Grassmannian Codes from Multiple Families of Mutually Unbiased Bases

Olav Tirkkonen[1,2], Christopher Boyd[1] and Roope Vehkalahti[1]
[1]School of Electrical Engineering, Aalto University, Finland
[2]School of Electrical and Computer Engineering, Cornell University, NY, USA
e-mail: {olav.tirkkonen,christopher.boyd,roope.vehkalahti}@aalto.fi

***Abstract*—We explore the underlying algebraic structure of Mutually Unbiased Bases (MUBs), and their application to code design. Columns in MUBs have inner products with absolute values less or equal to $1/\sqrt{N}$. MUBs provide a systematic way of generating optimal codebooks for various coding and precoding applications. A maximal set of MUBs (MaxMUBs) in $N = 2^m$ dimensions, with $m \in \mathbb{Z}$, can produce codebooks of QPSK lines with good distance properties and alphabets which limit processing complexity. We expand the construction by identifying that in $N = 2^m$ dimensions there exists $N^{(m-1)/2}$ families of MUB, each with N matrices. Inner products of columns of these matrices are less or equal to $1/\sqrt{2}$. As an example, we construct Grassmannian line codes from the columns of these matrices. Then decoding or encoding these codebooks can be performed without multiplications, and with a number of additions that scales linearly with the number of codewords, irrespectively of the dimension.**

I. Introduction

Two $N \times N$ unitary matrices, i.e. bases in $\mathbb{C}^N$, are *Mutually Unbiased* if the absolute value of the inner product of any columns of the matrices is $1/\sqrt{N}$. Thus if $\mathbf{M}_1$ and $\mathbf{M}_2$ are unbiased, we have

$$\left|\mathbf{M}_1^{\mathrm{H}}\mathbf{M}_2\right| = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{bmatrix} , \qquad (1)$$

i.e. all the entries in the inner product matrix have norm $1/\sqrt{N}$. Collections of matrices which are all pairwise mutually unbiased can be called Mutually Unbiased Bases (MUBs).

MUBs have a central role in quantum information theory (see [1] for a recent review), and can be applied in many information processing problems, such as in the design of codes on projective spaces [2], and compressive sensing [3]. Codes on projective spaces can be used either for channel coding, e.g. as space-time [4] or random access codes [5], for network coding [6], or for source coding, such as vector quantization for precoding in (MIMO) systems [7].

In dimensions $N = p^m$ that are powers of a prime p, it is known that the maximum set of MUBs (MaxMUB) consists of $N + 1$ unitary $N \times N$ matrices [8]. Prime power MUBs can be systematically constructed from finite fields in two different ways. In [2], a construction based on $\mathbb{Z}_4$ quadratic forms was presented for powers of $p = 2$, whereas in [9], MUBs for generic prime powers were constructed from eigenspaces of commuting operators. Alternatively, MUBs can be generated as a multiplicative group arising from powers of a $N + 1$st root of unity generator matrix [10]. Based on these constructions, multiple quantum information problems can be approached [1], and Grassmannian codes of different ranks can be constructed [11].

The motivation for this paper is in code construction, and we concentrate on dimensions $N = 2^m$. Codes on projective spaces (e.g. Grassmannians) can be constructed in a natural way from MUBs. The reasons for this are that the property of unbiasedness between two matrices is preserved under arbitrary column rotations, and that unbiasedness sets specific conditions on the absolute value of inner products of columns of matrices, which gives a direct relation to chordal distance properties of sets of columns of MUBs.

Codes arising from MUBs are intriguing from the perspective that they are, in many cases, either optimal or the best known codes for their parameters. Also, they have the interesting characteristic that MUBs can be constructed so that all entries are $2p$th roots of unity. In particular this means that in dimensions that are powers of 2, codebooks with 4ary entries from Quaternary Phase Shift Keying (QPSK) alphabets can be constructed. Such codes are desirable from implementation perspective. In systems where encoding and/or decoding is performed real-time in hardware, such as MIMO precoding and digital communication, implementation complexity is an issue. Filtering with codebooks having only QPSK entries can be performed only by additions, and shifts of real and imaginary parts of numbers, without using any multiplications in $\mathbb{R}$.

Codes that are constructed as subsets of MUBs have the apparent drawback, however, that they have a rather low cardinality. Here, we seek to improve on this. We expand from maximal MUBs, which in dimensions $N = 2^m$ consist of N matrices with 4-ary entries, to collections of $N^{(m+1)/2}$ matrices which consist of $N^{(m-1)/2}$ families of N MUBs.

As an example of codes that can be constructed from these families of MUBS, we consider the collection of Grassmannian lines that are columns of these MUBs. There are $N^{(m+3)/2}$ such lines, and minimum they have chordal distance $1/\sqrt{2}$ irrespectively of the dimensionality. They have intriguing similarity with rank-1 operator Reed-Muller codes of [12].

II. Underlying Extraspecial Group

For simplicity, we concentrate on dimensions $N = 2^m$ that are powers of 2. In these dimensions, one can generate codebooks from MUBs with entries that are normalized fourth roots of unity, i.e. in the set $\mathcal{Q} = \{\pm 1, \pm \mathrm{i}\}/\sqrt{N} \sim \mathbb{Z}_2^2$. Such codebooks are particularly beneficial from an implementation perspective, as multiplication in $\mathcal{Q}$ can be realized simply as a shift operation. This can be used to significantly reduce decoding in channel coding applications, and encoding in source coding.

MUBs can be generated in the algebra of Weyl operators, which for $m = 2$ can be represented in a particularly simple form as Pauli matrices. We have the 2D matrices

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \ , \quad \sigma_y = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \ , \tag{2}$$

which fulfill the defining anti-commutation relation

$$\sigma_x \sigma_y = -\sigma_y \sigma_x \ , \tag{3}$$

and square to identity, $\sigma_x^2 = \sigma_y^2 = \mathbf{I}_2$. Corresponding to the binary vectors

$$\mathbf{c} = \begin{bmatrix} a & b \end{bmatrix}^{\mathrm{T}} \in \mathbb{F}_2^2 \tag{4}$$

we have the matrices

$$\mathbf{E}(\mathbf{c}) = \sigma_x^a \sigma_y^b \ , \tag{5}$$

so that the eight matrices $\{\pm \mathbf{E}(\mathbf{c}) \mid \mathbf{c} \in \mathbb{F}_2^2\}$ form a 2D fundamental representation of the (extraspecial) quaternion group. As we are interested in codebooks with complex-valued entries, we extend to the 16-element Weyl/Pauli group by multiplying with powers of i. The matrices

$$\mathbf{X}(\mathbf{c}) = \mathrm{i}^{-ab} \sigma_x^a \sigma_y^b \tag{6}$$

are Hermitian by definition, and form an Frobenius-orthogonal basis of the algebra of 2×2 Hermitian matrices. Extending to $N = 2^m$ dimensions, we get higher dimensional extra-special/Weyl/Pauli groups as m-fold tensor products of the 2D groups, see [2], [12]. The elements are indexed by vectors

$$\mathbf{c} = \begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix} \ , \quad \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m \ , \tag{7}$$

so that

$$\mathbf{E}(\mathbf{c}) = \sigma_x^{a_1} \sigma_y^{b_1} \otimes \sigma_x^{a_2} \sigma_y^{b_2} \otimes \ldots \otimes \sigma_x^{a_m} \sigma_y^{b_m} \tag{8}$$

have real entries and $\pm \mathbf{E}$ are the elements in the extraspecial group, whereas

$$\mathbf{X}(\mathbf{c}) = \mathrm{i}^{-\mathbf{a}^{\mathrm{T}}\mathbf{b}} \mathbf{E}(\mathbf{c}) \tag{9}$$

are Hermitian.

Note that the vector $\mathbf{a}$ encodes the diagonality stucture of $\mathbf{X}$ (and $\mathbf{E}$). Each $\mathbf{X}$ has precisely $N = 2^m$ non-zero elements. If $a_k = 0$, the kth tensor product component is diagonal; if $a_k = 1$, it is offdiagonal. Thus if $\mathbf{a} = \mathbf{0}$, the resulting $\mathbf{X}$ is diagonal, and if $\mathbf{a} = \mathbf{1}$, it is fully offdiagonal. The values of the non-zero elements are determined by the vector $\mathbf{b}$.

From (3) it follows that

$$\mathbf{E}(\mathbf{c}_1)\mathbf{E}(\mathbf{c}_2) = (-1)^{\mathbf{a}_2^{\mathrm{T}}\mathbf{b}_1} \mathbf{E}(\mathbf{c}_1 \oplus \mathbf{c}_2) \ , \tag{10}$$

where $\oplus$ indicates the modulo-2 sum in $\mathbb{F}_2$. Furthermore, we have the commutation relations

$$\begin{aligned} \mathbf{E}(\mathbf{c}_1)\mathbf{E}(\mathbf{c}_2) &= (-1)^{\mathbf{a}_2^{\mathrm{T}}\mathbf{b}_1 + \mathbf{a}_1^{\mathrm{T}}\mathbf{b}_2} \mathbf{E}(\mathbf{c}_2)\mathbf{E}(\mathbf{c}_1) \\ &\equiv (-1)^{\mathbf{c}_1 * \mathbf{c}_2} \mathbf{E}(\mathbf{c}_2)\mathbf{E}(\mathbf{c}_1) \ , \end{aligned} \tag{11}$$

where $\mathbf{c}_1 * \mathbf{c}_2 = \mathbf{a}_2^{\mathrm{T}}\mathbf{b}_1 \oplus \mathbf{a}_1^{\mathrm{T}}\mathbf{b}_2 \in \mathbb{F}_2$ is the *symplectic* inner product of the vectors $\mathbf{c}_1$ and $\mathbf{c}_2$. Thus two matrices $\mathbf{E}(\mathbf{c}_1)$ and $\mathbf{E}(\mathbf{c}_2)$ commute if $\mathbf{c}_1 * \mathbf{c}_2 = 0$. The same holds for their Hermitian counterparts $\mathbf{X}(\mathbf{c}_1)$ and $\mathbf{X}(\mathbf{c}_2)$.

The 2^{2m} matrices $\mathbf{X}$ form a Frobenius-orthogonal basis for the vector space of $2^m \times 2^m$-dimensional Hermitian matrices. This is a very specific basis, as all $\mathbf{X}$:s are unitary by construction, and thus square to $\mathbf{I}_N$. Moreover, each $\mathbf{a} \in \mathbb{F}_2^m$ characterizes a unique *diagonality subspace* in this algebra. There are $N = 2^m$ such diagonality subspaces, each defines a set of 2^m matrix elements that may be non-zero, and these sets do not overlap for different subspaces.

III. GF_2 Description of MUBs

In $N = 2^m$ dimensions, there are $N+1$ MUBs [8]. Without loss of generality, one of these can be taken to be the identity matrix. As a consequence of (1), all the remaining ones are such that all their entries have norm $1/\sqrt{N}$. They can always be chosen so that all entries are in $\mathcal{Q}$, which can be seen by direct construction. Accordingly, maximal sets $\mathcal{M}_{\max}$ of MUBs exist, which consist of the identity matrix $\mathbf{M}_0 = \mathbf{I}_N$, and a set $\widetilde{\mathcal{M}}_{\max}$ of N matrices with entries in $\mathcal{Q}$.

The matrices $\mathbf{M}_k$ in a collection of MUBs can be constructed from families of commuting $N \times N$ matrices. A set of commuting matrices can, according to (11), be generated from sets of $N+1$ vectors $\mathbf{c}_n \in \mathbb{F}_2^{2m}$ which are all mutually orthogonal w.r.t. the symplectic inner product [2], [9]. Thus a basis matrix $\mathbf{M}_k$ can be characterized by a binary $(2m) \times m$ matrix $\mathbf{C}_k$, which is orthogonal w.r.t. $*$.

A concrete example is given in [9]. Choosing the first matrix $\mathbf{M}_0$ to be identity, the corresponding $\mathbf{C}_0^{\mathrm{T}} = \begin{bmatrix} \mathbf{0}_{m \times m} & \mathbf{I}_m \end{bmatrix}$. The other matrices can then be taken to be

$$\mathbf{C}_k^{\mathrm{T}} = \begin{bmatrix} \mathbf{I}_m & \mathbf{B}_k \end{bmatrix} \ , k = 1, \ldots, N \ . \tag{12}$$

When the $m \times m$ binary matrix $\mathbf{B}_k$ is symmetric, the columns of $\mathbf{C}_k$ are symplectic orthogonal. Moreover, if all the $\mathbf{B}_k$ are linearly independent, such that $\mathbf{B}_k \oplus \mathbf{B}_l$ is invertible for $k \neq l$, the constructed matrices are MUB. In [8] it was shown that the maximal size of a set of linearly independent matrices $\mathbf{B}_k$ is N, and sets of N linearly independent symmetric matrices exist. Thus one can characterize a maximal family of MUBs $\mathcal{M}_{\max}$ by the set $\{\mathbf{C}_k\}_{k=0}^N$.

Each $\mathbf{C}$ has m columns $\mathbf{c}_l$, $l = 1, \ldots, m$. Using these in (9) one gets m matrices $\mathbf{X}(\mathbf{c}_l)$, which all commute. Considering the 2^m binary vectors $\mathbf{d} \in \mathbb{F}_2^m$ one can then construct 2^m matrices $\mathbf{X}(\mathbf{c}_1)^{d_1}\mathbf{X}(\mathbf{c}_2)^{d_2} \ldots \mathbf{X}(\mathbf{c}_m)^{d_m}$. By construction, these are proportional to $\mathbf{X}(\mathbf{C}\mathbf{d})$, and they all commute. In [9],

the MUB-matrices $\mathbf{M}_k$ were constructed as the common eigenspaces of these commuting matrices.

In order to formulate the generalization of interest of this paper, we depart from [9], [12] at this point, and construct MUBs directly from the $\mathbf{X}$-matrices. This is also a departure from [12], where codes were constructed from eigenspaces of the $\mathbf{X}$s. Constructing matrices directly has the benefit that we have full control over the entries of the resulting codebooks, as no eigendecomposition has to be performed.

From the m commuting Hermitian matrices $\mathbf{X}(\mathbf{c}_k)$, one may construct the unitary matrix

$$\begin{aligned}\mathbf{M} &= \prod_{k=1}^{m} \frac{1}{\sqrt{2}}\big(\mathbf{I}_N + \mathrm{i}\,\mathbf{X}(\mathbf{c}_k)\big) && (13)\\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{d}\in\mathbb{F}_2^m} \mathrm{i}^{\Sigma\mathbf{d}}\, \mathbf{X}(\mathbf{c}_1)^{d_1}\mathbf{X}(\mathbf{c}_2)^{d_2}\ldots\mathbf{X}(\mathbf{c}_m)^{d_m} && (14)\\ &= \frac{1}{\sqrt{N}} \sum_{\mathbf{d}\in\mathbb{F}_2^m} \mathrm{i}^{\mathbf{d}^{\mathrm{T}}(\mathbf{I}_m+\widetilde{\mathbf{B}})\mathbf{d}}\, \mathbf{E}\left(\mathbf{C}\mathbf{d}\right)\ . && (15)\end{aligned}$$

This is unitary by construction, as the $\mathbf{X}$s are Hermitian, commute, and square to identity. We have used the shorthand $\Sigma\mathbf{d} \equiv \sum_{k=1}^{m} d_k = \mathbf{d}^{\mathrm{T}}\mathbf{d}$ for the weight of a binary vector. The symmetric matrix $\widetilde{\mathbf{B}}$ has entries $r_{kl} = \mathbf{a}_k^{\mathrm{T}}\mathbf{b}_l$ for $k \le l$. Thus for $\mathbf{C}$ of the form (12), we simply have $\widetilde{\mathbf{B}} = \mathbf{B}$. Note that the off-diagonal terms of $\widetilde{\mathbf{B}}$ just give rise to sign changes, not factors of i.

When $\mathbf{C}$ is of the form (12), we have $\mathbf{a} = \mathbf{d}$. Recalling that the vector $\mathbf{a}$ determines a unique diagonality subspace, each element in the sum (15) is in a different diagonality subspace. In each diagonality subspace, there is a unique vector $\mathbf{b} = \mathbf{B}\mathbf{d}$. Accordingly, all matrix elements in $\mathbf{M}$ have norm $1/\sqrt{N}$, and $\mathbf{M}$ is mutually unbiased with $\mathbf{I}_N$.

Next we continue with two basis matrices $\mathbf{M}_1$ and $\mathbf{M}_2$, which correspond to two binary matrices $\mathbf{C}_1$ and $\mathbf{C}_2$ of the form (12). Their inner product matrix can be expanded as in (15), resulting in

$$\begin{aligned}\mathbf{M}_1^{\mathrm{H}}\mathbf{M}_2 &= \frac{1}{N} \sum_{\mathbf{d}_1,\mathbf{d}_2\in\mathbb{F}_2^m} \mathrm{i}^{\mathbf{d}_2^{\mathrm{T}}(\mathbf{I}_m+\mathbf{B}_2)\mathbf{d}_2 - \mathbf{d}_1^{\mathrm{T}}(\mathbf{I}_m+\mathbf{B}_1)\mathbf{d}_1}\\ &\qquad \times (-1)^{\mathbf{d}_1^{\mathrm{T}}\mathbf{B}_1\mathbf{d}_2}\, \mathbf{E}\left(\mathbf{C}_1\mathbf{d}_1 \oplus \mathbf{C}_2\mathbf{d}_2\right)\end{aligned}$$

To proceed, we change the summation variables so that $\mathbf{d} = \mathbf{d}_1 \oplus \mathbf{d}_2$. Care has to be taken in this change of variables, as the exponent of i is $\bmod 4$, not $\bmod 2$. The result can be written in the form

$$\mathbf{M}_1^{\mathrm{H}}\mathbf{M}_2 = \frac{1}{N} \sum_{\mathbf{d}\in\mathbb{F}_2^m} \mathrm{i}^{-\mathbf{d}^{\mathrm{T}}(\mathbf{I}_m+\mathbf{B}_2)\mathbf{d}}\, \mathbf{V}(\mathbf{C}_1 \oplus \mathbf{C}_2, \mathbf{d})\, \mathbf{E}\left(\mathbf{C}_2\mathbf{d}\right) \tag{16}$$

where

$$\mathbf{V} = \sum_{\mathbf{d}_1\in\mathbb{F}_2^m} (-1)^{\mathbf{d}^{\mathrm{T}}\mathbf{d}_1}\, \mathrm{i}^{\mathbf{d}_1^{\mathrm{T}}(\mathbf{B}_1-\mathbf{B}_2)\mathbf{d}_1}\, \mathbf{E}\left((\mathbf{C}_1 \oplus \mathbf{C}_2)\mathbf{d}_1\right)\ . \tag{17}$$

Here, in the argument of $\mathbf{E}$ we have the matrix $\mathbf{C}_1 \oplus \mathbf{C}_2 = \begin{bmatrix} \mathbf{0}_{m\times m} & \mathbf{B}_1 \otimes \mathbf{B}_2 \end{bmatrix}$. Thus all matrices in the sum are diagonal. As a consequence of the linear independence, the matrix $\mathbf{B}_1 \otimes \mathbf{B}_2$ is full rank. Thus all matrices in the sum are Frobenius orthogonal. Also, we can change variables in the sum so that $\mathbf{d}_1 = \sqrt{\mathbf{B}_1 \otimes \mathbf{B}_2}\ \tilde{\mathbf{d}}$. This change of variables exists in $\mathbb{F}_2^m$, and is one-to-one as $\mathbf{B}_1 \otimes \mathbf{B}_2$ is full rank. As a result, $\mathbf{V}$ can be written in the form (14), where there are certain additional signs that depend on the individual bits $\tilde{\mathbf{d}}$ and their products with bits from $\mathbf{d}$, but not on products of bits in $\tilde{\mathbf{d}}$. Also, the normalization $\sqrt{N}$ is missing. Then $\mathbf{V}$ can be written in the product form (13), in terms of some diagonal matrices $\mathbf{X}$, and $\mathbf{V}$ is $\sqrt{N}$ times a diagonal unitary matrix. As a consequence, the inner product matrix is precisely a sum over unitary matrices in the 2^m diagonality subspaces, and each entry has norm $1/\sqrt{N}$. The bases $\mathbf{M}_1$ and $\mathbf{M}_2$ are thus MUB.

It is worth noting that the construction (13) with $\mathbf{C}$ of form (12) gives directly a matrix where all entries are in $\mathcal{Q}$. However, using $\mathbf{C}_0$ in (12) does not give the identity matrix, but a diagonal one, and the elements are not in $\mathcal{Q}$.

IV. $2^{m(m-1)/2}$ Families of MaxMUBs

Taking $\mathbf{C}$s of the form (12), the construction (13) produces a unitary $2^m \times 2^m$ matrix $\mathbf{M}(\mathbf{B})$ from a symmetric binary $m \times m$ matrix $\mathbf{B}$. By construction, all of these matrices have entries in $\mathcal{Q}$, and all are mutually unbiased with $\mathbf{I}_N$. In the previous section we saw that one can choose a subset of 2^m matrices $\mathbf{B}_k$ such that all sums have full $\mathbb{F}_2$ rank; that the corresponding matrices $\mathbf{M}_k$ form a Maximal set $\widetilde{\mathcal{M}_{\max}}$ of MUBs with entries in $\mathcal{Q}$; and that $\mathcal{M}_{\max} = \{\mathbf{I}_N\} \cup \widetilde{\mathcal{M}_{\max}}$ is a maximal set of MUBs without constraints on the entries, i.e., $|\mathcal{M}_{\max}| = N + 1$.

The set of binary symmetric matrices $G_m(\mathbb{F}_2) \subset M_m(\mathbb{F}_2)$ has cardinality $2^{m(m+1)/2}$. The MUB construction of [8], [9] uses 2^m of them. Here we consider the full set

$$\mathcal{U} = \Big\{ \mathbf{M}(\mathbf{B}_k) \ \Big|\ \mathbf{B}_k \in G_m(\mathbb{F}_2) \Big\} \tag{18}$$

of $2^{m(m+1)/2}$ unitary matrices with entries in $\mathcal{Q}$ that can be constructed from $G_m(\mathbb{F}_2)$ by (13).

First we note that when constructing MaxMUBs, Wootters & al. constructed a set $S_0 \subset G_m(\mathbb{F}_2)$ of binary matrices with 2^m elements [8]. S_0 has the property that each non-zero element is invertible. We skip the proof of the following.

Lemma 1: We can find a set of $2^{m(m-1)/2}$ elements $x_i \in G_m(\mathbb{F}_2)$ so that

$$G_m(\mathbb{F}_2) = \bigcup_{i=1}^{2^{m(m-1)/2}} \{x_i + S_0\} \equiv \bigcup_{i=1}^{2^{m(m-1)/2}} S_i\ , \tag{19}$$

where $\{x_i + S_0\} \cap \{x_j + S_0\} = \emptyset$, when $i \neq j$.

From Lemma 1 it follows that we can partition the set (18) of unitary matrices

$$\mathcal{U} = \bigcup_{i=1}^{2^{m(m-1)/2}} \widetilde{\mathcal{M}}_{\max,i} \tag{20}$$

where each set $\mathcal{M}_{\max,i}$ has N elements, is a MaxMUB with entries in $\mathcal{Q}$, and $\mathcal{M}_{\max,i} \cup \{\mathbf{I}_N\}$ is a MaxMUB. We have thus

TABLE I
CODE CARDINALITIES K FOR DIFFERENT N

N	$\lvert\mathcal{C}_{\mathrm{mMUB}}\rvert$	$\lvert\mathcal{C}_{\mathrm{O-RM}}\rvert$
4	32	30
8	512	1080
16	2^{14}	$2^{15}+\sum_{k=4}^{11}2^k \;-\; 2^7$

partitioned the set $\mathcal{U}$ with $2^{m(m+1)/2}$ matrices into $2^{m(m-1)/2}$ maximal families of 2^m MUBs.

It is clear that not all of these matrices are unbiased. However, based on (16), precise statements about their inner product matrices can be given. We have

Lemma 2: For any $\mathbf{M}_1, \mathbf{M}_2 \in \mathcal{U}$ with $\mathbf{M}_1 \neq \mathbf{M}_2$, the absolute values of entries of $\mathbf{M}_1^{\mathrm{H}}\mathbf{M}_2$ come from the set

$$\mathcal{E} = \{0\} \cup \left\{ \frac{1}{\sqrt{2^k}} \right\}_{k=1}^{m} . \tag{21}$$

With $\mathrm{rank}_{\mathbb{F}_2}(\mathbf{B}_1 \otimes \mathbf{B}_2) = r$, $\mathbf{M}_1^{\mathrm{H}}\mathbf{M}_2$ vanishes in 2^{N-r} diagonality subspaces, whereas all other entries have absolute value $1/\sqrt{2^r}$.

The proof hinges on analysis of (16), and is ommitted.

V. CODE CONSTRUCTIONS FROM MULTIPLE MAXMUBS

The set of matrices $\mathcal{U}$ with inner product properties controlled as indicated by Lemma 2 provide a platform for multiple code constructions.

The inner product properties of the matrices in $\mathcal{U}$ are, by construction, invariant under column permutations and rotations. The matrices $\mathbf{M}$ are thus elements of the *permutation invariant flag manifold* $\vec{\mathcal{F}}_{N,N} = \mathrm{U}_N/(\mathrm{U}_1^p \mathrm{S}_N)$, i.e. representatives of equivalence classes of unitary matrices modulo column rotations and permutations. Thus $\mathcal{U}$ and its subsets are codebooks on $\vec{\mathcal{F}}_{N,N}$. They can be expanded to codebooks of generic unitary matrices by adding column permutations and rotations. See [13] for a discussion on flag manifold codebooks.

Grassmannian codebooks can in turn be generated from $\mathcal{U}$ by taking subspaces of p columns from the matrices. Here we concentrate on the simplest case, where $p = 1$. Thus we generate complex Grassmannian line codebooks directly from collections of columns $\mathbf{u}_k$ of matrices in $\mathcal{U}$ or its subsets. If $\mathbf{u}$ is a column of a matrix $\mathbf{M}$, we denote $\mathbf{u} \in \mathbf{M}$. The distance of interest for a Grassmannian code is the chordal distance, which for lines reduces to $d_c = \sqrt{1 - |\mathbf{u}_1^{\mathrm{H}}\mathbf{u}_2|^2}$. We have

Proposition 1: The codebook

$$\mathcal{C}_{\mathrm{mMUB}} = \left\{ \mathbf{u} \;\middle|\; \mathbf{u} \in \mathbf{M} \;;\quad \mathbf{M} \in \mathcal{U} \right\} \tag{22}$$

consists of $K = N^{(m+3)/2}$ Grassmannian lines, and has a minimum chordal distance $d_{c,\min} = 1/\sqrt{2}$. All $\mathbf{u}$ consist of scaled fourth-root-of unity entries from $\mathcal{Q}$.

Proof: Follows directly from Construction (13), and lemmas 1 and 2. ∎

In Table I, the properties of these codes can be compared to the best known Grassmannian codes in the literature, which can be found in [12]. There, line codes $\mathcal{C}_{\mathrm{O-RM}}$ with precisely the same minimum distance $1/\sqrt{2}$ are constructed as operator

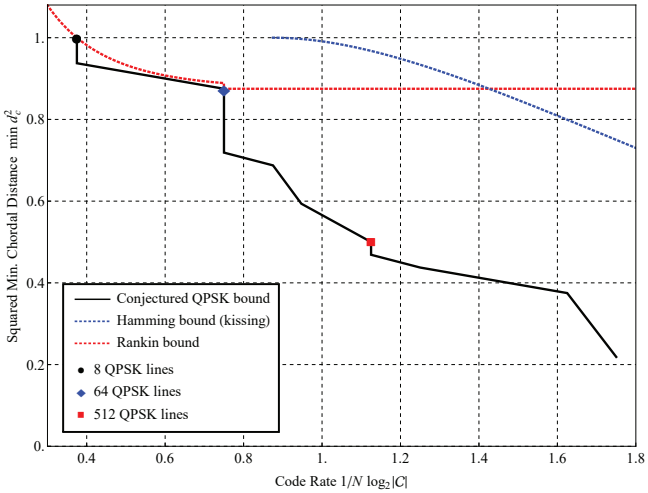

Fig. 1. Squared minimum distance of codes in $N = 8$ dimensions.

Reed-Muller codes. It is our understanding that, except for $N = 4$, $\mathcal{C}$ is the subset of $\mathcal{C}_{\mathrm{O-RM}}$ with entries in $\mathcal{Q}$. We conjecture that by expanding $\mathcal{U}$ with matrices of the same form, but with the possibility for zero-entries, one may expand $\mathcal{C}_{\mathrm{mMUB}}$.

In Figure 1, we concentrate on the case $N = 8$. We have plotted $\min d_c^2$ against the code rate $R = (\log_2 K)/N$. The Rankin bound, and a Hamming type bound are reported. The latter is from [14], [15], and is based on spherical cap Kissing radius. These are bounds for codebooks with unconstrained entries. In addition, a numerically found bound for codebooks with entries in $\mathcal{Q}$ is shown. The three codebooks that can be created from MUBs are separately shown. A codebook with $K = 8$ elements and $\min d_c^2 = 1$ can be created from one unitary matrix $\mathbf{M}$. Taking the columns of a MaxMUB $\widetilde{\mathcal{M}}_{\max}$ with entries in $\mathcal{Q}$ one gets a code with $K = 64$ and $\min d_c^2 = 7/8$. This is close to the Rankin bound, which can be reached by adding the 8 columns of $\mathbf{I}_8$ so that one gets an unconstrained MaxMUB. Finally, the code $\mathcal{C}_{\mathrm{mMUB}}$ constructed from $\mathcal{U}$ has $K = 512$ and $\min d_c^2 = 1/2$.

VI. ENCODING/DECODING AND STORAGE COMPLEXITY

Given that codes constructed from multiple MUBs are likely subsets of known codes, the main benefit from the presented construction comes from the control on the code alphabet, and the identified structure in terms of MUBs. This can be used to reduce decoding complexity.

Irrespectively of the use of a code in an information processing system, a matched filter stage is needed. If a code is used for channel coding, the decoder faces the challenge of identifying the codeword that is closest to a received signal. If it used for source coding, the quantizer faces the encoding problem of finding the codeword closest to a source signal. In both, optimum en/decoding would start by a distance calculation, which again starts with matched filtering, i.e. calculating the inner products between all codeword vectors and the signal. When the signal, and the codewords are vectors, the codebook can be described as a matrix $\mathbf{U}$ where the

TABLE II
ENCODING/DECODING AND STORAGE COMPLEXITY FOR $\mathcal{Q}$ CODES.

Code	Encoding/Decoding	Storage
$\mathcal{C}_{\mathcal{Q}}$	NK	$2NK$
$\mathcal{C}_{\mathbb{C}-\mathrm{Hadamard}}$	$\log_2 N\ K$	$\frac{(\log_2 N)^2}{N}K$
$\mathcal{C}_{\mathrm{mMUB}}$	K	$\frac{\log_2 N}{N}K$

codewords are columns. The matched filter stage would be

$$\mathbf{z} = \sqrt{N}\mathbf{U}^{\mathrm{H}}\mathbf{y}\ . \tag{23}$$

Here, for a channel coding problem, such as for sending Random Access signatures over a non-coherent channel [5], $\mathbf{y}$ would be the received signal. For a vector quantization problem, such as MIMO precoding [7], the signal $\mathbf{y}$ would be a channel vector.

When all entries of $\mathbf{U}$ are in $\mathcal{Q}$, $\mathbf{z}$ can be calculated without a single multiplication. Instead, one only needs to switch real and imaginary parts, and signs. However, the number of additions depend on the code construction. For a generic $\mathcal{Q}$ code $\mathcal{C}_{\mathcal{Q}}$ with no structure, NK additions are needed in (23). For a codebook $\mathcal{C}_{\mathbb{C}-\mathrm{Hadamard}}$ consisting of columns of K/N complex Hadamard matrices without further structure, one can calculate N entries of $\mathbf{z}$ with a fast transform consisting of mN additions. In all, mK additions are needed. For the codebook $\mathcal{C}_{\mathrm{mMUB}}$ discussed in the previous section, the complex Hadamard matrices can be grouped according to the common columns in their $\mathbf{B}$-matrices. In total, K additions are needed.

Similarly, one may consider the storage needed for a code. For an unstructured code $\mathcal{C}_{\mathcal{Q}}$, $2NK$ bits are needed. For a Complex Hadamard code, each matrix can be stored with m^2 bits, so that in total m^2K/N bits are needed. For $\mathcal{C}_{\mathrm{mMUB}}$ one only needs to store K/N binary m-vectors. Note that the elements in the codebooks need not be generated when calculating (23), an algorithm operating directly with the stored bits can be devised.

The encoding/decoding complexity in terms of additions needed for calculating (23), and the number of bits for codebook storage, are summarized in Table II. The numbers for an unconstrained $\mathcal{Q}$-code, a code of complex Hadamard matrices, and $\mathcal{C}_{\mathrm{mMUB}}$ are reported. It is remarkable that the complexity of calculating the matched filter (23) for $\mathcal{C}_{\mathrm{mMUB}}$ is *linear* in the code cardinality, and does not depend on the dimension N. The decoding algorithm of the operator Reed-Muller codes of [12] for rank-1 codes is slightly larger than the complexity of the arbitrary $\mathbb{C}$-Hadamard codes discussed above.

VII. CONCLUSION

We have provided a construction of unitary matrices in $N = 2^m$ dimension with scaled fourth-root-of-unity (QPSK) entries, which have column inner products of absolute value at most $1/\sqrt{2}$. The construction produces a multifamily set of Mutually Unbiased Bases, and is directly expressed in terms of basis matrices. No decompositions are needed to create Grassmannian codes from these matrices—it is sufficient to take collections of columns to get Grassmannian codebooks with controlled properties. As an example, we have constructed QPSK codebooks with $K = N^{(m+3)/2}$ lines at minimum chordal distance $1/\sqrt{2}$ for any m. The structure of the codebooks enables reduced complexity encoding/decoding with complexity K, irrespectively on N. The codes have intriguing connections with Operator Reed-Muller codes, which will be explored in future work.

ACKNOWLEDGEMENTS

This work was funded in part by Kaute foundation, Nokia Foundation, the Academy of Finland (grant 299916) and EIT ICT (HII:ACTIVE).

REFERENCES

[1] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *Int. J. Quantum Inform.*, vol. 8, no. 4, pp. 535–640, 2010.

[2] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.*, vol. 3, pp. 436–480, 1997.

[3] R. Gribonval and M. Nielsen, "Sparse representations in unions of bases," *IEEE Trans. Inf. Th.*, no. 12, pp. 3320–3325, Dec. 2003.

[4] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: a geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.

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

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

[7] T. Inoue and R. W. Heath, "Kerdock codes for limited feedback MIMO systems," in *Proc. IEEE ICASSP*, Mar. 2008, pp. 3113–3116.

[8] W. Wootters and B. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys*, vol. 191, no. 2, pp. 363–381, 1989.

[9] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, "A new proof for the existence of mutually unbiased bases," *Algorithmica*, vol. 34, no. 4, pp. 512–528, Nov. 2002.

[10] R. Gow, "Generation of mutually unbiased bases as powers of a unitary matrix in 2-power dimensions," preprint arxiv:math/0703333, Apr. 2017.

[11] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "A group-theoretic framework for the construction of packings in Grassmannian spaces," *J. Algebraic Combin.*, vol. 9, pp. 129–140, 1999.

[12] A. Ashikhmin and A. Calderbank, "Grassmannian packings from operator Reed–Muller codes," *IEEE Trans. Inf. Th.*, vol. 56, no. 11, pp. 5689–5714, Nov. 2010.

[13] R.-A. Pitaval and O. Tirkkonen, "Flag orbit codes and their expansion to stiefel codes," in *Proc. IEEE Inf. Th. Worksh.*, Sep. 2013, pp. 1–5.

[14] K. K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, "On beamforming with finite rate feedback in multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2562–2579, Oct. 2003.

[15] P. Xia and G. B. Giannakis, "Design and analysis of transmit-beamforming based on limited-rate feedback," *IEEE Trans. Sign. Proc.*, vol. 54, no. 5, pp. 1853–1863, May 2006.