Grassmannian Frames in Composite Dimensions by Exponentiating Quadratic Forms

Renaud-Alexandre Pitaval and Yi Qin
Huawei Technologies Sweden AB, Stockholm, Sweden
Emails: {renaud.alexandre.pitaval, qinyi4}@huawei.com

***Abstract*—Grassmannian frames in composite dimensions D are constructed as a collection of orthogonal bases where each is the element-wise product of a mask sequence with a generalized Hadamard matrix. The set of mask sequences is obtained by exponentiation of a q-root of unity by different quadratic forms with m variables, where q and m are the product of the unique primes and total number of primes, respectively, in the prime decomposition of D. This method is a generalization of a well-known construction of mutually unbiased bases, as well as second-order Reed-Muller Grassmannian frames for power-of-two dimension $D = 2^m$, and allows to derive highly symmetric nested families of frames with finite alphabet. Explicit sets of symmetric matrices defining quadratic forms leading to constructions in non-prime-power dimension with good distance properties are identified.**

***Index Terms*—Grassmannian frames, quadratic forms, Kerdock codes, Delsarte–Goethals codes, Reed-Muller codes.**

I. Introduction

A frame is a generalization of the notion of basis of a vector space such that $\mathbf{F} = \{\mathbf{f}_k\}_k$ spans the space. Each column in $\mathbf{F}$ represents a complex line, or an element in the Grassmann manifold $\mathcal{G}^{\mathbb{C}}_{n,1}$, and can be defined to be normalized as $\|\mathbf{f}_j\| = 1$. The quality of a Grassmannian frame is typically measured by its worst-case coherence

$$\mu(\mathbf{F}) = \max_{i \neq j} |\mathbf{f}_j^{\mathrm{H}} \mathbf{f}_i|. \tag{1}$$

The problem of designing frames with good (i.e. low) coherence is directly related to Grassmannian packing [1], [2] and the worst-case coherence of $\mathbf{F}$ can be directly reformulated in terms of its minimum chordal distance as $\delta_c^2(\mathbf{F}) = 1 - \mu^2(\mathbf{F})$. Although the wording *frame* and *coherence* is more prominent in mathematics and signal processing, the equivalent wordings of *codebook* and *distance* is more consistent with coding theory, and we will use both without distinctions.

The application of Grassmannian frames is vast [1], [2]. Traditional motivations in information theory have been in quantum codes [3]–[5], CDMA signatures [6], limited-feedback beamforming for multi-antenna systems [7], multi-dimensional constellations for non-coherent communications [8], [9], and overcomplete dictionaries for sparse signal processing [10]. More recently, sparse vector coding [11] is at the cross-road of these two latter applications where coding is done by superposition of multi-dimensional codewords, decoded by sparse signal processing algorithms. Grassmannian frames have also been recently considered in [12] for non-orthogonal-multiple-access (NOMA), and in [13], [14] for grant-free massive access.

The work of [10], [15] provides an analytical construction of Grassmannian frames with practical interest, and considered for different applications in e.g. [9]–[11], [13]. This construction arises from the exponentiation of the imaginary number by Kerdock, Delsarte-Goethals, and Reed-Muller codes over the ring of integers modulo 4. It is based on a simplification of the representation such codes given in [16], and other works by Calderbank *et al.* on mutually unbiased bases (MUB) and Grassmannian packings, see notably [17]. The codebook can be equivalently seen as the collection of orthogonal bases where each basis is constructed from a Hadamard matrix multiplied by different mask sequences, and where each mask sequence is the exponentiation of the 4-root of unity by a different quadratic form.

The construction from [10], [15] is unfortunately specific to power-of-two dimensions, $D = 2^m$, and a main motivation for this present work is that if Grassmannian frames are to be deployed in practical wireless systems, and notably for data-transmission by multi-dimensional constellations, it would be desirable to have a systematic construction even more flexible in D. Specifically, it would be preferable to be able to accommodate practical resource allocations such as 12 subcarriers in a physical resource block as defined in 3GPP standards [18], [19]. With this in mind, we investigate and present in this paper a framework to generalize the construction in [10] to any dimension and notably composite dimensions which are not a prime-power. The method reduces to defining sets of symmetric matrices, equivalently quadratic forms, whose size and input coefficients follows from the prime decomposition of D. Explicit constructions with large minimum chordal distance are provided.

II. Prime-Power Dimensions

We start by describing constructions in ($D = 2^m$)-dimensions related to Kerdock, Delsarte-Goethals, and 2nd-order Reed-Muller codes [10], [17], [20], [21], which mainly follows from [10], [15] with some slight generalizations.

A. $\mathbb{Z}_4$- Kerdock, Delsarte-Goethals, and Reed-Muller Frames

Let us consider $D = 2^m$ with $m \geq 1$. The frame is constructed as in [10], [15] from a set of orthogonal bases which are all covered version of a Hadamard matrix. Each orthogonal basis is a $2^m \times 2^m$ unitary matrix whose rows and

columns are indexed by m-binary vectors. We remark that m is originally restricted in [10], [15] to be odd but it is generalized here to any m with few modifications. More specifically, the frame is a set of column vectors $\mathbf{F} = \{\{\mathbf{f}_{\mathbf{S},\mathbf{k}}\}_{\mathbf{k}\in\mathbb{F}_2^m}\}_{\mathbf{S}\in\mathcal{S}}$, where for each the $\mathbf{l}$th-entry is defined by

$$[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \frac{1}{\sqrt{D}} \mathrm{i}^{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}+2\mathbf{k}^{\mathrm{T}}\mathbf{l}} \tag{2}$$

where $\mathrm{i} = \sqrt{-1}$, $\mathbf{k},\mathbf{l} \in \mathbb{F}_2^m$, and $\mathbf{S}$ is a $m \times m$ binary symmetric matrix belonging to a predefined set $\mathcal{S}$. Given $\mathbf{S}$ and $\mathbf{k}$, the vector $\{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}+2\mathbf{k}^{\mathrm{T}}\mathbf{l}\}_{\mathbf{l}\in\mathbb{F}_2^m}$ (modulo 4) is a 2nd-order multivariate polynomial and thus a codeword in the quaternary 2nd-order Reed-Muller code.

For each $\mathbf{S}$, $\mathbf{F}_{\mathbf{S}} = \{\mathbf{f}_{\mathbf{S},\mathbf{k}}\}_{\mathbf{k}\in\mathbb{F}_2^m}$ is a unitary matrix where the binary vectors $\mathbf{l}$, $\mathbf{k}$ are indexing rows and columns, respectively. By writing $[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \frac{1}{\sqrt{D}}\mathrm{i}^{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}} \times (-1)^{\mathbf{k}^{\mathrm{T}}\mathbf{l}}$, one sees that codewords are constructed by element-wise product of a Hadamard matrix $\{(-1)^{\mathbf{k}^{\mathrm{T}}\mathbf{l}}\}_{\mathbf{k},\mathbf{l}\in\mathbb{F}_2^m}$ with a mask sequence $\frac{1}{\sqrt{D}}\{\mathrm{i}^{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}}\}_{\mathbf{l}\in\mathbb{F}_2^m}$ which is the exponentiation of the 4-th root of unity by the quadratic form $\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}$. The coherence between two such codewords constructed from two different symmetric matrices is at worst [10]

$$|\mathbf{f}_{\mathbf{S},\mathbf{k}}^{\mathrm{H}}\mathbf{f}_{\mathbf{S}',\mathbf{k}'}| \leq 2^{-R/2} \tag{3}$$

where $R = \mathrm{rank}[\mathbf{S}-\mathbf{S}']_{(\mathrm{mod}\,2)}$, which can be equivalently expressed in chordal distance by $d_c^2(\mathbf{f}_{\mathbf{S},\mathbf{k}}^{\mathbf{H}}, \mathbf{f}_{\mathbf{S}',\mathbf{k}'}) \geq 1-2^{-R}$. Therefore, the distance properties of the frame, as well as its size, only depends on the set of symmetric matrices $\mathcal{S}$ that defines a collection of quadratic forms.

There is a maximum of $2^{m(m+1)/2}$ possible binary symmetric matrices which can be constructed as nested subspaces, known as the Delsarte-Goethals (DG) sets [20]:

$$\begin{aligned}\mathrm{K}_m \triangleq \mathrm{DG}(m,0) \subset \mathrm{DG}(m,1) \subset \ldots \\ \subset \mathrm{DG}\left(m, \left\lfloor \tfrac{m-1}{2} \right\rfloor\right) \subseteq \mathrm{DG}\left(m, \tfrac{m-1}{2}\right) \triangleq \mathrm{S}_m.\end{aligned}$$

For integers $r \leq \left\lfloor \frac{m-1}{2} \right\rfloor$, $\mathrm{DG}(m,r)$ is a $(r+1)m$-dimensional binary subspace leading to a collection of $2^{(r+1)m}$ symmetric matrices such that any non-zero matrix in $\mathrm{DG}(m,r)$ has rank at least equal to $R = m-2r$. The first set $\mathrm{K}_m = \mathrm{DG}(m,0)$ is a subspace of full-rank binary matrices, called the Kerdock set such that given $\mathbf{S} \in \mathrm{DG}(m,0)$ the vector $\{\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}\}_{l\in\mathbb{F}_2^m}$ is a codeword in the quaternary Kerdock code. By selecting the set of symmetric matrices $\mathcal{S}$ to be one of the DG sets $\mathrm{DG}(m,r)$, we obtained a frame of size $N = 2^{(r+2)m}$ with maximum coherence $2^{-(m-2r)/2}$ [10].

For the case m even, the set $\mathrm{DG}\left(m, \left\lfloor \frac{m-1}{2} \right\rfloor\right)$ does not include all binary symmetric matrices so that one can construct a larger set $\mathrm{S}_m = \mathrm{DG}\left(m, \frac{m-1}{2}\right)$ in which all non-zero matrices have rank at least equal to $R = 1$. This last set has only $m/2$ extra dimensions over $\mathrm{DG}\left(m, \left\lfloor \frac{m-1}{2} \right\rfloor\right)$. Thus for any m odd or even, by selecting $\mathcal{S} = \mathrm{S}_m$, one gets a frame of size $N = 2^{m(m+3)/2}$ with maximum coherence $2^{-1/2}$.

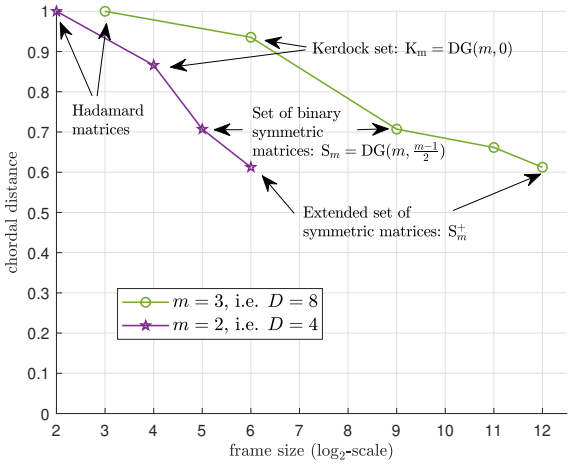

Fig. 1. DG set construction and its extension.

B. Algorithmic Construction of the DG Sets

We provide here a systematic computation of the DG sets described in [15] by generalizing the algorithm in [6]. The basis of the Kerdock set $\mathrm{DG}(m,0)$ are found in [6] by identifying the m matrices $\mathbf{B}_0^{(0)}, \mathbf{B}_1^{(0)}, \ldots, \mathbf{B}_{m-1}^{(0)}$ of size $m \times m$ such that

$$\mathbf{a}\mathbf{a}^T = \mathbf{B}_0^{(0)} + \alpha\mathbf{B}_1^{(0)} + \ldots + \alpha^{m-1}\mathbf{B}_{m-1}^{(0)}. \tag{4}$$

where $\mathbf{a} = [1, \alpha, \alpha^2, \cdots, \alpha^{m-1}]^{\mathrm{T}}$ is a basis of the Galois field $\mathrm{GF}(2^m)$. As such, the basis can easily be found in e.g. MATLAB [6].

Similarly, for $0 < r \leq \left\lfloor \frac{m-1}{2} \right\rfloor$, the basis of $\mathrm{DG}(m,r)$ can be found incrementally as the union of the basis of $\mathrm{DG}(m,r-1)$ and m matrices $\mathbf{B}_0^{(r)}, \mathbf{B}_1^{(r)}, \ldots, \mathbf{B}_{m-1}^{(r)}$ such that

$$\mathbf{a}\mathbf{b}^T + \mathbf{b}\mathbf{a}^T = \mathbf{B}_0^{(r)} + \alpha\mathbf{B}_1^{(r)} + \ldots + \alpha^{m-1}\mathbf{B}_{m-1}^{(r)} \tag{5}$$

where $\mathbf{a}$ is as before and $\mathbf{b} = [1, \alpha^{2^r}, \alpha^{2\cdot 2^r}, \ldots, \alpha^{(m-1)2^r}]^{\mathrm{T}}$. For $r = \frac{m-1}{2}$ with m even, $\mathbf{b} = \{\alpha^{2^{k\lceil r\rceil}}\}_{k=0}^{m-1}$ and only the first $m/2$ matrices $\mathbf{B}_0^{(r)}, \mathbf{B}_1^{(r)}, \ldots, \mathbf{B}_{m/2-1}^{(r)}$ should be kept.

C. Enlarged Construction S_m^+ in $D = 2^m$

The original frame construction above is based on an exponentiation by *almost all* possible second-order polynomials defined over the ring of integers modulo 4 with binary multi-dimensional variable $\mathbf{l}$. We can further increase the frame size by a more exhaustive constructions where off-diagonal entries of $\mathbf{S}$ are any $a/2$ with $a \in \mathbb{Z}_4$.

For example, consider the case $m = 2$ so that $\mathbf{l} = [l_1, l_2]^{\mathrm{T}}$, $\mathbf{k} = [k_1, k_2]^{\mathrm{T}}$ and $\mathbf{S} = \begin{bmatrix} s_1 & s_{12} \\ s_{12} & s_2 \end{bmatrix}$. By expansion and observing that $x^2 = x$ for binary variables, we have $\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l} + 2\mathbf{k}^{\mathrm{T}}\mathbf{l} = 2s_{12}l_1l_2 + (2k_1+s_1)l_1 + (2k_2+s_2)l_2$. So by restricting $\mathbf{S}$ to be binary, we are able to list all possible coefficients modulo 4 only for the first-order terms, but the coefficient of the second-order term is limited to 0 or 2. This leads originally to a frame of 32 codewords with maximum coherence $\sqrt{1/2}$. By considering also $s_{12} = 1/2$ and $3/2$, we are able to construct more 2nd-order polynomials, extending the frame to 64 codewords with maximum coherence $\sqrt{5/8}$.

This observation extends to larger m, where larger frames are obtained by considering symmetric matrices with binary diagonal entries but off-diagonal entries equal to 0, $1/2$, 1 or $3/2$. We denote the set containing all such symmetric matrices by S_m^+, which is of size 2^{m^2}. This means we can increase the original maximum frame size of $2^{m(m+3)/2}$ to $2^{m(m+1)}$. Illustration is provided in Fig. 1. With $m = 2$ and 3, the frame size is increased from 5 bits to 6 bits, and from 9 bits to 12 bits, respectively. For both cases, the minimum distance is then dropping from $1/\sqrt{2} \approx 0.71$ to $\sqrt{3/8} \approx 0.61$. As shown in Fig. 1 for the case $m = 3$, we heuristically found an intermediate frame of size 11 bits with minimum distance $\sqrt{7}/4 \approx 0.66$, which is obtained by restricting the three off-diagonal elements to be such that always two of them are either $1/2$ or $3/2$ and the remaining one is either 0 or 1.

D. Similar Constructions in $D = p^m$ with p odd prime

Related constructions also exist in the literature for $D = p^m$ with p being an odd prime [5], [17], [20]–[22]. In [21], codewords are constructed similarly as

$$[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \frac{1}{\sqrt{D}} e^{\frac{2\pi \mathrm{i}}{p}\left(\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}+\mathbf{k}^{\mathrm{T}}\mathbf{l}\right)}. \tag{6}$$

The construction in [21] considered only full-rank symmetric matrices to construct MUBs, analogous to the Kerdock set. In [22], larger frames are obtained for $m > 1$ using related algebraic tools from [17]. Part of this enlargement can be constructed similarly as above by considering exponentiation by quadratic forms from any symmetric matrices in modulo-p arithmetic. Intermediate constructions from DG sets are possible as Delsarte and Goethals constructed such sets for p odd as well but only with m odd [20] .

III. Generalization to Non-Prime Power Dimensions

Consider the prime factorization of the dimension

$$D = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \tag{7}$$

where $p_1 < \cdots < p_n$ are the n unique prime factors, each of order $m_1, \ldots, m_n$. Each factor $p_k^{m_k}$ is called a primary. There are $m = \sum_{k=1}^n m_k$ constituent primes in the factorization and the product of the unique prime factors is $q = \prod_{k=1}^n p_k$. Let us also define $\lambda = 2$ for D even and $\lambda = 1$ otherwise.

To index entries of a D-dimensional vector, we will use a one-to-one mapping from the ring $\mathbb{Z}_D$ of integers modulo D to a Cartesian product of the Galois fields with order the primaries from the prime factorization of D:

$$\mathbb{Z}_D \mapsto \mathbb{F}_{p_1}^{m_1} \times \mathbb{F}_{p_2}^{m_2} \times \cdots \times \mathbb{F}_{p_n}^{m_n}. \tag{8}$$

Consistently, elements in $\mathbb{Z}_D$ are represented by m-dimensional vectors. For example, any $x \in \mathbb{Z}_{12}$ can be written as $[b_2, b_1, t] \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_3$ where $x = t \times 2^0 \cdot 2^0 \cdot 3^0 + b_1 \times 2^0 \cdot 2^0 \cdot 3^1 + b_2 \times 2^0 \cdot 2^1 \cdot 3^1$, such that we have $5 \to [0, 1, 2]^{\mathrm{T}}$ or $8 \to [1, 0, 2]^{\mathrm{T}}$, etc.

TABLE I
BD constructions for $N = p_1 p_2$.

	$\mathcal{S}$	μ^2	N
BD1	$\left\{ \begin{bmatrix} a\frac{p_2}{\lambda} & 0 \\ 0 & ap_1 \end{bmatrix} : a \in \mathbb{Z}_{p_1} \right\}$	$(p_1 p_2)^{-1}$	$p_1^2 p_2$
BD2	$\left\{ \begin{bmatrix} a\frac{p_2}{\lambda} & 0 \\ 0 & ap_1 \end{bmatrix}, \begin{bmatrix} a_0\frac{p_2}{\lambda} & 0 \\ 0 & bp_1 \end{bmatrix} : a \in \mathbb{Z}_{p_1}, a_0 \text{ fixed}, b \in (\mathbb{Z}_{p_2} \setminus \mathbb{Z}_{p_1}) \right\}$	p_2^{-1}	$p_1 p_2^2$
BD3	$\left\{ \begin{bmatrix} a\frac{p_2}{\lambda} & 0 \\ 0 & bp_1 \end{bmatrix} : a \in \mathbb{Z}_{p_1}, b \in \mathbb{Z}_{p_2} \right\}$	p_1^{-1}	$p_1^2 p_2^2$

Using this, codewords are constructed as the exponentiation by different second-order polynomials over m variables as

$$[\mathbf{f}_{\mathbf{S},\mathbf{k}}]_{\mathbf{l}} = \frac{1}{\sqrt{D}} e^{\frac{2\pi \mathrm{i}}{q}\left(\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}+\mathbf{k}^{\mathrm{T}}\mathbf{D}\mathbf{l}\right)} \tag{9}$$

where $\mathbf{l}, \mathbf{k} \in \mathbb{Z}_D$, $\mathbf{S}$ is a $m \times m$ symmetric matrix from a predefined set $\mathcal{S}$, and

$$\mathbf{D} = \mathrm{blkdiag}\left(\frac{q}{p_1}\mathbf{I}_{p_1}, \frac{q}{p_2}\mathbf{I}_{p_2}, \ldots, \frac{q}{p_n}\mathbf{I}_{p_n}\right) \tag{10}$$

is a diagonal matrix where $\mathbf{I}_n$ is an $n \times n$ identity matrix, and $\mathrm{blkdiag}(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)$ defines a block diagonal matrix with matrices $(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_n)$ along its diagonal.

Each codeword is again the product of a mask sequence $\frac{1}{\sqrt{D}}\{e^{\frac{2\pi \mathrm{i}}{q}\mathbf{l}^{\mathrm{T}}\mathbf{S}\mathbf{l}}\}_{\mathbf{l}\in\mathbb{Z}_D}$, which is the exponentiation of the q-root of unity by a quadratic form, and a column of a generalized Hadamard matrix $\{e^{\frac{2\pi \mathrm{i}}{q}\mathbf{k}^{\mathrm{T}}\mathbf{D}\mathbf{l}}\}_{\mathbf{l},\mathbf{k}\in\mathbb{Z}_D}$. The distance properties of the frame depend again only on the set of symmetric matrices $\mathcal{S}$. We discuss below explicit examples of such sets leading to frames with good distance properties.

A. General Constructions

1) General Construction 1 (GC1): While any real symmetric matrices could be considered, we will restrict ourselves to polynomials having integer coefficients modulo q. For this, the off-diagonal entries of $\mathbf{S}$ can be restricted to be integers modulo q divided by 2 in order to account that $\mathbf{S}$ is a symmetric matrix. If $p_1 > 2$, the diagonal entries of $\mathbf{S}$ can be restricted to be integers modulo q. If $p_1 = 2$, the first m_1 diagonal entries in $\mathbf{S}$ must be divided by 2, i.e. in general by λ, to avoid ambiguity between the second-order terms in the quadratic forms and the first-order terms with the generalized Hadamard matrix. This is related to the discussion in Section II.C. and again because $x^2 = x$ only in the binary field. It follows that if $p_1 = 2$ the entries of the codewords are not powers of the q-root but of the $2q$-root of unity.

As such, we can construct a total $N = Dq^{m(m+1)/2}$ codewords. This number is rather large, e.g. ≈ 19 bits for $D = 12$, for which the frame will inevitably have a small minimum distance, and it is therefore relevant to look for smaller frames with larger minimum distance.

2) General Construction 2 (GC2): We further restrict the symmetric matrix $\mathbf{S}$ to be made of n blocks on its main diagonal where the kth block for $k > 1$ is $\frac{q}{p_k}\mathbf{S}_k = \left(\prod_{i\neq k} p_i\right)\mathbf{S}_k$ where $\mathbf{S}_k$ is $m_k \times m_k$ symmetric matrix with integer entries modulo p_k. For $k = 1$, the first block is $\frac{q}{\lambda p_1}\mathbf{S}_1$ where $\mathbf{S}_1$ is also with integer entries modulo p_1 but divided by λ, i.e., 2 if

TABLE II
BD CONSTRUCTIONS FOR $D = 2^{m_1} \cdot 3$.

	$\mathcal{S}$	μ^2	N
BD4	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A}_i & 0 \\ 0 & 2b_i \end{bmatrix} : \mathbf{A}_i \in \mathrm{K}_{m_1} \text{ uniquely associated to a } b_i \in \mathbb{Z}_3 \right\}$	$2^{-m_1} \cdot 3^{-1}$	$2^{m_1} \cdot 3$
BD5	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 0 \\ 0 & 2b_0 \end{bmatrix} : \mathbf{A} \in \mathrm{K}_{m_1}, b_0 \text{ fixed} \right\}$	2^{-m_1}	$2^{2m_1} \cdot 3$
BD6	For $m_1 = 2$ $\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 0 \\ 0 & 2b_i \end{bmatrix} : \mathbf{A} \in \{\mathbf{A}_i + \mathrm{K}_2\} \text{ where } \mathbf{A}_0 = 0, \mathbf{A}_1 \in (\mathrm{S}_2 \setminus \mathrm{K}_2), \mathbf{A}_2 \in (\mathrm{S}_2^+ \setminus \mathrm{S}_2), \text{ and } b_i \in \mathbb{Z}_3 \right\}$	2^{-2}	$2^4 \cdot 3^2$
BD7	For $m_1 \geq 3$ $\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 0 \\ 0 & 2b_i \end{bmatrix} : \mathbf{A} \in \{\mathbf{A}_i + \mathrm{K}_{m_1}\} \text{ where } \mathbf{A}_0 = 0, \mathbf{A}_1, \mathbf{A}_2 \in (\mathrm{DG}(m_1, 1) \setminus \mathrm{K}_{m_1}), \text{ and } b_i \in \mathbb{Z}_3 \right\}$	$2^{(2-m_1)} \cdot 3^{-1}$	$2^{2m_1} \cdot 3^2$
BD8	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 0 \\ 0 & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{S}_{m_1}, b \in \mathbb{Z}_3 \right\}$	2^{-1}	$2^{\frac{m_1(m_1+3)}{2}} \cdot 3^2$
BD9	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 0 \\ 0 & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{S}_{m_1}^+, b \in \mathbb{Z}_3 \right\}$	$\frac{5}{8}$	$2^{m_1(m_1+1)} \cdot 3^2$

TABLE III
EBD CONSTRUCTIONS FOR $D = p_1 p_2$.

	$\mathcal{S}$	μ^2	N
EBD1	$\left\{ \begin{bmatrix} a\frac{p_2}{\lambda} & cp_1 \\ cp_1 & ap_1 \end{bmatrix}, \begin{bmatrix} a_0\frac{p_2}{\lambda} & cp_1 \\ cp_1 & bp_1 \end{bmatrix} : a \in \mathbb{Z}_{p_1}, a_0 \text{ fixed}, b \in \mathbb{Z}_{p_2} \setminus \mathbb{Z}_{p_1}, c \in \mathbb{Z}_{p_2} \right\}$	p_1^{-2} if $p_1 = 2$, $p_2 > 3$; p_2^{-1} otherwise	$p_1 p_2^3$
EBD2	$\left\{ \begin{bmatrix} a\frac{p_2}{\lambda} & cp_1 \\ cp_1 & bp_1 \end{bmatrix} : a \in \mathbb{Z}_{p_1}, b, c \in \mathbb{Z}_{p_2} \right\}$	p_1^{-1}	$p_1^2 p_2^3$

TABLE IV
EBD CONSTRUCTIONS FOR $D = 12$.

	$\mathcal{S}$	μ^2	N
EBD4	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b_0 \end{bmatrix} : \mathbf{A} \in \mathrm{K}_2, \mathbf{c} \in \mathbb{Z}_3^2, b_0 \text{ fixed} \right\}$	2^{-2}	$2^4 \cdot 3^3$
EBD5	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{K}_2, \mathbf{c} \in \mathbb{Z}_3^2, b \in \mathbb{Z}_3 \right\}$	3^{-1}	$2^4 \cdot 3^4$
EBD6	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{S}_2, \mathbf{c} \in \mathbb{Z}_3^2, b \in \mathbb{Z}_3 \right\}$	2^{-1}	$2^5 \cdot 3^4$
EBD7	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{S}_2^+, \mathbf{c} \in \mathbb{Z}_3^2, b \in \mathbb{Z}_3 \right\}$	$\frac{5}{8}$	$2^6 \cdot 3^4$

$p_1 = 2$. If $p_1 = 2$ and $m_1 > 1$, this construction can be further extended by considering $\mathbf{S}_1 \in \mathrm{S}_{m_1}^+$ described in Section II.C. Below, we describe explicit sub-frames of GC2.

B. Block diagonal (BD) constructions

We start by considering the case where the off-blockdiagonal entries of $\mathbf{S}$ are set to zero such that

$$\mathbf{S} = \mathrm{blkdiag}\left(\frac{q}{\lambda p_1}\mathbf{S}_1, \frac{q}{p_2}\mathbf{S}_2, \ldots, \frac{q}{p_n}\mathbf{S}_n \right) \tag{11}$$

where each $\mathbf{S}_k$ is a p_k-ary symmetric matrix of size $m_k \times m_k$.

By setting the off-blockdiagonal entries to zero, the codewords are Kronecker products of codewords in sub-dimensions $p_k^{m_k}$, and thus the coherence between one with $\mathbf{S}$ in (11) and one with $\mathbf{S}' = \mathrm{blkdiag}\left(\frac{q}{\lambda p_1}\mathbf{S}_1', \frac{q}{p_2}\mathbf{S}_2', \ldots, \frac{q}{p_n}\mathbf{S}_n' \right)$ is less than $\prod_i p_i^{-R_i/2}$ where $R_i = \mathrm{rank}[\mathbf{S}_i - \mathbf{S}_i']_{(\mathrm{mod}\, p_i)}$. The maximum frame size is then $N = \prod_i p_i^{m_i(m_i+3)/2}$ with maximum coherence $p_1^{-1/2}$ and thus a maximum minimum distance never less than $1/\sqrt{2} \approx 0.71$. Again if $p_1 = 2$, the first block $\mathbf{S}_1$ can be further extended to be in $S_{m_1}^+$ with offdiagonal entries equal to 0, 1/2, 1 or 3/2.

To construct sub-frames with larger distance, the $\mathbf{S}_k$ should be carefully selected. Some specific examples for $D = p_1 p_2$ and $D = 2^{m_1} 3$ are given in Tables I and II, respectively, and further described below.

1) Examples for $D = p_1 p_2$: In this case, D is the product of two primes and each $\mathbf{S}_k$ reduces to a scalar in $\mathbb{Z}_{p_k}$. In BD1, the same scalar is used on each diagonal element providing two rank-one differences among a maximum of p_1 matrices. In BD2, all other values in $\mathbb{Z}_{p_2}$ for the 2nd diagonal element are considered such that there is always a rank-one difference on the 2nd element. In BD3, all possible values in both diagonal elements are considered so that they have least at a rank-one difference in one of the two elements.

2) Examples for $D = 2^{m_1} \cdot 3$: In this case, the first block is a $m_1 \times m_1$ matrix while the second block is a scalar. Good frames are found by limiting the first block to be inside the corresponding Kerdock set or cosets of the Kerdock set. In BD4, the first block is limited to only three matrices in the Kerdock set K_{m_1} such that it can be uniquely associated to a ternary number in the second block. In BD5, the first block is any matrices from K_{m_1}, while the second block is a fixed ternary value e.g. 0.

BD6 is specific to $N = 12$, in this case the first block is any binary matrix in three different cosets of the Kerdock set K_2, where one coset leader is in $\mathrm{S}_2 = \mathrm{DG}(2, \frac{1}{2})$ but not in K_2, and another coset leader is in the extension S_2^+ but not in S_2. Here, S_2 contains only one non-trivial coset of K_2, and so another coset can only be found in S_2^+. BD7 is similar to BD6 but for $m_1 \geq 3$, the first block is any binary matrix in three different cosets of the Kerdock set K_{m_1} where two coset leaders are in the DG set $\mathrm{DG}(m_1, 1)$ but not in K_{m_1}. For both BD6 and BD7, the second block is a ternary number uniquely associated to a coset leader of the first block.

BD8 is the largest type of the general BD construction as described above and BD9 is its extension using $\mathrm{S}_{m_1}^+$.

C. Extended BD (EBD) Constructions

The BD constructions above lead to good frames, notably for the smallest size cases. Next, we show that it is possible to subsequently enlarge some of these previous constructions without sometimes even affecting the minimum distance by considering specific non-zero off-blockdiagonal entries.

A good choice for the off-blockdiagonal entries is to limit them to multiples of the first prime factor as $(\rho \cdot c \cdot p_1/2)$ where

TABLE V
EBD CONSTRUCTIONS FOR $D = 24$.

	$\mathcal{S}$	μ^2	N
EBD8	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2c\mathbf{1}_{3\times 1} \\ 2c\mathbf{1}_{1\times 3} & 2b_0 \end{bmatrix} : \mathbf{A} \in \mathrm{K}_3, c \in \mathbb{Z}_3, b_0 \text{ fixed} \right\}$	$2^{-6} \cdot 3^2$	$2^6 \cdot 3^2$
EBD9	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b_0 \end{bmatrix} : \mathbf{A} \in \mathrm{K}_3, \mathbf{c} \in \mathbb{Z}_3^2, b_0 \text{ fixed} \right\}$	2^{-2}	$2^6 \cdot 3^4$
EBD10	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c}^{\mathrm{T}} \\ 2\mathbf{c}^{\mathrm{T}} & 2b_i \end{bmatrix} : \mathbf{A} \in \{\mathbf{A}_i + \mathrm{K}_3\} \text{ where } \mathbf{A}_0 = 0, \mathbf{A}_1, \mathbf{A}_2 \in (\mathrm{S}_3 \setminus \mathrm{K}_3), \text{ and } \mathbf{c} \in \mathbb{Z}_3^3 \right\}$	≈ 0.311	$2^6 \cdot 3^5$
EBD11	$\left\{ \begin{bmatrix} \frac{3}{2}\mathbf{A} & 2\mathbf{c} \\ 2\mathbf{c}^{\mathrm{T}} & 2b \end{bmatrix} : \mathbf{A} \in \mathrm{S}_3, \mathbf{c} \in \mathbb{Z}_3^3, b \in \mathbb{Z}_3 \right\}$	2^{-1}	$2^9 \cdot 3^5$

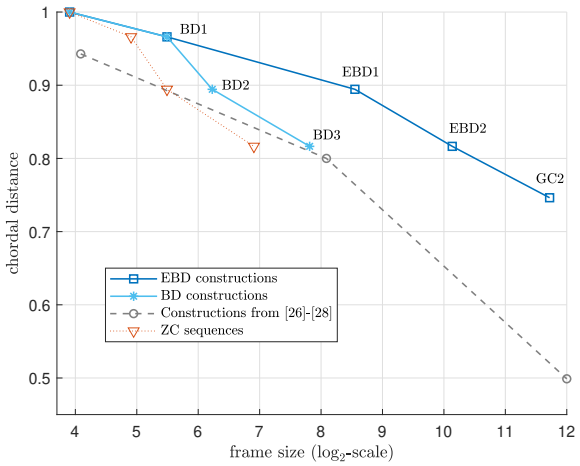

Fig. 2. Constructions in $D = 15$.

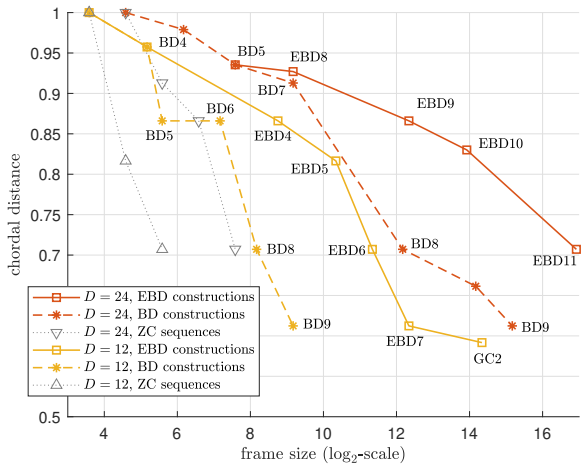

Fig. 3. Constructions in $D = 12$ and 24.

$c \in \mathbb{Z}_{q/p_1}$ and ρ can be any integer such that $(\rho \mod q/p_1) \neq 0$. Without loss of generality we can select $\rho = 2$ such that the off-blockdiagonal values are then any $c \cdot p_1$ with $c \in \mathbb{Z}_{q/p_1}$. In the same manner, a kth good choice of off-blockdiagonal values would be $(c \cdot p_k)$ with $c \in \mathbb{Z}_{q/p_k}$.

Examples of such constructions for $N = p_1 p_2$ are given in Table III. The construction EBD1 and EBD2 enlarges the construction BD2 and BD3, respectively, without decreasing the minimum distance.

Examples of such constructions for $N = 12 = 2^2 \times 3$ and $N = 24 = 2^3 \times 3$ are given in Tables IV and V, respectively. EBD4, EBD6 and EBD7 extends BD5, BD8 and BD9, respectively, for $D = 12$ without decreasing the minimum distance. EBD8 and EBD9 extends BD5 for $D = 24$ but here with a decrease of minimum distance. EBD10 extends BD7 as here again three cosets of the Kerdock set are selected for the first block uniquely associated with a value in the second diagonal block. EBD11 is the counterpart construction of EBD6 for $D = 24$, extending also BD8 without decreasing the minimum distance.

D. Illustrations and Comparisons

The obtained minimum chordal distances as a function of the frame sizes from Tables I and III are plotted for $D = 15$ in Fig. 2. Similarly, Fig. 3 shows the constructions of Tables II, IV and V for $D = 12$ and 24.

On both figures, the proposed constructions are compared to Zadoff-Chu (ZC) sequences [23]. Such comparison is relevant because they lead to frames with very same structure, derived from a similar alphabet, and being a collection of bases where each basis is a product of Hadamard matrix with a mask sequence which is the exponentiation by a single-variate quadratic polynomial [24]. If D is a prime, ZC sequences correspond to $D - 1$ MUBs. However, if D is not a prime, this generates much fewer bases with rather poor cross-correlation properties [25]. The proposed construction exploits more degrees of freedom in the polynomial phase construction and is therefore better than ZC sequences for non-prime-power dimensions.

For $D = 15 = 2^4 - 1$ in Fig. 2, the constructions are also compared to the nested codebook family [26]–[28] with 4- and 8-root of unity alphabet which can be applied to non-prime dimensions of the form $2(2^m - 1)$ and $(2^m - 1)$. Such constructions have a smaller size or lower minimum distance than the constructions discussed in this paper, which is reasonable as they are constrained to smaller alphabets.

IV. CONCLUSIONS

A framework for constructing families of Grassmannian frames with root-of-unity alphabet in any dimension D was presented. Generalizing Reed-Muller Grassmannian frames specific to power-of-two dimensions, frames were constructed by exponentiating multiple quadratic forms defined based on the prime decomposition of D, and multiplying the resulting sequences with the columns of a generalized Hadamard matrix. Explicit constructions with good minimum chordal distance were identified and discussed in dimensions relevant to practical applications, as e.g. for transmitting a multi-dimensional constellation in a physical resource block of $D = 12$ subcarriers as defined in 3GPP standards.

REFERENCES

[1] J. H. Conway, R. H. Hardin, and N. J. A. Sloane, "Packing lines, planes, etc.: Packings in Grassmannian space," *Exper. Math.*, vol. 5, pp. 139–159, 1996.

[2] T. Strohmer and R. W. Heath Jr, "Grassmannian frames with applications to coding and communication," *Applied and computational harmonic analysis*, vol. 14, no. 3, pp. 257–275, 2003.

[3] A. R. Calderbank, E. M. Rains, P. M. 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, July 1998.

[4] 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, no. 2, p. 129–140, Mar. 1999.

[5] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[6] R. W. Heath, T. Strohmer, and A. J. Paulraj, "On quasi-orthogonal signatures for CDMA systems," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1217–1226, Mar. 2006.

[7] D. J. Love, R. W. Heath, 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.

[8] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–564, Mar. 2000.

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

[10] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE J. Sel. Topics Sig. Proc.*, vol. 4, no. 2, pp. 358–374, Apr. 2010.

[11] H. Ji, S. Park, and B. Shim, "Sparse vector coding for ultra reliable and low latency communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6693–6706, Oct. 2018.

[12] B. Tahir, S. Schwarz, and M. Rupp, "Joint codebook design for multi-cell NOMA," in *Proc. IEEE Int. Conf. Acoustics, Speech and Sig. Proc.*, May 2019, pp. 4814–4818.

[13] H. Zhang, R. Li, J. Wang, Y. Chen, and Z. Zhang, "Reed-Muller sequences for 5G grant-free massive access," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–7.

[14] R. Calderbank and A. Thompson., "CHIRRUP: a practical algorithm for unsourced multiple access," *math.ST arXiv:1811.00879*, Nov. 2018.

[15] R. Calderbank and S. Jafarpour, "Reed Muller sensing matrices and the LASSO," in *Proc. Int. Conf. Sequences and Their Applications*. Springer, 2010, pp. 442–463.

[16] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[17] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," in *Proc. London Math. Soc*, vol. 75, no. 3, May 1997, p. 436–480.

[18] 3GPP TS 36.211, "LTE; evolved universal terrestrial radio access (E-UTRA); physical channels and modulation," V10.0.0, Jan. 2011.

[19] 3GPP TS 38.211, "NR; physical channels and modulation," v. 15.0.0, Dec. 2017.

[20] P. Delsarte and J. Goethals, "Alternating bilinear forms over GF(q)," *J. Combin. Th. A*, vol. 19, p. 26–50, 1975.

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

[22] R.-A. Pitaval, O. Tirkkonen, and S. D. Blostein, "Low complexity MIMO precoding codebooks from orthoplex packings," in *IEEE Int. Conf. Commun.*, July 2011, pp. 1–5.

[23] B. M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1406–1409, July 1992.

[24] B. M. Popovic, "Quasi-orthogonal supersets," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2011, pp. 155–159.

[25] J. W. Kang, Y. Whang, B. H. Ko, and K. S. Kim, "Generalized cross-correlation properties of Chu sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 438–444, Jan. 2012.

[26] S. Boztas, R. Hammons, and P. Y. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 1101–1113, May 1992.

[27] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons, "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579–592, Mar. 1996.

[28] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 456–468, Mar. 1995.