts the number of non-zero entries in a binary vector. The overall sign $(-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}$ is insignificant for our purposes since we are dealing with Grassmannian/projective codebooks. Thus, in what follows, we will use (93) as the definition of BSSCs.

A. Algebraic Structure of BSSCs

In what follows we fix a rank r, invertible $\mathbf{P}$, symmetric $\mathbf{S}$, and $\mathbf{b} \in \mathbb{F}_2^m$. As usual, $\mathbf{P}$ is uniquely associated with $H \in \mathcal{G}(m,r;2)$, $\mathbf{S}$ contains an $r \times r$ symmetric in its upper left corner and 0 otherwise, and $\mathbf{b}^\mathsf{T} = [\mathbf{b}_r^\mathsf{T}\ \mathbf{b}_{m-r}^\mathsf{T}]$. Next, let $\mathbf{F} := \mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\mathbf{S})\mathbf{F}_D(\mathbf{P}^\mathsf{T}) \in \mathrm{Sp}(m;2)$ and let $\mathbf{G}_{\mathbf{F}} = \mathbf{G}_D(\mathbf{P}^\mathsf{T})\mathbf{G}_U(\mathbf{S})\mathbf{G}_{\mathbf{\Omega}}(r) \in \mathrm{Cliff}_N$, so that $\Phi(\mathbf{G}_{\mathbf{F}}) = \mathbf{F}$. Recall also that $\{\mathbf{e}_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_2^m\}$ is the standard basis of $\mathbb{C}^N$. With a substitution $\mathbf{u} := \mathbf{P}^{-1}\mathbf{a}$ in (93) we have

$$\mathbf{w}_{\mathbf{b}} = \sum_{\mathbf{a}\in\mathbb{F}_2^m} \mathbf{w}_{\mathbf{b}}(\mathbf{a})\mathbf{e}_{\mathbf{a}} \tag{94}$$

$$= \frac{(-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}}{\sqrt{2^r}} \sum_{\mathbf{u}\in\mathbb{F}_2^m} i^{\mathbf{u}^\mathsf{T}\mathbf{S}\mathbf{u}}(-1)^{\mathbf{b}^\mathsf{T}\mathbf{u}} f(\mathbf{b},\mathbf{u},r)\mathbf{e}_{\mathbf{P}\mathbf{u}} \tag{95}$$

$$= \mathbf{G}_D(\mathbf{P}^\mathsf{T}) \cdot \mathbf{G}_U(\mathbf{S}) \cdot \frac{(-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}}{\sqrt{2^r}} \sum_{\mathbf{u}\in\mathbb{F}_2^m} (-1)^{\mathbf{b}^\mathsf{T}\mathbf{u}} f(\mathbf{b},\mathbf{u},r)\mathbf{e}_{\mathbf{u}} \tag{96}$$

$$= \mathbf{G}_D(\mathbf{P}^\mathsf{T})\mathbf{G}_U(\mathbf{S}) \left((-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}\right) \mathbf{G}_{\mathbf{\Omega}}(r)\mathbf{Z}(m,r)\mathbf{e}_{\mathbf{b}} \tag{97}$$

$$= \mathbf{G}_D(\mathbf{P}^\mathsf{T})\mathbf{G}_U(\mathbf{S})\mathbf{G}_{\mathbf{\Omega}}(r)\mathbf{e}_{\mathbf{b}} \tag{98}$$

$$= \mathbf{G}_{\mathbf{F}}\mathbf{e}_{\mathbf{b}}, \tag{99}$$

where (96) follows by (74) and (75), (97) follows by (78), and (98) follows by the fact that $\mathbf{Z}(m,r)\mathbf{e}_{\mathbf{b}} = (-1)^{\mathrm{wt}(\mathbf{b}_{m-r})}\mathbf{e}_{\mathbf{b}}$. We have proved the following.

Theorem 2: With the same notation as above, the BSSC $\mathbf{w}_{\mathbf{b}}$ is the $\mathbf{b}$th column of the Clifford matrix $\mathbf{G}_{\mathbf{F}}$.

Corollary 1: Each binary subspace chirp is a stabilizer state. The converse is also true. In particular, the BSSC codebook is a group code of the Clifford group with generating vector $\mathbf{e}_{\mathbf{0}}$.

Proof: Stabilizer states can be defined equivalently as the orbit of $\mathbf{e}_{\mathbf{0}}$ under the action of Cliff_N; see [46] for instance. Then the first statement follows by (99). The converse is true due to cardinalities. ∎

Example 3 (Examples 1 and 2 Continued): Let us consider the case $u = 0$, and for simplicity, let us set the symmetric $\mathbf{S}$ to be the zero matrix,[5] so that $\mathbf{G}_U(\mathbf{S})$ is the identity matrix. The on-off pattern of the resulting BSSCs is governed by the $r = 2$ dimensional subspace $H = \{000^\mathsf{T}, 100^\mathsf{T}, 001^\mathsf{T}, 101^\mathsf{T}\} = \mathrm{cs}(\mathbf{H}_{\{1,3\}})$. The above argument tells us that these BSSCs are precisely the columns of $\mathbf{G}_{u=0}$ from (80). One verifies this directly using the definition (93). Moreover, the structure of the on-off patterns is completely determined by (89). Indeed, we see in (80) two on-off patterns: one determined by H (if $\mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} \in H$) and one determined by its coset[6] (if $\mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} \notin H$). In our specific case, we have $\mathcal{I} = \{1,3\}$, and thus $\mathbf{I}_{\widetilde{\mathcal{I}}} = \mathbf{I}_{\{2\}} = 010^\mathsf{T}$. Thus $\mathbf{I}_{\widetilde{\mathcal{I}}}\mathbf{b}_{m-r} \in H$ iff $\mathbf{b}_{m-r} = 0$ iff $\mathbf{b} \in \{000^\mathsf{T}, 010^\mathsf{T}, 100^\mathsf{T}, 110^\mathsf{T}\}$, which corresponds to columns $\{1,3,5,7\}$. Additionally, within each of these columns, the on-off pattern is again governed by H. Indeed, the non-zero entries in these columns are in positions/rows indexed by H, that is, $\{1,2,5,6\}$ – precisely as described by (91). Since cosets form a partition, it follows immediately that columns indexed by different cosets are orthogonal. Orthogonality of columns within each coset is a bit more delicate to see directly. We will further discuss the general structure of on-off patterns in Section IV-B.

Equation (49) gives a one-to-one correspondence between canonical coset representatives and maximal stabilizers. Above we mentioned that BSSCs are columns of Clifford matrices parametrized by such coset representatives. The last piece of the puzzle is found by simultaneously diagonalizing the commuting matrices of a maximal stabilizer. We make this precise in the following.

Theorem 3: Let $\mathbf{F}$ and $\mathbf{G}_{\mathbf{F}}$ be as above. The set $\{\mathbf{w}_{\mathbf{b}} \mid \mathbf{b} \in \mathbb{F}_2^m\}$ consisting of the columns of $\mathbf{G}_{\mathbf{F}}$ is the common eigenspace of the maximal stabilizer $\mathbf{E}(\mathbf{I}_{m|r}\mathbf{P}^\mathsf{T}, (\mathbf{I}_{m|r}\mathbf{S} + \mathbf{I}_{m|-r})\mathbf{P}^{-1})$ from (49).

Proof: Consider the matrix $\mathbf{G} := \mathbf{G}_{\mathbf{F}}$ parametrized by the symplectic matrix $\mathbf{F}$, and recall that $\mathbf{w}_{\mathbf{b}}$ is the $\mathbf{b}$th column of $\mathbf{G}_{\mathbf{F}}$. It follows from Remark 7 that the columns of $\mathbf{G}$ are the eigenspace of $\mathbf{E}(\mathbf{x},\mathbf{y})$ iff

$$\mathbf{G}^\dagger\mathbf{E}(\mathbf{x},\mathbf{y})\mathbf{G} = \pm\mathbf{E}([\mathbf{x},\mathbf{y}]^\mathsf{T}\mathbf{F}^{-1}) \tag{100}$$

is diagonal. Recall also that $\mathbf{E}(\mathbf{x},\mathbf{y})$ is diagonal iff $\mathbf{x} = \mathbf{0}$, and observe that $\mathbf{F}_{\mathbf{\Omega}}(r)^{-1} = \mathbf{F}_{\mathbf{\Omega}}(r)$. Thus, $\mathbf{G}_{\mathbf{\Omega}}(r)$ will be the common eigenspace of the maximal stabilizer $\mathcal{S}$ iff $\pm\mathbf{E}([\mathbf{x}\ \mathbf{y}]^\mathsf{T}\mathbf{F}_{\mathbf{\Omega}}(r))$ is diagonal for all $\mathbf{E}(\mathbf{x},\mathbf{y}) \in \mathcal{S}$. Then it is easy to see that such maximal stabilizer is $\mathbf{E}(\mathbf{I}_{m|r}, \mathbf{I}_{m|-r})$. Next, if $\mathbf{w}$ is an eigenvector of $\mathbf{E}(\mathbf{c})$ then

$$\mathbf{G}\mathbf{w} = \pm\mathbf{G}\mathbf{E}(\mathbf{c})\mathbf{w} = \pm\mathbf{G}\mathbf{E}(\mathbf{c})\mathbf{G}^\dagger\mathbf{G}\mathbf{w} = \pm\mathbf{E}(\mathbf{c}^\mathsf{T}\Phi(\mathbf{G}))\mathbf{G}\mathbf{w}$$

implies that $\mathbf{G}\mathbf{w}$ is an eigenvector of $\mathbf{E}(\mathbf{c}^\mathsf{T}\Phi(\mathbf{G}))$. The proof is concluded by computing $[\mathbf{I}_{m|r}\ \ \mathbf{I}_{m|-r}]\mathbf{F}_U(\mathbf{S})\mathbf{F}_D(\mathbf{P}^\mathsf{T})$. ∎

The result above is well-known in the sense that of course stabilizer states are common eigenvectors of maximal stabilizers. However, the parametrization above has a nice duality built in (see also (110)) which is to the best of our knowledge novel. It also serves our main purpose in the sense that it clearly distinguishes between the "chirp part" and the

[5] $\mathbf{G}_U(\mathbf{S})$ does not affect the on-off pattern at all.

[6] There are exactly $2 = 2^3/2^2$ cosets since H has dimensions 2.

"on-off pattern part". Namely, the subspace H governs the off-diagonal part of the maximal stabilizer and it will be used to decode the "chirp part", whereas, its dual governs the diagonal part of the maximal stabilizer and it completely determines the "on-off pattern part". It is precisely this duality that we leverage for decoding BSSCs. Additionally, (93) provides a parametrization of stabilizer states. Other parametrizations are known in literature, e.g. [24, Thms. 5&6], that as well capture their subspace structure. It is our conviction that the natural way to capture this structure is via partial Hadamard matrices and Schubert Cells, as facilitated by (79) and (92). The canonical form of the invertible matrix $\mathbf{P}$ in (14) (which in the complex domain corresponds to qubit permutations) explicitly encodes the subspace/coset on which a stabilizer state is nonzero. Additionally, it can provides a simplified description of the underlying quadratic form that determines the nonzero entries. It is also our conviction that, as indicated by the semiproduct rule (28), this is the natural way to capture such quadratic form.

Remark 9: Note that for $r = m$ one has $\mathbf{E}(\mathbf{I}_{m|r}, \mathbf{I}_{m|-r}) = \mathbf{E}(\mathbf{I}_m, \mathbf{0}_m)$ and $\mathbf{G}_{\mathbf{\Omega}}(r) = \mathbf{H}_N$. Thus the above theorem covers the well-known fact that $\mathbf{H}_N$ is the common eigenspace of the maximal stabilizer $\mathcal{X}_N = \mathbf{E}(\mathbf{I}_m, \mathbf{0}_m)$. It is also well-known that the standard basis of $\mathbb{C}^N$ (that is, $\mathbf{I}_N$) is the common eigenspace of the maximal stabilizer $\mathcal{Z}_N = \mathbf{E}(\mathbf{0}_m, \mathbf{I}_m)$ of diagonal Paulis. This is of course consistent with the aforesaid fact since $[\mathbf{0}_m \;\; \mathbf{I}_m]\mathbf{\Omega} = [\mathbf{I}_m \;\; \mathbf{0}_m]$ and $\mathbf{H}_N = \Phi^{-1}(\mathbf{\Omega})$. In this extremal case we also have $\mathbf{P}_{\mathcal{I}} = \mathbf{I}_m$ and $\widetilde{\mathbf{S}_r} = \mathbf{S} \in \mathrm{Sym}(m; 2)$. So the above theorem also covers [30, Lem. 11] which (in the language of this paper) says that the common eigenspace of $\mathbf{E}(\mathbf{I}_m, \mathbf{S})$ is $\mathbf{G}_U(\mathbf{S})\mathbf{H}_N$. Additionally, because $\mathbf{S}$ is symmetric, it can be thought of as an adjacency matrix of some underlying graph, and therefore binary chirps are nothing else but *graph states*. In this way, the BC to BSSC extension can be realized as the graph states to the stabilizer states extension.

Remark 10: Theorem 3 is a closed form realization of a more general fact. Let $\mathcal{S}$ be a maximal stabilizer and let $S = \mathrm{rs}\,[\mathbf{A} \;\; \mathbf{B}] \subset \mathbb{F}_2^{2m}$ be its corresponding isotropic subspace. Consider also the diagonal Paulis $\mathcal{Z}_N$ and its corresponding subspace $Z_N = \mathrm{rs}\,[\mathbf{0}_m \;\; \mathbf{I}_m]$. Then, by [35, Alg. 1] there exists $\mathbf{G} \in \mathrm{Cliff}_N$ such that $\mathbf{G}\mathcal{S}\mathbf{G}^\dagger = \mathcal{Z}_N$. In other words, $\mathbf{G}^\dagger$ simultaneously diagonalizes $\mathcal{S}$, and moreover, the respective diagonal is a Pauli. In the symplectic domain, it follows by [35, Thm. 25] that there are precisely $2^{m(m+1)/2}$ symplectic solutions to the equation $[\mathbf{A} \;\; \mathbf{B}]\mathbf{F} = [\mathbf{0}_m \;\; \mathbf{I}_m]$.

Corollary 2: Let $\mathcal{S}$ be a maximal stabilizer. Then the stabilizer state $V(\mathcal{S})$ is a rank r BSSC iff $|\mathcal{S} \cap \mathcal{Z}_N| = 2^{m-r}$.

Proof: By Corollary 1 we know that $V(\mathcal{S})$ is a BSSC of rank r, which in turn is stabilized by the maximal stabilizer of Theorem 3. Such stabilizer has precisely 2^{m-r} diagonal Paulis; see also (110). ∎

We mentioned that the extremal case $r = m$ gives the codebook $\mathcal{V}_{\mathrm{BC}}$. Before discussing general on-off patterns, we consider the lower-end extremal cases $r = 0, 1$.

Remark 11: Let $r = 0$. In this case we again have $\mathbf{P} = \mathbf{I}_m$ and $\mathbf{S} = \mathbf{0}_m$. In addition $f(\mathbf{v}, \mathbf{w}, 0) = \delta_{\mathbf{v},\mathbf{w}}$. Thus, from (93) we see that $\mathbf{w}_{\mathbf{b}}(\mathbf{a}) \neq 0$ iff $\mathbf{a} = \mathbf{b}$, in which case we have $\mathbf{w}_{\mathbf{b}}(\mathbf{a}) = (-1)^{\mathrm{wt}(\mathbf{b})}$. This can also be seen from (99). Indeed, since $\mathbf{G}_{\mathbf{\Omega}}(0) = \mathbf{I}_N$ we have $\mathbf{G}_{\mathbf{F}} = \mathbf{I}_N$. Note also that $\mathbf{Z}(m, 0) = \sigma_z \otimes \cdots \otimes \sigma_z = \mathbf{E}(\mathbf{0}, \mathbf{1})$ is the common eigenspace of the maximal stabilizer $\mathbf{E}(\mathbf{I}_m, \mathbf{I}_m)$, as established by Theorem 3.

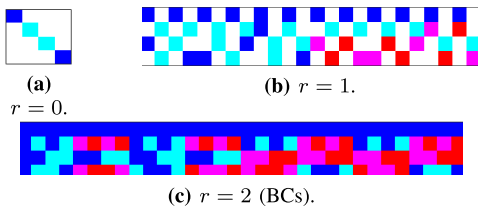

Fig. 3. BSSCs in $N = 4$ dimensions. White $= 0$, Blue $= 1$, Cyan $= -1$, Red $= i$, Magenta $= -i$.

Remark 12: Let $r = 1$. In this case, either $\mathbf{S} = \mathbf{0}_m$ or $\mathbf{S} = \mathbf{e}_1\mathbf{e}_1^{\mathsf{T}}$, where $\mathbf{e}_1 \in \mathbb{F}_2^m$ is the first standard basis vector. It follows that, up to a Pauli matrix, $\mathbf{G}_U(\mathbf{S})$ is either $\mathbf{I}_N$ or the *transvection* $(\mathbf{I}_N + iZ_1)/\sqrt{2}$ where $Z_1 = \mathbf{E}(\mathbf{0}, \mathbf{e}_1)$ has σ_z on the first qubit and identity elsewhere; see also (87). Similarly $\mathbf{G}_{\mathbf{\Omega}}(1) = (X_1 + Z_1)/\sqrt{2}$ is another transvection. Thus, rank one BSSCs are columns of transvections, permuted by some Clifford permutation $\mathbf{G}_D(\mathbf{P})$. See [47], [48] for more on transvections.

Example 4: Let $m = 2$. There are $3 = \binom{2}{1}_2$ one dimensional spaces in $\mathbb{F}_2^m$ and there are two 1×1 symmetric matrices. Thus there are $2^2 \cdot 3 \cdot 2 = 24$ BSSCs of rank $r = 1$ in $N = 2^m = 4$ dimensions, as depicted in Figure 3b. Furthermore, there are eight 2×2 symmetric matrices, and these yield $32 = 2^2 \cdot 8$ BCs, as depicted in Figure 3c. Along with $4 = 2^2$ BSSCs of rank 0 depicted on Figure 3a, we have in total $60 = 4{+}24{+}32 = 4{\cdot}3{\cdot}5$ BSSCs in $N = 4$ dimensions, as given by (8).

B. Structure of On-Off Patterns

As discussed, for $\mathbf{S}_r \in \mathrm{Sym}(r; 2)$ and $H \in \mathcal{G}(m, r; 2)$ we obtain a unitary matrix

$$\mathbf{U}_{H,\mathbf{S}_r}(\mathbf{a}, \mathbf{b}) = \big[\mathbf{w}_{\mathbf{b}}(\mathbf{a})\big]_{\mathbf{a},\mathbf{b}} \in \mathbb{U}(N). \tag{101}$$

We will omit the subscripts when the context is clear. We know from (99) that such a matrix is an element of Cliff_N. The subspace H determines the *sparsity* of $\mathbf{U}$. Indeed, we see from (88) that the on-off pattern is supported either on H or on a coset of it. Thus, the on-off patterns of different columns are either equal or disjoint. It also follows that in $\mathbf{U}$ there are 2^{m-r} different on-off patterns, each of which repeat 2^r times.

In [29] it was shown that BCs form a group under coordinate-wise multiplication. Whereas, we can immediately see that this is not the case for BSSCs. For instance, if one considers two BSSCs with disjoint on-off patterns then they coordinate-wise multiply to $\mathbf{0} \in \mathbb{C}^N$. When two BSSCs have the same on-off pattern the coordinate-wise multiplication can be determined as follows. Let $\mathbf{w}_1$ and $\mathbf{w}_2$ be two columns of $\mathbf{U}$ with the same on-off pattern, indexed by $\mathbf{b}_1$ and $\mathbf{b}_2$ respectively. Let $\widetilde{r} = m - r$. In such case, (91) implies $\mathbf{b}_{1,\widetilde{r}} = \mathbf{b}_{2,\widetilde{r}}$, that is, they are equal in their last $\widetilde{r}$ coordinates.

Recall also that the non-zero coordinates of a BSSC are determined by (89). We have that

$$2^r \mathbf{w}_1(\mathbf{a})\mathbf{w}_2(\mathbf{a}) = (-1)^{\mathbf{x}^\mathsf{T}\mathbf{S}\mathbf{x}+(\mathbf{b}_{1,r}+\mathbf{b}_{2,r})^\mathsf{T}\mathbf{x}}, \tag{102}$$

where $\mathbf{x} \in \mathbb{F}_2^r$ is such that

$$\mathbf{P}^{-1}\mathbf{a} = \begin{bmatrix} \mathbf{x} \\ \mathbf{b}_{1,\widetilde{r}} \end{bmatrix} = \begin{bmatrix} \mathbf{x} \\ \mathbf{b}_{2,\widetilde{r}} \end{bmatrix}. \tag{103}$$

The matrix $\mathbf{P}$ above corresponds to H as usual. Next, the map $\mathbf{x} \longmapsto \mathbf{x}^\mathsf{T}\mathbf{S}\mathbf{x}$ is additive modulo 2, and thus it is of form $\mathbf{x} \longmapsto \mathbf{b}_\mathbf{S}^\mathsf{T}\mathbf{x}$ for some $\mathbf{b}_\mathbf{S} \in \mathbb{F}_2^m$. It follows that

$$2^r \mathbf{w}_1(\mathbf{a})\mathbf{w}_2(\mathbf{a}) = (-1)^{(\mathbf{b}_\mathbf{S}+\mathbf{b}_{1,r}+\mathbf{b}_{2,r})^\mathsf{T}\mathbf{x}}. \tag{104}$$

Then it is easy to see that the right-hand-side of (104) is, up to a sign, a column of $\mathbf{G}_D(\mathbf{P}^\mathsf{T})\mathbf{G}_\mathbf{\Omega}(r)$.

With a similar argument, when two BSSCs with the same on-off pattern, but different symmetric matrices $\mathbf{S}_1$ and $\mathbf{S}_2$, are coordinate-wise multiplied, we obtain, up to sign, a column of $\mathbf{G}_D(\mathbf{P}^\mathsf{T})\mathbf{G}_U(\mathbf{S}_1+\mathbf{S}_2)\mathbf{G}_\mathbf{\Omega}(r)$. In all cases, the "up to sign" is determined by $\mathrm{wt}(\mathbf{b}_{\widetilde{r}})$, that is, the Hamming weight of the last $\widetilde{r}$ coordinates of the column index.

Also with a similar argument, one determines the conjugate of BSSCs and the coordinate-wise multiplication of BSSCs with $H_1 \in \mathcal{G}(m, r_1)$ and $H_2 \in \mathcal{G}(m, r_2)$. Without diving in details, in this case the on-off pattern will be determined by $H_1 \cap H_2$ and of course the sparsity will be determined by $r = \dim H_1 \cap H_2$.

In particular, we have proved the following.

Theorem 4: The set $\mathcal{V}_{\mathrm{BSSC}}$ is closed with respect to coordinate-wise conjugation. The set $\mathcal{V}_{\mathrm{BSSC}} \cup \{\mathbf{0}_N\}$ is closed with respect to coordinate-wise multiplication. The set of all BSSCs of given sparsity r and on-off pattern is isomorphic to $\mathrm{Sym}(r; 2)$.

By Theorem 1, the codebooks $\mathcal{V}_{\mathrm{BC}}$ and $\mathcal{V}_{\mathrm{BSSC}}$ have the same minimum distance, and the latter is 2.384 bigger. Thus, from a coding prospective the codebook $\mathcal{V}_{\mathrm{BSSC}}$ provides a clear improvement. Additionally, we will see next that $\mathcal{V}_{\mathrm{BSSC}}$ can be decoded with similar complexity as $\mathcal{V}_{\mathrm{BC}}$. For these reasons, $\mathcal{V}_{\mathrm{BSSC}}$ is an optimal candidate for extending $\mathcal{V}_{\mathrm{BC}}$ also from a communication prospective. The alphabet of $\mathcal{V}_{\mathrm{BC}}$ is $\{\pm 1, \pm i\}$ whereas the alphabet of $\mathcal{V}_{\mathrm{BSSC}}$ is $\{\pm 1, \pm i\} \cup \{0\}$, which is a minimal extension from the implementation complexity prospective.

Corollary 3: Let $\mathbf{G}_j = \mathbf{G}_U(\mathbf{S}_j)\mathbf{H}_N \in \mathrm{Cliff}_N$ for $j = 1, 2$ and $\mathbf{S}_j \in \mathrm{Sym}(m; 2)$. Then $\mathbf{G} = \mathbf{G}_1^\dagger \mathbf{G}_2$ has sparsity r where $r = \mathrm{rank}\,(\mathbf{S}_1 + \mathbf{S}_2)$ and its on-off pattern is determined by $H = \mathrm{rs}\,(\mathbf{S}_1 + \mathbf{S}_2)$.

Proof: Recall that $\mathbf{G}_j$ constitutes all the BCs parametrized by $\mathbf{S}_j$. Then the statement follows directly by (9). ∎

Remark 13: The vector space of symmetric matrices can be written in terms of a chain of nested subspaces, referred in literature as Delsarte-Goethals sets,

$$\mathrm{DG}(m, 0) \subset \mathrm{DG}(m, 1) \subset \cdots \subset \mathrm{DG}(m, (m-1)/2) \tag{105}$$

with the property that every nonzero matrix in $\mathrm{DG}(m, r)$ has rank at least $m-2r$ [49], [50]. For applications in deterministic compressed sensing, random access, and quantum computation see [6], [30], [51]. Since $\mathrm{DG}(m, r)$ is a vector space, it comes with the property that the sum of every two different matrices also has rank at least $m-2r$. Thus, for $\mathbf{S}_1, \mathbf{S}_2 \in \mathrm{DG}(m, (m-r)/2)$, the construction of Corollary 3 yields a Clifford matrix of sparsity at least r. This is an alternative way of creating rank r BSSCs in terms of BCs. However, this will not yield all the BSSCs because not every subspace H is the row/column space of a symmetric matrix $\mathbf{S}$.

V. Reconstruction Algorithms

In this section we use the rich algebraic structure of BSSCs to construct a low complexity decoding/reconstruction algorithm. We will build our way up by starting with the reconstruction of a single BSSC. In order to gain some intuition we disregard noise at first. The problem in hand is to recover $H, \mathbf{S}_r$, and $\mathbf{b}$ given a binary subspace chirp $\mathbf{w}_\mathbf{b}$ as in (93). In this noiseless scenario, the easiest task is the recovery of the rank r. Namely, by (91) we have

$$\mathbf{w}_\mathbf{b}(\mathbf{a})\overline{\mathbf{w}_\mathbf{b}(\mathbf{a})} = \begin{cases} 1/2^r, & 2^r \text{ times}, \\ 0, & 2^{m-r} \text{ times}. \end{cases} \tag{106}$$

To reconstruct H and then eventually $\mathbf{S}_r$ we generalize the *shift and multiply* technique used in [6] for the reconstruction of binary chirps. Here "shift" means shifting/permuting the coordinates of $\mathbf{w}_\mathbf{b}$ according to $\mathbf{a} \longmapsto \mathbf{a} + \mathbf{e}$ and "multiply" means coordinate-wise multiplication of the shifted version with the original vector. The underlying structure that enables this generalization is the fact that the on-pattern of BSSC is a BC of lower rank as discussed in Section IV. The prime focus will be to upgrade to a technique that also takes care of identifying the subspace H. Additionally, in our scenario extra care is required as the shifting can perturb the on-off pattern. Namely, we must use only shifts $\mathbf{a} \longmapsto \mathbf{a}+\mathbf{e}$ that preserve the on-off pattern. It follows by (91) that we must use only shifts by $\mathbf{e}$ that satisfy $(\widetilde{\mathbf{H}_\mathcal{I}})^\mathsf{T}\mathbf{e} = \mathbf{0}$, or equivalently $\mathbf{e} = \mathbf{H}_\mathcal{I}\mathbf{x}$ for $\mathbf{x} \in \mathbb{F}_2^r$. In this instance, thanks to (13) we have

$$\mathbf{P}^{-1}\mathbf{e} = \mathbf{P}^{-1}\mathbf{H}_\mathcal{I}\mathbf{x} = \begin{bmatrix} \mathbf{x} \\ \mathbf{0} \end{bmatrix}. \tag{107}$$

If we focus on the nonzero entries of $\mathbf{w}_\mathbf{b}$ and on shifts (107) that preserve the on-off pattern of $\mathbf{w}_\mathbf{b}$ we are left with a rank-r binary chirp which remains unaffected by the shift. It is beneficial to take $\mathbf{y}$ to be $\mathbf{f}_i$ - one of the standard basis vectors of $\mathbb{F}_2^r$ and identify $\mathbf{x}$ with $\mathbf{P}^{-1}\mathbf{e}$. With this preparation we are able to use the shift and multiply technique, that is, shift the given BSSC $\mathbf{w}_\mathbf{b}$ according to the shift $\mathbf{x} \longmapsto \mathbf{x} + \mathbf{f}_i$ (which only affects the on-pattern and fixes the off-pattern) and then multiply by its conjugate:

$$\mathbf{w}_\mathbf{b}(\mathbf{x}+\mathbf{f}_i)\overline{\mathbf{w}_\mathbf{b}(\mathbf{x})} = \frac{1}{2^r} \cdot i^{\mathbf{f}_i^\mathsf{T}\mathbf{S}_r\mathbf{f}_i} \cdot (-1)^{\mathbf{b}^\mathsf{T}\mathbf{f}_i} \cdot (-1)^{\mathbf{x}^\mathsf{T}\mathbf{S}_r\mathbf{f}_i}. \tag{108}$$

Note that above only the last term depends on $\mathbf{x}$. Now if we multiply (108) with the Hadamard matrix (77) we obtain

$$i^{\mathbf{f}_i^\mathsf{T}\mathbf{S}_r\mathbf{f}_i} \cdot (-1)^{\mathbf{b}^\mathsf{T}\mathbf{f}_i} \sum_{\mathbf{x}\in\mathbb{F}_2^r} (-1)^{\mathbf{x}^\mathsf{T}(\mathbf{v}+\mathbf{S}_r\mathbf{f}_i)}, \tag{109}$$

for all $\mathbf{x} \in \mathbb{F}_2^r$ (where we have omitted the scaling factor). Then (109) is nonzero precisely when $\mathbf{v} = \mathbf{S}_r\mathbf{f}_i$ - the ith column of $\mathbf{S}_r$. With $\mathbf{S}_r$ in hand, one recovers $\mathbf{b}_r$ similarly by multiplying $\mathbf{w}_\mathbf{b}(\mathbf{x})\overline{\mathbf{w}_\mathbf{0}(\mathbf{x})}$ with the Hadamard matrix.

To recover $\mathbf{b}_{m-r}$ one simply uses the knowledge of nonzero coordinates and (89). Next, with $\mathbf{b}$ in hand and the knowledge of the on-off pattern one recovers $\mathbf{H}_{\mathcal{I}}$ (and thus H) using (91). We will refer to the process of finding the column index $\mathbf{b}$ as *dechirping*.

In the above somewhat ad-hoc method we did not take advantage of the geometric structure of the subspace chirps as eigenvectors of given maximal stabilizers or equivalently as the columns of given Clifford matrices. We do this next by following the line of [22].

Let $\mathbf{w}$ be a subspace chirp as in (93), and recall that, by Theorem 2, it is the column of $\mathbf{G} := \mathbf{G}_{\mathbf{F}} = \mathbf{G}_D(\mathbf{P}^{\mathsf{T}})\mathbf{G}_U(\mathbf{S})\mathbf{G}_{\mathbf{\Omega}}(r)$ where $\mathbf{F} := \mathbf{F}_{\mathbf{\Omega}}(r)\mathbf{F}_U(\mathbf{S})\mathbf{F}_D(\mathbf{P}^{\mathsf{T}})$. Then by construction $\mathbf{G}$ and $\mathbf{F}$ satisfy $\mathbf{G}^{\dagger}\mathbf{E}(\mathbf{c})\mathbf{G} = \pm\mathbf{E}(\mathbf{c}^{\mathsf{T}}\mathbf{F}^{-1})$ for all $\mathbf{c} \in \mathbb{F}_2^{2m}$. Recall also from Theorem 3 that $\mathbf{G}$ is the common eigenspace of the maximal stabilizer

$$\mathbf{E}(\mathbf{I}_{m|r}\mathbf{P}^{\mathsf{T}},\, (\mathbf{I}_{m|r}\mathbf{S} + \mathbf{I}_{m|-r})\mathbf{P}^{-1}) = \mathbf{E}\left(\left[\begin{array}{c|c} \mathbf{H}_{\mathcal{I}}^{\mathsf{T}} & \mathbf{S}_r\mathbf{I}_{\mathcal{I}}^{\mathsf{T}} \\ \mathbf{0} & \widetilde{\mathbf{H}_{\mathcal{I}}}^{\mathsf{T}} \end{array}\right]\right). \tag{110}$$

Thus, to reconstruct the unknown subspace chirp $\mathbf{w}$, it is sufficient to first identify the maximal stabilizer that stabilizes it, and then identify $\mathbf{w}$ as a column of $\mathbf{G}$. The best way to accomplish the latter task, dechirping that is, is as described above, and thus we focus only on the former task. A crucial observation at this stage is the fact that the maximal stabilizer in (110) has precisely 2^r off-diagonal and 2^{m-r} diagonal Pauli matrices; see also Corollary 2.

We now make use of the argument in Theorem 3, that is, $\mathbf{w}$ is an eigenvalue of $\mathbf{E}(\mathbf{c})$ iff $\mathbf{E}(\mathbf{c}^{\mathsf{T}}\mathbf{F}^{-1})$ is diagonal. Let us focus first on identifying the 2^{m-r} diagonal Pauli matrices that stabilize $\mathbf{w}$, that is, $\mathbf{c} = \begin{bmatrix}\mathbf{0}\\ \mathbf{y}\end{bmatrix}$. First we see that

$$\mathbf{F}^{-1} = \begin{bmatrix} \mathbf{I}_{\mathcal{I}}\mathbf{S}_r & \widetilde{\mathbf{H}_{\mathcal{I}}} & \mathbf{I}_{\mathcal{I}} & \mathbf{0} \\ \mathbf{H}_{\mathcal{I}} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}. \tag{111}$$

Then for such $\mathbf{c}$, $\mathbf{w}$ is an eigenvector of $\mathbf{E}(\mathbf{c})$ iff $\mathbf{y}^{\mathsf{T}}\mathbf{H}_{\mathcal{I}} = 0$ iff $\mathbf{y} = \widetilde{\mathbf{H}_{\mathcal{I}}}\mathbf{z}$ for some $\mathbf{z} \in \mathbb{F}_2^{m-r}$. Thus, to identify the diagonal Pauli matrices that stabilize $\mathbf{w}$, and consequently the subspaces $\mathbf{H}_{\mathcal{I}}, \widetilde{\mathbf{H}_{\mathcal{I}}}$, it is sufficient to find 2^{m-r} vectors $\mathbf{y} \in \mathbb{F}_2^m$ such that

$$0 \neq \mathbf{w}^{\dagger}\mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w} = \mathbf{w}^{\dagger}\mathbf{E}(\mathbf{0}, \widetilde{\mathbf{H}_{\mathcal{I}}}\mathbf{z})\mathbf{w}. \tag{112}$$

It follows by (59) that the above is equivalent with finding 2^{m-r} vectors $\mathbf{y}$ such that

$$0 \neq \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{y}^{\mathsf{T}}\mathbf{v}}|\mathbf{w}(\mathbf{v})|^2 = \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{z}^{\mathsf{T}}\widetilde{\mathbf{H}}^{\mathsf{T}}\mathbf{v}}|\mathbf{w}(\mathbf{v})|^2. \tag{113}$$

The above is just a Hadamard transform which can be efficiently undone.

With a similar argument, $\mathbf{w}$ is an eigenvector of a general Pauli matrix $\mathbf{E}(\mathbf{x}, \mathbf{y})$ iff

$$\mathbf{w}^{\dagger}\mathbf{E}(\mathbf{x}, \mathbf{y})\mathbf{w} = i^{\mathbf{x}^{\mathsf{T}}\mathbf{y}} \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{v}^{\mathsf{T}}\mathbf{y}}\overline{\mathbf{w}(\mathbf{v}+\mathbf{x})}\mathbf{w}(\mathbf{v}) \neq 0. \tag{114}$$

The above is again just a Hadamard transform. In fact, we see here both the "shift" (by $\mathbf{x}$), the "multiply", and the Hadamard transform of the "shift and multiply". This is the main insight that transfers the shift and multiply technique of [6] to computation with Pauli matrices. By definition, the Pauli matrix $\mathbf{E}(\mathbf{x}, \mathbf{y})$ has a diagonal part determined by $\mathbf{y}$ and an off-diagonal part determined by $\mathbf{x}$. The off-diagonal part of a Pauli determines the shift of coordinates whereas the diagonal part takes care of the rest.

Computing $\mathbf{w}^{\dagger}\mathbf{U}\mathbf{w}$ for a generic $N \times N$ matrix is expensive, and even more so if the same computation is repeated N^2 times. However, when $\mathbf{U}$ is a Pauli matrix, which is a monomial matrix of sparsity 1, the same computation is much faster. Moreover, as we will see, for a rank r BSSC we need not compute all the possible N shifts but only r of them. This is an intuitive observation based on the shape of the maximal stabilizer (110). Indeed, once the diagonal Pauli matrices are identified, one can use that information to search the off-diagonal Pauli matrices only for $\mathbf{x} \in \mathrm{cs}\,(\mathbf{H}_{\mathcal{I}})$, which reduces the search from 2^m to 2^r. In fact, as we will see, instead of 2^r shifts we will need only use the r shifts determined by columns of $\mathbf{H}_{\mathcal{I}}$.

Let us now explicitly make use of (114) to reconstruct the symmetric matrix $\mathbf{S}_r$, while assuming that we have already reconstructed $\mathbf{H}_{\mathcal{I}}, \widetilde{\mathbf{H}_{\mathcal{I}}}$. In this case, as we see from (111), the only missing piece of the puzzle is the upper-left block of $\mathbf{F}^{-1}$. We proceed as follows. For $\mathbf{c} = \begin{bmatrix}\mathbf{x}\\ \mathbf{y}\end{bmatrix}$, we have $\mathbf{w}^{\dagger}\mathbf{E}(\mathbf{x}, \mathbf{y})\mathbf{w} \neq 0$ iff $\mathbf{E}(\mathbf{c}^{\mathsf{T}}\mathbf{F}^{-1})$ is diagonal, iff

$$\mathbf{x}^{\mathsf{T}}[\mathbf{I}_{\mathcal{I}}\mathbf{S}_r \;\; \widetilde{\mathbf{H}_{\mathcal{I}}}] = \mathbf{y}^{\mathsf{T}}[\mathbf{H}_{\mathcal{I}} \;\; \mathbf{0}]. \tag{115}$$

As before, we are interested in $\mathbf{y} \in \mathbb{F}_2^m$ that satisfy (115). First note that solutions to (115) exist only if $\mathbf{x}^{\mathsf{T}}\widetilde{\mathbf{H}_{\mathcal{I}}} = \mathbf{0}$, that is only if $\mathbf{x} = \mathbf{H}_{\mathcal{I}}\mathbf{z}$, $\mathbf{z} \in \mathbb{F}_2^r$. For such $\mathbf{x}$, making use of (13), we conclude that (115) holds iff

$$\mathbf{z}^{\mathsf{T}}\mathbf{S}_r = \mathbf{y}^{\mathsf{T}}\mathbf{H}_{\mathcal{I}}. \tag{116}$$

Solutions of (116) are given by

$$\mathbf{y} = \widetilde{\mathbf{H}_{\mathcal{I}}}\mathbf{v} + \mathbf{I}_{\mathcal{I}}\mathbf{S}_r\mathbf{z}, \quad \mathbf{v} \in \mathbb{F}_2^{m-r}. \tag{117}$$

If we take $\mathbf{z} = \mathbf{f}_i$ - the ith standard basis vector of $\mathbb{F}_2^r$ - we have that $\mathbf{z}^{\mathsf{T}}\mathbf{S}_r$ is the ith row/column of $\mathbf{S}_r$ while $\mathbf{x} = \mathbf{H}_{\mathcal{I}}\mathbf{z}$ is the ith column of $\mathbf{H}_{\mathcal{I}}$.

We collect all these observations in Algorithm 2.

A. Reconstruction of Single BSSC in the Presence of Noise

In order to move towards a multi-user random access scenario, one needs a reliable reconstruction algorithm of noisy BSSCs. For this we consider a signal model

$$\mathbf{s} = \mathbf{w} + \mathbf{n}, \tag{118}$$

where $\mathbf{n}$ is Additive White Gaussian Noise (AWGN). In such instance, the subspace reconstruction, that is, step (2) of Algorithm 2 is a delicate procedure. However, one can proceed as follows. For each $\mathbf{y} \in \mathbb{F}_2^m$ we compute $\mathbf{s}^{\dagger}\mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{s}$ and use it as an estimate of $\mathbf{w}^{\dagger}\mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w}$. We sort these scattered real values in decreasing order and make rank hypothesis, that is,

Algorithm 2 Reconstruction of Single Noiseless BSSC

Input: Unknown BSSC $\mathbf{w}$

1. Compute $\mathbf{w}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w}$ for $\mathbf{y} \in \mathbb{F}_2^m$.
2. Find $\mathbf{H}_\mathcal{I}$ using
$$\mathbf{w}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w} \neq 0 \text{ iff } \mathbf{y}^\mathsf{T} \mathbf{H}_\mathcal{I} = \mathbf{0} \text{ iff } \mathbf{y} \in \mathrm{cs}\,(\widetilde{\mathbf{H}_\mathcal{I}}).$$
3. Construct $\mathbf{P}_\mathcal{I}$ as in (14).
4. $r = \mathrm{rank}\,(\mathbf{H}_\mathcal{I})$.
5. **for** $i = 1, \ldots, r$ do:
6. Compute $\mathbf{w}^\dagger \mathbf{E}(\mathbf{H}_\mathcal{I} \mathbf{f}_i, \mathbf{y})\mathbf{w}$ for $\mathbf{y} \in \mathbb{F}_2^m$.
7. Determine the ith row of $\mathbf{S}_r$ using (117).
8. **end for**
9. Dechirp $\mathbf{w}$ to find $\mathbf{b}$.

Output: $r, \mathbf{S}_r, \mathbf{P}_\mathcal{I}, \mathbf{b}$.

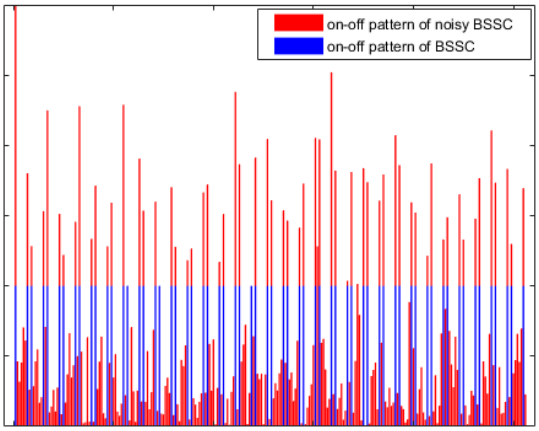

Fig. 4. On-off pattern of noisy BSSC versus on-off pattern of noiseless BSSC.

for each $0 \leq r \leq m$ we select 2^{m-r} largest values *that form a subspace of rank r*, and then proceed with Algorithm 2 to obtain $\mathbf{w}_r$. We then select the best rank using the Euclidean norm:

$$\widetilde{\mathbf{w}} = \arg\min_r \|\mathbf{s} - \mathbf{w}_r\|_2. \tag{119}$$

In Figure 4 we see an instance of a rank $r = 2$ BSSC on-off pattern in $N = 2^8$ dimensions, with and without noise. In this case $\mathbf{w}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w}$ is non-zero $2^{m-r} = 64$ times. In this instance, only 94% of the 64 highest $\mathbf{s}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{s}$ values of the noisy version match the on-off pattern of $\mathbf{w}$. However, this can be overcame in recusntruction by using the fact that the on-off pattern is determined by a subspace. Thus one can build up $\widetilde{\mathbf{H}_\mathcal{I}}$ in a greedy manner by starting with the highest values and then including linear combinations. This strategy was tested in [22] with Monte-Carlo simulations yielding low error rates even for low Signal-to-Noise Ratio (SNR); see [22, Fig. 1]. There it was observed that, rather remarkably, BSSCs outperform BCs despite having the same minimum distance.

VI. Multi-BSSC Reconstruction

The strategy of noisy single BSSC reconstruction can be used as a guideline to generalize Algorithm 2 to decode multiple simultaneous transmissions in a block fading multi-user scenario

$$\mathbf{s} = \sum_{\ell=1}^{L} h_\ell \mathbf{w}_\ell + \mathbf{n}. \tag{120}$$

Here the channel coefficients h_ℓ are $\mathcal{CN}(0, 1)$, with neither phase nor amplitude known, and $\mathbf{w}_\ell$ are BSSCs. Noise $\mathbf{n}$ may be added, depending on the scenario. This model represents, e.g., a random access scenario, where L randomly chosen active users transmit a signature sequence, and the receiver should identify the active users. In such application, the channel gain is not known at the receiver, and thus one cannot use the amplitude to transmit information. For this reason, the amplitude/norm is assumed, without loss of generality, to be one. Additionally, the channel phase is also not known at the receiver and should not carry any information. Thus without loss of generality, the codewords can be assumed to come from a Grassmannian codebook, such as $\mathcal{V}_{\mathrm{BC}}$ or $\mathcal{V}_{\mathrm{BSSC}}$.

We generalize the single-user algorithm to a multi-user algorithm, where the coefficients h_ℓ are estimated to identify the most probable transmitted signals. For this, we use Orthogonal Matching Pursuit (OMP), which is analogous with the strategy of [6]. We assume that we know L.

The estimated error probability of single user transmission for $L = 2, 3$ is given in Figure 5. For the simulation, the rank r is selected in a weighted manner, according to the relative size of rank r BSSCs (recall that there are $2^m \cdot \binom{m}{r}_2 \cdot 2^{r(r+1)/2}$ rank r BSSCs). Whereas, within a given rank, BSSCs are chosen uniformly. We compare the results with BC codebooks and random codebooks with the same cardinality. For random codebooks, steps (2)-(5) of Algorithm 3 are substituted with exhaustive search (which is infeasible is beyond $m = 6$).

The erroneous reconstructions of Algorithm 3 come in part from steps (3)-(4). Specifically, from the cross-terms of

$$\mathbf{s}^\dagger \mathbf{s} = \sum_{\ell=1}^{L} |h_\ell|^2 \|\mathbf{w}_\ell\|^2 + \sum_{i \neq \ell} \overline{h_i} h_\ell \mathbf{w}_i^\dagger \mathbf{w}_\ell. \tag{121}$$

Algorithm 3 Reconstruction of Noiseless Multi-BSSCs

Input: Signal $\mathbf{s}$ as in (120).

1. **for** $\ell = 1 : L$ do
2. **for** $r = 0 : m$ do
3. Greedily construct the $m - r$ dimensional subspace $\widetilde{\mathbf{H}_\mathcal{I}}$ using the highest values of $|\mathbf{s}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{s}|$.
4. Estimate $\widetilde{\mathbf{w}}_r$ as in Alg. 2.
5. **end for**
6. Select the best estimate $\widetilde{\mathbf{w}}_\ell$.
7. Determine $\widetilde{h}_1, \ldots, \widetilde{h}_\ell$ that minimize
$$\left\| \mathbf{s} - \sum_{j=1}^{\ell} h_j \widetilde{\mathbf{w}}_j \right\|_2.$$
8. Reduce $\mathbf{s}$ to $\mathbf{s}' = \mathbf{s} - \sum_{j=1}^{\ell} \widetilde{h}_j \widetilde{\mathbf{w}}_j$.
9. **end for**

Output: $\widetilde{\mathbf{w}}_1, \ldots, \widetilde{\mathbf{w}}_L$.

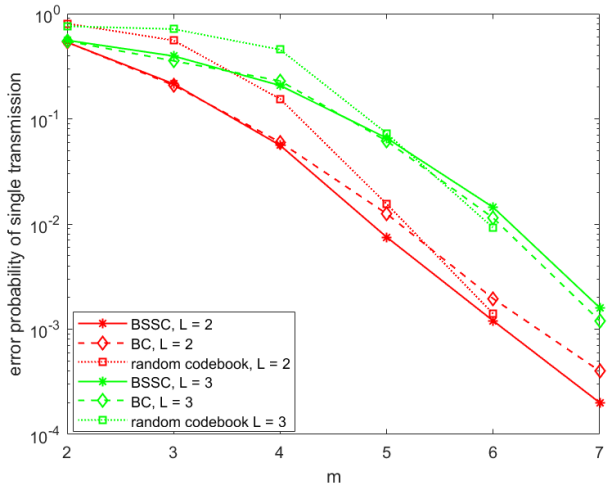

Fig. 5. Error probability of Algorithm 3 on absence of noise. Random codebook included for comparison.

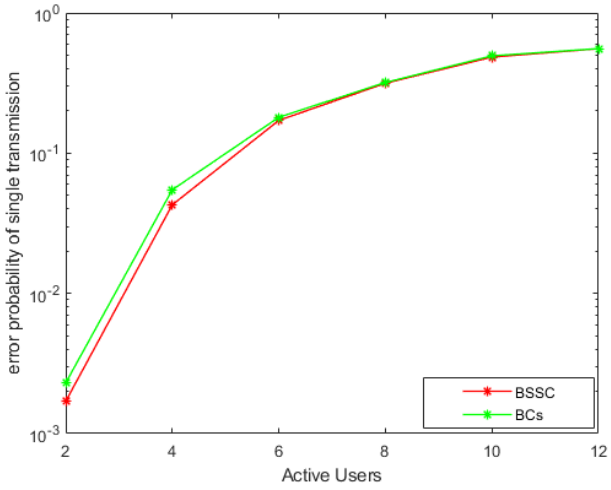

Fig. 7. Error probability of Algorithm 3 for noisy multi-user transmission in $N = 256$ dimensions and SNR $= 30$ dB.

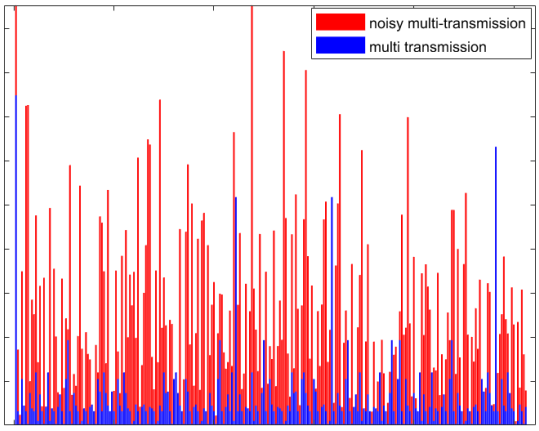

Fig. 6. On-off pattern of a noiseless vs. noisy linear combination of BSSCs.

For BCs, these cross-terms are the well-behaved *second order Reed-Muller functions*. The BSSCs, unlike the BCs [29], do not form a group under point-wise multiplication (Theorem 4), and thus the products $\mathbf{w}_i^\dagger \mathbf{w}_\ell$ are more complicated. Indeed, when two BSSCs of different ranks and/or different on-off patterns are multiplied coordinate-wise (which we do during the "shift and multiply") the resulting BSSCs could be potentially very different (if not zero) as described in Theorem 4. In addition, linear combinations of BSSCs (120) may perturb the on-off patterns of the constituents, and depending on the nature of the channel coefficients h_ℓ, the algorithm may detect a higher rank BSSC in $\mathbf{s}$. If the channel coefficients of two BSSCs happen to have similar amplitudes, the algorithm may detect a lower rank BSSC that corresponds to the overlap of the on-off patterns of the BSSCs. These phenomena are depicted in Figure 6 (in blue) in which the on-off pattern of a linear combination of a rank two, a rank three, and a rank six BSSCs in $N = 2^8$ dimensions is displayed. There, we see multiple levels (in blue) of $\mathbf{s}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{s}$, only some of which correspond to actual on-off patterns $\mathbf{w}_\ell^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{w}_\ell$ of the given BSSCs, and the rest corresponds to different combinations of overlaps. The problem for multi-BSSC reconstruction caused by these phenomena is alleviated by the fact that most BSSC codewrods have high rank. E.g., as m grows, it follows by Theorem 1 that about 42% of BSSCs are BCs. Low rank BSSCs are very unlikely in (120).

Despite these phenomena affecting BSSC on-off patterns in multi-BSSC scenarios, a decoding algorithm like the one discussed is able to distinguish different levels and provide reliable performance. It is worth mentioning that by comparing Figure 5 with [22, Fig. 1] we see that the interference of BSSCs is much more benign than general AWGN, which in turn explains the reliable reconstruction of noiseless multi-user transmission.

Interestingly, even in this multi-user scenario, we see that BSSCs outperform BCs. With increasing m, the performance benefit of the algebraically defined codebook over random codebooks diminishes. However, the decoding complexity remains manageable for the algebraic codebooks.

In [22] it was demonstrated that reconstruction of a single noisy BSSC was possible even for low SNR. We have performed preliminary simulations and have tested Algorithm 3 on a noisy multi-user transmission. Unlike the single BSSC scenario, the multi BSSCs scenario requires a higher SNR regime for reliable performance. In Figure 6 we have shown (in red) $|\mathbf{s}^\dagger \mathbf{E}(\mathbf{0}, \mathbf{y})\mathbf{s}|$ for a noisy version of the same linear combination as before (displayed in blue). In this instance we have fixed SNR $= 8$ dB. A close look shows that this scenario is different from the single user scenario displayed in Figure 4. In this instance, even an exhaustive search over ranks r as in Algorithm 3 produces an on-off pattern that matches at most 61% *any* actual on-off pattern, and thus the subspace reconstruction inevitably fails. On the other hand, if the on-off pattern is reconstructed correctly, then the corresponding r-dimensional BC can be reconstructed reliably. When noise is on manageable level, reliable reconstruction of multi-user BSSCs is possible with Algorithm 3. In Figure 7, we depict the performance of $N = 256$ BSSC and BCs in a scenario

with SNR 30 dB, for a varying number of simultaneously transmitting users. Again, we see that BSSCs provide slightly better error performance than BCs, despite the codebook being larger.

VII. Conclusion and Future Research

Algebraic and geometric properties of BSSCs are described in details. BSSCs are characterized as common eigenspaces of maximal sets of commuting Pauli matrices, or equivalently, as columns of Clifford matrices. This enables us to fully exploit connections between symplectic geometry and quantum computation, which in turn yield considerable complexity reductions. Further, we have developed a low complexity decoding algorithm for multi BSSCs transmission with low error probability.

By construction, BSSCs inherit all the desirable properties of BCs, while having a higher cardinality. In wireless communication scenarios BSSCs exhibit slightly lower error probability than BCs. For these reasons we think that BSSCs constitute good candidates for a variety of applications.

Algorithm 3 is a generalization of the BC decoding algorithm of [6] to BSSCs. As pointed out in [12], the decoding algorithm of [6] does not scale well in a multi-user scenario, in terms of the number of users supported as a function of codeword length. In [12], [25] slotting arrangements were added on top of BC codes to increase the length, and the number of supported users. Part of the information in a transmission is embedded in the choice of a BC, part in the choice of active slots. In [12], interference cancellation across slots is applied, and the discussed scheme can be considered a combination of physical layer (PHY) BC coding, and a Medium Access Control (MAC) Layer code of the type discussed in [52]. The works of [12], [25] show that following such principles, practically implementable massive random access schemes, operating in the regime of interest of [13], can be designed. If the small-m BC-transmissions in the slots would be replaced with BSSC transmissions with the same m, the results of this paper indicate that performance per slot would be the same, if not slightly better than in [12], [25]. This indicates that combined MAC/PHY codes, where BSSC would be the PHY component instead of BC as used in [12], [25], are likely to provide slightly higher rates with otherwise similar performance as [12], [25]. In future work, we plan to investigate such codes.

As mentioned, we have seen in all our simulations that BSSCs outperform BCs. Although our algorithms do not find the closest codeword, this may be due to a fact that BSSCs have fewer closest neighbors on average than BCs. We will investigate this in future work with a statistical analysis of Algorithm 3 along the lines of [29].

Binary chirps have been generalized in various works to prime dimensions, and recently to non-prime dimensions [53]. In future work we will consider analogues generalizations of BSSCs, by adding a sparsity component to generalized BCs and/or by lifting BSSCs modulo $2t$.

As a byproduct, we have obtained a Bruhat decomposition of the symplectic group that involves five elementary symplectic matrices (compared to the seven layers of [34], c.f., (32)). We think that this has implications in quantum computation. In future research we will explore whether Algorithm 1 can be leveraged to improve upon [33], [54].

Acknowledgment

The authors would like to thank Narayanan Rengaswamy for helpful discussions.

References

[1] T. Pllaha, O. Tirkkonen, and R. Calderbank, "Reconstruction of multi-user binary subspace chirps," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 531–536.

[2] P. Viswanath and V. Anantharam, "Optimal sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1984–1991, Sep. 1999.

[3] D. J. Love, R. W. Heath, Jr., and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

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

[5] R. A. DeVore, "Deterministic constructions of compressed sensing matrices," *J. Complex.*, vol. 23, nos. 4–6, pp. 918–925, 2007.

[6] S. D. Howard, A. R. Calderbank, and S. J. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed–Müller codes," in *Proc. IEEE Conf. Inf. Sci. Syst.*, Mar. 2008, pp. 11–15.

[7] S. Li and G. Ge, "Deterministic sensing matrices arising from near orthogonal systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2291–2302, Apr. 2014.

[8] G. Wang, M.-Y. Niu, and F.-W. Fu, "Deterministic constructions of compressed sensing matrices based on codes," *Cryptography Commun.*, vol. 11, no. 4, pp. 759–775, Sep. 2018.

[9] A. Thompson and R. Calderbank, "Compressed neighbour discovery using sparse Kerdock matrices," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 2286–2290.

[10] D. Guo and L. Zhang, "Virtual full-duplex wireless communication via rapid on-off-division duplex," in *Proc. 48th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2010, pp. 412–419.

[11] C.-R. Tsai and A.-Y. Wu, "Structured random compressed channel sensing for millimeter-wave large-scale antenna systems," *IEEE Trans. Signal Process.*, vol. 66, no. 19, pp. 5096–5110, Oct. 2018.

[12] R. Calderbank and A. Thompson, "CHIRRUP: A practical algorithm for unsourced multiple access," *Inf. Inference, A, J. IMA*, vol. 9, no. 4, pp. 875–897, Dec. 2020.

[13] Y. Polyanskiy, "A perspective on massive random-access," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 2523–2527.

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

[15] S. S. Kowshik, K. Andreev, A. Frolov, and Y. Polyanskiy, "Energy efficient random access for the quasi-static fading MAC," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 2768–2772.

[16] S. S. Kowshik, K. Andreev, A. Frolov, and Y. Polyanskiy, "Short-packet low-power coded access for massive MAC," in *Proc. 53rd Asilomar Conf. Signals, Syst., Comput.*, Nov. 2019, pp. 827–832.

[17] A. Glebov, L. Medova, P. Rybin, and A. Frolov, "On LDPC code based massive random-access scheme for the Gaussian multiple access channel," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, O. Galinina, S. Andreev, S. Balandin, and Y. Koucheryavy, Eds. Cham, Switzerland: Springer, 2018, pp. 162–171.

[18] A. Vem, K. R. Narayanan, J.-F. Chamberland, and J. Cheng, "A user-independent successive interference cancellation based coding scheme for the unsourced random access Gaussian channel," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8258–8272, Dec. 2019.

[19] A. Fengler, G. Caire, P. Jung, and S. Haghighatshoar, "Massive MIMO unsourced random access," 2019, *arXiv:1901.00828*.

[20] S. S Kowshik and Y. Polyanskiy, "Fundamental limits of many-user MAC with finite payloads and fading," 2019, *arXiv:1901.06732*.

[21] 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, no. 2, pp. 283–290, Mar. 2009.

[22] O. Tirkkonen and R. Calderbank, "Codebooks of complex lines based on binary subspace chirps," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.
[23] Q. Qiu, A. Thompson, R. Calderbank, and G. Sapiro, "Data representation using the Weyl transform," *IEEE Trans. Signal Process.*, vol. 64, no. 7, pp. 1844–1853, Apr. 2016.
[24] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A, Gen. Phys.*, vol. 68, Oct. 2003, Art. no. 042318.
[25] P. Yang, D. Guo, and H. Yang, "Massive access in multi-cell wireless networks using Reed-Muller codes," 2020, *arXiv:2003.11568*.
[26] G. E. Andrews, *Q-Series: Their Development and Application in Analysis, Number Theory, Combinatorics, Physics, and Computer Algebra* (CBMS Regional Conference Series in Mathematics), vol. 66. Providence, RI, USA: American Mathematical Society, 1986.
[27] D. Slepian, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, no. 4, pp. 575–602, Apr. 1968.
[28] M. Thill and B. Hassibi, "Low-coherence frames from group Fourier matrices," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3386–3404, Jun. 2017.
[29] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of matrices satisfying a statistical isometry property," *IEEE J. Sel. Topics Signal Process., Special Issue Compressive Sens.*, vol. 4, no. 2, pp. 358–374, Feb. 2010.
[30] T. Can, N. Rengaswamy, R. Calderbank, and H. D. Pfister, "Kerdock codes determine unitary 2-Designs," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6104–6120, Oct. 2020.
[31] N. Bourbaki, *Elements of Mathematics—Lie Groups and Lie Algebras*. Berlin, Germany: Springer, 1968, chs. 4–6.
[32] R. R. Rao, "On some explicit formulas in the theory of Weil representation," *Pacific J. Math.*, vol. 157, no. 2, pp. 335–371, Feb. 1993.
[33] D. Maslov and M. Roetteler, "Shorter stabilizer circuits via Bruhat decomposition and quantum circuit transformations," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 4729–4738, Jul. 2018.
[34] T. Can, "The Heisenberg-Weyl group, finite symplectic geometry, and their applications," Senior thesis, Dept. Math., Duke University, Durham, NC, USA, May 2018.
[35] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Synthesis of logical Clifford operators via symplectic geometry," in *Proc. IEEE ISIT*, Jun. 2018, pp. 791–795.
[36] A. K. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett*, vol. 78, nos. 3–20, pp. 405–408, 1997.
[37] A. K. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[38] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. thesis, Division Phys., Math. Astron., California Inst. Technol., Pasadena, CA, USA, 1997.
[39] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[40] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.
[41] O. Tirkkonen, C. Boyd, and R. Vehkalahti, "Grassmannian codes from multiple families of mutually unbiased bases," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 789–793.
[42] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," 2009, *arXiv:0904.2557*.
[43] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Logical Clifford synthesis for stabilizer codes," *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–17, 2020.
[44] S. Bravyi and D. Maslov, "Hadamard-free circuits expose the structure of the Clifford group," 2020, *arXiv:2003.09412*.
[45] R. Steinberg, "Generators for simple groups," *Can. J. Math.*, vol. 14, no. 2, pp. 277–283, 1962.
[46] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Phys. Rev. A, Gen. Phys.*, vol. 70, no. 5, Nov. 2004, Art. no. 052328.
[47] T. Pllaha, N. Rengaswamy, O. Tirkkonen, and R. Calderbank, "Un-Weyl-ing the Clifford hierarchy," *Quantum*, vol. 4, p. 370, Dec. 2020, doi: 10.22331/q-2020-12-11-370.
[48] T. Pllaha, K. Volanto, and O. Tirkkonen, "Decomposition of Clifford gates," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 01–06.
[49] P. Delsarte and J. M. Goethals, "Alternating bilinear forms over GF(q)," *J. Combinat. Theory A*, vol. 19, no. 1, pp. 26–50, Jul. 1975.
[50] 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. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.
[51] R. Calderbank and S. Jafarpour, "Reed–Müller sensing matrices and the LASSO," in *Sequences and Their Applications*, C. Carlet and A. Pott, Eds. Berlin, Germany: Springer, 2010, pp. 442–463.
[52] G. Liva, "Graph-based analysis and optimization of contention resolution diversity slotted ALOHA," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 477–487, Feb. 2011.
[53] R.-A. Pitaval and Y. Qin, "Grassmannian frames in composite dimensions by exponentiating quadratic forms," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 13–18.
[54] R. Koenig and J. A. Smolin, "How to efficiently select an arbitrary Clifford group element," *J. Math. Phys.*, vol. 55, no. 12, Dec. 2014, Art. no. 122202.

Tefjol Pllaha received the B.Sc. and M.Sc. degrees in mathematics from the University of Tirana, Albania, in 2009 and 2011, respectively, and the Ph.D. degree in mathematics from the University of Kentucky, Lexington, KY, USA, in 2019. He is currently a Post-Doctoral Faculty at the Department of Mathematics, University of Nebraska, Lincoln, USA. Before that, he was a Post-Doctoral Researcher at the Department of Communications and Networking, Aalto University, Finland. His current research interests are in aspects of wireless communication and quantum computation.

Olav Tirkkonen (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in theoretical physics from the Helsinki University of Technology in 1990 and 1994, respectively. After post-doctoral positions at UBC, Vancouver, Canada, and NORDITA, Copenhagen, Denmark, he was with the Nokia Research Center (NRC), Helsinki, Finland, from 1999 to 2010. In 2016–2017, he was a Visiting Associate Professor at Cornell University, Ithaca, NY, USA. He is currently a Full Professor in communication theory at Aalto University, Finland, where he has been holding a faculty position since 2006. He has published some 300 papers and is the inventor of some 85 families of patents and patent applications which include 1% of all patents declared essential for the first standardized version of 4G LTE. His current research interests are in coding for random access and quantization, quantum computation, and machine learning for cellular networks. He is an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Robert Calderbank (Life Fellow, IEEE) received the B.S. degree in mathematics from Warwick University, U.K., in 1975, the M.S. degree in mathematics from Oxford University, U.K., in 1976, and the Ph.D. degree in mathematics from the California Institute of Technology in 1980.

He is currently a Professor of electrical and computer engineering with Duke University, where he directs the Rhodes Information Initiative at Duke (iiD). Prior to joining Duke in 2010, he was with Princeton University, where he directed the Program in Applied and Computational Mathematics. Prior to joining Princeton in 2004, he was the Vice President of research at AT&T. At the start of his career with Bell Labs, he developed signal processing methods that were incorporated in a progression of voiceband modem standards that moved communications practice close to the Shannon limit. Together with Peter Shor and colleagues at AT&T Labs, he developed the mathematical framework for quantum error correction. He is an inventor of space-time codes for wireless communication, where correlation of signals across different transmit antennas is the key to reliable transmission. He was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2006 to 2008. He has received the IEEE Information Theory Prize Paper Award in 1995 for his work on the Z4 linearity of Kerdock and Preparata Codes (joint with A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane, and P. Sole) and in 1999 for the invention of space-time codes (joint with V. Tarokh and N. Seshadri). He has received the 2006 IEEE Donald G. Fink Prize Paper Award, the IEEE Millennium Medal, the 2013 IEEE Richard W. Hamming Medal, and the 2015 Shannon Award. He was elected to the U.S. National Academy of Engineering in 2005. He has served as an Associate Editor for Coding Techniques from 1986 to 1989 and the Editor-in-Chief for IEEE TRANSACTIONS ON INFORMATION THEORY from 1995 to 1998.