Frames for Linear Reconstruction without Phase

Bernhard G. Bodmann
Department of Mathematics
University of Houston
Houston, TX 77204-3008

Pete Casazza
and Dan Edidin
Department of Mathematics
University of Missouri
Columbia, MO 65211-4100

Radu Balan
Mathematics Department
and CSCAMM
University of Maryland
College Park, MD 20742

Abstract— **The objective of this paper is the linear reconstruction of a vector, up to a unimodular constant, when all phase information is lost, meaning only the magnitudes of frame coefficients are known. Reconstruction algorithms of this type are relevant for several areas of signal communications, including wireless and fiber-optical transmissions. The algorithms discussed here rely on suitable rank-one operator valued frames defined on finite-dimensional real or complex Hilbert spaces. Examples of such frames are the rank-one Hermitian operators associated with vectors from maximal sets of equiangular lines and maximal sets of mutually unbiased bases. We also study erasures and show that in addition to loss of phase, a maximal set of mutually unbiased bases can correct up to one lost frame coefficient occurring in each basis except for one without loss.**

I. Introduction

Maximizing bandwidth is a high priority in today's digital communications. Analog transmissions, whether wireless or via optical fibers, have to exhaust what is physically possible for the given medium. To this end, transmissions send parallel streams of data, e.g., from antenna arrays through a number of links to the receiver, or through multiple electromagnetic modes in an optical fiber. The benefit of using analog channels in parallel comes, however, at the cost of an increased susceptibility to oscillator instabilities and of a resulting loss of coherence in the transmission.

The purpose of this paper is to investigate linear encoding and decoding strategies for analog signals that use redundancy to overcome the dependence on phase information. In other words, we are concerned with the question of reconstructing a vector in a finite-dimensional real or complex Hilbert space when only the magnitudes of the coefficients of the vector under a linear map are known. In a previous paper [BCE06], part of the authors discussed this problem in the context of signal processing, in particular the analysis of speech. It was shown that the magnitudes of inner products with a generic set containing a sufficient number of (frame) vectors characterize each vector, up to a unimodular constant. However, at least in the complex case, reconstruction algorithms were difficult to implement.

To obtain the linear algorithms presented here, we use that characterizing a vector x in a Hilbert space, up to a unimodular factor, is equivalent to reconstructing the rank-one Hermitian operator $x \otimes x^*$. After "squaring" the vector, we rely on operator-valued frames which provide linear reconstruction formulas. The same strategy appears under the name of state tomography in quantum theory, see e.g. [RBSC04] or [Sco06]. While the quantum literature emphasizes the design of minimal measurements (smallest number of frame coefficients) to characterize an unknown operator $x \otimes x^*$ with x of unit-norm ([Fin04], [FSC05]), we focus on efficient reconstruction algorithms once the frame coefficients are known. This paper presents a linear reconstruction algorithm which requires at least $N = d^2$ linear coefficients in the complex case and $N = d(d+1)/2$ in the real case.

In addition, we consider the situation when coefficients are lost, e.g. in the course of a data transmission ([GKK01], [KDG02], [CK03], [BP05], [Bod07]). We investigate which of the encoding strategies provide a correction mechanism for erasures. To correct up to d erasures in the complex case or $d/2$ in the real case, in addition to loss of phase information, we require $N = d(d+1)$ or $N = d(d/2+1)$ transmitted coefficients, respectively. Moreover, we require that for a given partition of the coefficients in subsets of size d, at most one loss occurs within each subset.

The organization of the paper is as follows. Section II introduces the notion of operator-valued frames. Section III presents examples of frames which provide a linear reconstruction algorithm from the magnitudes of frame coefficients, described in Section IV. Finally, Section V discusses the correction of erasures.

II. From Frames to Operator-Valued Frames

In this section we introduce the main idea in this paper: Reconstructing a vector in a Hilbert space, up to a unimodular constant, from the magnitudes of its frame coefficients, is equivalent to reconstructing the rank-one Hermitian operator $x \otimes x^*$ from its expansion with respect to an operator-valued frame.

Definition 2.1: Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space. A finite family of vectors $\mathcal{F} = \{f_1, f_2, \dots f_N\} \in \mathcal{H}^N$ is called a **frame**, if there are non-zero constants A_1 and A_2 such that for all $x \in \mathcal{H}$,

$$A_1 \|x\|^2 \leq \sum_{j=1}^{N} |\langle x, f_j \rangle|^2 \leq A_2 \|x\|^2 \,.$$

With each frame, we associate its **Grammian** $G = (\langle f_j, f_l \rangle)_{j,l=1}^N$, the matrix formed by the inner products of the frame vectors.

If we can choose $A_1 = A_2 = A$ in the above chain of inequalities, then the frame is called A-tight. If, in addition, there is $b > 0$ such that $\|f_j\| = b$ for all $j \in \{1, 2, \dots N\}$, then we call the family $\{f_j\}_{j=1}^N$ a **uniform** A-tight frame. Such frames are also called equal-norm tight frames.

A family of vectors $\mathcal{F}$ is a frame for a finite-dimensional Hilbert space $\mathcal{H}$ if and only if it spans $\mathcal{H}$, because then it contains a linearly independent, spanning subset, and thus it is straightforward to verify the norm inequalities in Definition 2.1.

If $\mathcal{F}$ is an A-tight frame, then any vector $x \in \mathcal{H}$ can be reconstructed from the sequence of frame coefficients $\{\langle x, f_j\rangle\}_{j=1}^N$ according to

$$x = \frac{1}{A}\sum_{j=1}^{N}\langle x, f_j\rangle f_j \, .$$

The reconstruction identity is equivalent to the matrix $\frac{1}{A}G$ being an orthogonal rank-d projection. Thus, $d = \frac{1}{A}\operatorname{tr}[G] = \frac{1}{A}\sum_{j=1}^N \|f_j\|^2$ implies that all the frame vectors in an A-tight uniform frame have the same norm

$$b = \sqrt{\frac{Ad}{N}} \, .$$

With a frame $\mathcal{F} = \{f_j\}_{j=1}^N$, we associate the set of rank-one Hermitian operators $\mathcal{S} = \{f_j \otimes f_j^*\}_{j=1}^N$ on $\mathcal{H}$.

Definition 2.2: Let $\{f_j\}_{j=1}^N$ be a frame for a Hilbert space $\mathcal{H}$. Let $S_j = f_j \otimes f_j^*$ denote the rank-one Hermitian operator associated with each f_j. Let $\mathcal{X}$ be the span of the family $\mathcal{S} = \{S_j\}_{j=1}^N$, equipped with the Hilbert-Schmidt inner product. We say that $\{S_j\}_{j=1}^N$ is the **operator-valued frame** for $\mathcal{X}$ associated with $\{f_j\}_{j=1}^N$. The Grammian H of $\mathcal{S}$ has entries $H_{j,k} = \operatorname{tr}[S_j S_k] = |\langle f_j, f_k\rangle|^2$.

In the following, we want to find conditions which guarantee that $\mathcal{X}$ contains all rank-one Hermitian operators. We then say that the operator-valued frame $\mathcal{S}$ has **maximal span**.

Proposition 2.3: Let $\{f_j\}_{j=1}^N$ be a frame for a real or complex Hilbert space $\mathcal{H}$ and $\mathcal{S}$ the associated operator-valued frame with span $\mathcal{X}$. The rank of the Grammian H is at most $d(d+1)/2$ in the real case or d^2 if $\mathcal{H}$ is complex. Moreover, the rank of H is maximal if and only if $\mathcal{X}$ contains all rank-one Hermitian operators on $\mathcal{H}$.

Proof: We note that the space $\mathcal{Q}$ spanned by all rank-one Hermitian operators has dimension $d(d+1)/2$ or d^2 in the real or complex case, respectively. Since $\mathcal{S}$ contains only such rank-one operators, $\mathcal{X} \subset \mathcal{Q}$ and the rank of H as well as the dimension of $\mathcal{X}$ can be at most $d(d+1)/2$ or d^2, respectively. Moreover, if the rank of H, and thus the dimension of $\mathcal{X}$, is maximal, then $\mathcal{X} = \mathcal{Q}$. ■

Corollary 2.4: If $\{f_j\}_{j=1}^N$ is a frame for a real or complex Hilbert space $\mathcal{H}$ and $\mathcal{S}$ the associated operator-valued frame with linear span $\mathcal{X}$, which contains all rank-one Hermitian operators, then $N \geq d(d+1)/2$ in the real case and $N \geq d^2$ in the complex case

Proof: By the preceding theorem, we require the rank of H to be $d(d+1)/2$ or d^2 in the real or complex case, respectively. This provides the desired lower bound for N, because the rank of the $N \times N$ matrix H can be at most N. ■

If the operator-valued frame $\{S_j\}_{j=1}^N$ associated with $\mathcal{F}$ has maximal span, then we can reconstruct any operator $x \otimes x^*$ from its Hilbert-Schmidt inner products with the family $\{S_j\}_{j=1}^N$. Since the values of these inner products are

$$\operatorname{tr}[x \otimes x^* S_j] = |\langle x, f_j\rangle|^2 \, ,$$

and $x \otimes x^*$ determines x up to a unimodular constant, this amounts to reconstructing x from the magnitudes of its frame coefficients with respect to the frame $\mathcal{F} = \{f_j\}_{j=1}^N$.

III. Operator-Valued Frames with Maximal Span

In this section we discuss types for frames for which the associated operator-valued frame has maximal span.

For this purpose, we consider uniform tight frames with the property that the magnitudes of the inner products between frame vectors form a small set. If this set has size one, we call the frame 2-uniform [HP04], [BP05] or (equal-norm) equiangular tight frame [vLS66], [LS73], [SH03], [VW05]. Another type of frame, for which this set has size two, is obtained from a number of bases for a Hilbert space which are chosen in such a way that, between basis vectors belonging to different bases, their inner products have a fixed magnitude. These frames are referred to as sets of mutually unbiased bases.

Definition 3.1: A family of vectors $\mathcal{F} = \{f_j\}_{j=1}^N$ is said to form a **2-uniform** or **equiangular** A-tight frame if it is uniform and if there is $c > 0$ such that for all pairs of frame vectors f_j and f_k, $j \neq k$, we have $|\langle f_j, f_k\rangle| = c$.

Using that G is a scaled projection, we obtain $d = \frac{1}{A}\operatorname{tr}[G] = \frac{1}{A^2}\operatorname{tr}[G^2] = \frac{1}{A^2}\sum_{j,k=1}^N |\langle f_j, f_k\rangle|^2$ which, together with the known value for the diagonal of G, determines the constant c in Definition 3.1,

$$c = \frac{A}{N}\sqrt{\frac{d(N-d)}{N-1}}.$$

An observation of Lemmens and Seidel [LS73] characterizes when the operator-valued frame associated with an equiangular tight frame has maximal span.

Proposition 3.2: Let $\mathcal{H}$ be a real or complex Hilbert space, and $\mathcal{F} = \{f_1, f_2, \dots f_N\}$ an equal-norm equiangular tight frame. Then operator-valued frame $\mathcal{S}$ associated with $\mathcal{F}$ has maximal span if and only if the frame consists of $N = d(d+1)/2$ or $N = d^2$ vectors in the real or complex case, respectively.

Proof: We observe that the Grammian H of the associated operator-valued frame, $H_{j,k} = |\langle f_j, f_k\rangle|^2$, is of rank N because $H = (b^2 - c^2)I + c^2 J$, the matrix J containing all 1's is non-negative and $b > c$. Thus, the span of $\mathcal{S}$ is maximal if and only if $N = d(d+1)/2$ or $N = d^2$ vectors, depending on whether $\mathcal{H}$ is real or complex. ■

For examples of such frames, see [WF89], [HP04], [BP05], [App05], [GR05]. We quote a simple example for a two-dimensional real or complex Hilbert space.

Example 3.3: Let $\{e_1, e_2\}$ denote the canonical basis for either $\mathbb{R}^2$ or $\mathbb{C}^2$.

We first consider the Hilbert space $\mathbb{R}^2$. Let R be the rotation matrix such that $R^3 = I$ and $R \neq I$. Choose $f_1 = e_1$, $f_2 = Re_1$ and $f_3 = R^2 e_1$. Then $\{f_1, f_2, f_3\}$ is a 2-uniform 3/2-tight frame with $|\langle f_i, f_j\rangle| = 1/2$ for $i \neq j$. This frame is sometimes called the Mercedes-Benz frame.

For the case of $\mathbb{C}^2$, we introduce the unitary Pauli matrices $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Let $f_1 = \alpha e_1 + \beta e_2$ where $\alpha = \sqrt{\frac{1}{2}(1 - \frac{1}{\sqrt{3}})}$ and $\beta = e^{(\frac{5\pi}{4})i}\sqrt{\frac{1}{2}(1 + \frac{1}{\sqrt{3}})}$, and let $f_2 = Xf_1$, $f_3 = Zf_1$, $f_4 = XZf_1$. Then $\{f_1, \ldots, f_4\}$ is an equal-norm equiangular 2-tight frame with $|\langle f_i, f_j\rangle| = \frac{1}{\sqrt{3}}$ for all $i \neq j$.

Mutually unbiased bases form another type of frame which has an associated operator-valued frame with maximal span. This type of frame contains vectors from a number of orthonormal bases for a Hilbert space which are chosen in such a way that, between basis vectors belonging to different bases, their inner products have a fixed magnitude.

Definition 3.4: Let $\mathcal{H}$ be a real or complex Hilbert space of dimension d. A family of vectors $\{e_k^{(j)}\}$ in $\mathcal{H}$ indexed by $k \in \mathbb{K} = \{1, 2, \ldots d\}$ and $j \in \mathbb{J} = \{1, 2, \ldots m\}$ is said to form **m mutually unbiased bases** if for all $j, j' \in \mathbb{J}$ and $k, k' \in \mathbb{K}$ the magnitude of the inner product between $e_k^{(j)}$ and $e_{k'}^{(j')}$ is given by

$$|\langle e_k^{(j)}, e_k^{(j')}\rangle| = \delta_{k,k'}\delta_{j,j'} + \frac{1}{\sqrt{d}}(1 - \delta_{j,j'}),$$

where Kronecker's δ symbol is one when its indices are equal and zero otherwise.

Proposition 3.5 (Delsarte, Goethals and Seidel [DGS77]): Let $\mathcal{H}$ be a real or complex Hilbert space, and $\mathcal{F} = \{f_1, f_2, \ldots f_N\}$ a frame formed by $m = d/2 + 1$ or $m = d + 1$ mutually unbiased bases, respectively. Then the operator-valued frame $\mathcal{S}$ associated with $\mathcal{F}$ has maximal span.

Proof: The Grammian H of the operator-valued frame associated with m mutually unbiased bases has the form $H = I_m \otimes I_d + (J_m - I_m) \otimes J_d/d$, where I_m and I_d are the $m \times m$ and $d \times d$ identity matrices, respectively, and J_m and J_d denote the $m \times m$ and $d \times d$ matrices containing only 1's. The kernel of the Grammian matrix is the space of vectors $a \otimes b$ such that $J_d b = db$ and $J_m a = 0$, so it is $m - 1$-dimensional. Consequently, the rank of H and thus the dimension of the span of $\mathcal{S}$ is $md - m + 1$. This shows that the maximal rank is achieved when there are $m = d + 1$ mutually unbiased bases in a d-dimensional complex Hilbert space $\mathcal{H}$ and $m = \frac{d}{2} + 1$ in the real case. For an alternative proof, see [WF89]. ■

Example 3.6: The simplest example of a set of mutually unbiased bases in a complex Hilbert space is the standard basis, together with the basis of eigenvectors of the Pauli matrices X and $Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

This example and others can be found in [BBRV02]. If d is prime, then there exists a maximal set of mutually unbiased bases called **discrete chirps**, see [CF06], [HCM06].

Example 3.7: Let d be a prime number, and ω a primitive d-th root of unity. Denote the canonical basis of $\mathbb{C}^d$ by $\{e_k^{(1)}\}_{k=1}^d$, then for $j \in \{2, 3, \ldots d + 1\}$,

$$e_k^{(j)} = \frac{1}{\sqrt{d}} \sum_{l=1}^{d} \omega^{-(j-1)l^2 + kl} e_l^{(1)}$$

defines together with the canonical basis a family of $d + 1$ mutually unbiased bases called the **discrete chirps**.

To see that these vectors form bases, we first consider inner products between vectors of same j. For $j = 1$, this is clear. If $j > 1$,

$$\langle e_{k'}^{(j)}, e_k^{(j)}\rangle = \frac{1}{d} \sum_{l=1}^{d} \omega^{k'l - kl} = \delta_{k,k'} .$$

The bases are mutually unbiased because if $j \neq j'$, and one of them is equal to one, then $|\langle e_{k'}^{(j')}, e_k^{(j)}\rangle| = 1/\sqrt{d}$. If neither basis index is equal to one, then

$$\langle e_{k'}^{(j')}, e_k^{(j)}\rangle = \frac{1}{d} \sum_{l=1}^{d} \omega^{-j'l^2 + jl^2 + k'l - kl}$$

and by completing the square and using cyclicity

$$|\langle e_{k'}^{(j')}, e_k^{(j)}\rangle| = \frac{1}{d} \left| \sum_{l=1}^{d} \omega^{l^2} \right| .$$

Now squaring this expression yields

$$|\langle e_{k'}^{(j')}, e_k^{(j)}\rangle|^2 = \frac{1}{d^2} \sum_{l,l'=1}^{d} \omega^{l^2 - (l')^2} = \frac{1}{d^2} \sum_{l,l'=1}^{d} \omega^{(l+l')(l-l')} = \frac{1}{d} .$$

Remark 3.8: A similar construction applies when d is a power of a prime [WF89]. If d is not prime, then the maximal number of mutually unbiased bases is generally unknown ([GR05]). In the real case, even in the case of prime dimensions, the construction of maximal sets of mutually unbiased bases is more difficult ([BSTW]), but at least for d a power of 4 this is possible, see [CS73], [CCKS97].

IV. Reconstruction of a vector from absolute values of its frame coefficients

The main motivation for this paper is to find a reconstruction formula for vectors in a finite-dimensional Hilbert space $\mathcal{H}$ equipped with a frame $\{f_j\}_{j=1}^N$ such that only the absolute values of the frame coefficients $\{\langle x, f_j\rangle\}_{j=1}^N$ are needed to determine each vector x up to a unimodular constant. This is equivalent to identifying the self-adjoint rank-one operator $x \otimes x^*$, given by $x \otimes x^* y = \langle y, x\rangle x$, $y \in \mathcal{H}$, from its Hilbert-Schmidt inner products with $\{S_j\}_{j=1}^N$. For this reason, our computations are mostly formulated in terms of operator-valued frames.

Theorem 4.1: Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space and $F = \{f_1, f_2, \ldots f_N\}$ an N/d-tight frame such that the associated operator-valued frame $\mathcal{S}$ has maximal span. Let M be the pseudo-inverse of the Grammian H, so $HMH = H$, and denote the canonical dual of $\mathcal{S}$ as $\mathcal{R}$, containing operators $R_j = \sum_{k=1}^N M_{j,k} S_k$. Given a vector $x \in \mathcal{H}$, then

$$x \otimes x^* = \sum_{j=1}^N |\langle x, f_j \rangle|^2 R_j \,.$$

Proof: Instead of deriving the claimed identity, we show that both sides coincide after taking their Hilbert-Schmidt inner product with any operator $y \otimes y^*$, $y \in \mathcal{H}$. Inserting the expression for R_j means we have to prove the identity

$$|\langle x, y \rangle|^2 = \sum_{j,k=1}^N |\langle x, f_j \rangle|^2 M_{j,k} |\langle f_k, y \rangle|^2$$

for all $y \in \mathcal{H}$. Using that $x \otimes x^* = \sum_{l=1}^N c_l f_l \otimes f_l^*$ with some coefficients $\{c_l\}$ by the maximality of the span of $\mathcal{S}$ and similarly $y \otimes y^* = \sum_{l'=1}^N c'_{l'} f_{l'} \otimes f_{l'}^*$, the matrix identity $HMH = H$ yields that both sides are equal to $\sum_{l,l'=1}^N c_l c'_{l'} H_{l,l'}$. ■

After this general result, we consider the examples of equiangular frames and of mutually unbiased bases.

Corollary 4.2: Let $\mathcal{H}$ be a complex Hilbert space. If $\mathcal{F}$ is an equal-norm equiangular N/d-tight frame or a tight frame formed by mutually unbiased bases, and the associated operator-valued frame $\mathcal{S}$ has maximal span, then the reconstruction identity becomes

$$x \otimes x^* = \frac{d(d+1)}{N} \sum_{j=1}^N |\langle x, f_j \rangle|^2 (f_j \otimes f_j^* - I/(d+1)) \,.$$

Proof: This result follows from the preceding theorem by proving that the canonical (Hilbert-Schmidt) dual of $\{S_j\}$ is $\{R_j\}$ with $R_j = d(d+1)S_j/N - dI/N$. Let $0 < c = |\langle f_j, f_k \rangle|$ for any $j \neq k$ if the frame is equiangular and a non-orthogonal pair if it consists of mutually unbiased bases. Since the frame vectors are normalized in either case, it is straightforward to verify that $\mathrm{tr}[S_j R_j] = d^2/N$. If $j \neq k$,

$$\mathrm{tr}[S_j R_k] = \frac{d(d+1)}{N} |\langle f_j, f_k \rangle|^2 - \frac{d}{N} \,.$$

If $\mathcal{F}$ is equiangular, then $|\langle f_j, f_k \rangle|^2 = c^2 = (N-d)/d(N-1) = 1/(d+1)$ and consequently $\mathrm{tr}[S_j R_k] = 0$.

In the case of mutually unbiased bases, we have either $\mathrm{tr}[S_j R_k] = -d/N$ if the indices j and k belong to two vectors from the same basis, or $|\langle f_j, f_k \rangle|^2 = 1/d$ and $\mathrm{tr}[S_j R_k] = 1/N$. Thus, the matrix K with entries $K_{j,k} = \mathrm{tr}[S_j R_k]$ has the form $K = \frac{d(d+1)}{N} I_{d+1} \otimes I_d - \frac{1}{N}((d+1)I_{d+1} - J_{d+1}) \otimes J_d$, where the first component specifies the basis and the second refers to the index within each basis. Since $N = d(d+1)$, K can be identified as a rank-d^2 orthogonal projection with the same range as H. This shows that in both cases, whether equiangular tight frame or mutually unbiased bases, $\{R_j\}_{j=1}^N$ is the canonical dual of the operator-valued frame $\{S_j\}_{j=1}^N$. ■

From a practical point of view, the above corollary gives an algorithm that allows us to reconstruct x, up to an overall unimodular constant, by considering one non-vanishing row of the $d \times d$ matrix $x \otimes x^*$.

V. Loss of Phase and Erasures

In this section, we show that a maximal set of mutually unbiases bases admits the reconstruction from magnitudes of frame coefficients even if some of these coefficients are lost. Since we want to reconstruct linearly from the remaining coefficients, the operator-valued frame must retain maximal span after removing elements corresponding to erased coefficients.

Definition 5.1: Let $\{e_j\}_{j=1}^N$ be a frame for a real or complex Hilbert space $\mathcal{H}$ and $\mathcal{S} = \{S_j\}_{j=1}^N$ the associated operator-valued frame. We call an erasure of coefficients indexed with $\mathbb{L} \subset \mathbb{J} = \{1, 2, \dots N\}$ **correctible** if the set $\{S_j\}_{j \in \mathbb{J} \setminus \mathbb{L}}$ is a frame for the span of all rank-one Hermitian operators.

By rank considerations, it is clear that an equiangular tight frame cannot admit erased coefficients. However, since the number of frame vectors coming from a maximal family of mutually unbiased bases is larger than the dimension of the space spanned by all Hermitian rank-one operators, we expect that possibly, lost coefficients are correctible. This is indeed the case for at most one lost coefficient in each basis, as long as the coefficients belonging to at least one basis are not lost.

Theorem 5.2: Let $\mathcal{H}$ be a real or complex Hilbert space of dimension d. Let $\{e_k^{(j)} : k \in \mathbb{K}, j \in \mathbb{J}\}$, $\mathbb{K} = \{1, 2, \dots d\}$, $\mathbb{J} = \{1, 2, \dots m\}$, be a family of m mutually unbiased bases for $\mathcal{H}$ such that the associated operator-valued frame $\{S_k^{(j)}\}_{j \in \mathbb{J}}$ has maximal span. If for each $j \in \mathbb{J}$, $\mathbb{L}_j \subset \mathbb{K}$ is of size at most one, and for at least one j, $\mathbb{L}_j = \emptyset$, then $\{S_k^{(j)} : j \in \mathbb{J}, k \in \{1, 2, \dots d\} \setminus \mathbb{L}_j\}$ has maximal span.

Proof: As before, the span of the operators $\{S_k^{(j)} : j \in \mathbb{J}, k \in \mathbb{K} \setminus \mathbb{L}_j\}$ is maximal if and only if the rank of the Grammian H is.

We consider the equation $Ha = 0$, where we view H as a block matrix with blocks labeled by the basis indices such that $H^{(j,j)} = I_{d_j}$ for diagonal blocks and $H^{(j,l)} = J_{d_j,d_l}/d$ for the off-diagonal blocks.

Collecting the entries of the vector a belonging to one basis index j in $a^{(j)}$, we deduce from $a^{(j)} = \sum_l J_{d_j,d_l} a^{(l)}$ that all of its entries are identical, $a_k^{(j)} = \alpha_j$, for each $j \in \{1, 2, \dots m\}$.

This means for each solution a of $Ha = 0$, there is a corresponding solution $H'\alpha = 0$, where each diagonal block $H^{(j,j)}$ in the matrix H has been replaced by the eigenvalue 1 of $a^{(j)}$ and each off-diagnal block $H^{(j,l)}$ by $\delta_l = 1 - |\mathbb{L}_l|/d$ to obtain H'.

We assume that we have ordered the blocks in such a way that $\{\delta_l\}_{l=1}^m$ is increasing. Since at least one $\mathbb{L}_j$ is empty, there is $r \geq 0$ such that $\delta_j = 1$ for all $j > r$. Thus, the last $m - r$ columns of H' contain 1's. Moreover taking the difference between consecutive rows of H' gives the equation $H''\alpha = 0$

with

$$H'' = \begin{pmatrix} 1 & \delta_2 & \delta_3 & \dots & \delta_r & 1 & \dots & 1 \\ \delta_1 - 1 & 1-\delta_2 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \delta_2 - 1 & 1-\delta_3 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & & \dots & \\ 0 & \dots & \dots & 0 & \delta_r - 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 & 0 & \dots & \\ 0 & \dots & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Since we assumed $\delta_r \neq 1$, we conclude $\alpha_r = 0$. Now using the identity $(\delta_{j-1}-1)\alpha_{j-1} = (\delta_j - 1)\alpha_j$ from rows $2 \leq j \leq r$, it can be verified that $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 0$. This means, $H''\alpha = 0$ if and only if the first r entries of α vanish and $\sum_{j>r} \alpha_j = 0$, which is a space of solutions of dimension $m - r - 1$.

Since we assumed $m-r$ empty sets among the family $\{\mathbb{L}_j\}$, the Grammian H is an $(md - r) \times (md - r)$ matrix of rank $md - r - (m - r - 1) = m(d - 1) + 1$.

In the real case, the rank is $(d/2+1)(d-1)+1 = d(d+1)/2$, in the complex case, $(d+1)(d-1)+1 = d^2$. This means, the rank of H is maximal. ■

VI. Conclusion

Maximal equal-norm equiangular tight frames and maximal sets of mutually unbiased bases provide simple reconstruction algorithms that only use the magnitudes of frame coefficients. We have linked the reason for the existence of these algorithms to the associated rank-one operator valued frames with maximal span. In addition, we have seen that using mutually unbased bases provides an error-correction mechanism for up to one erasure per basis, with one basis without losses.

References

[App05] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, J. Math. Phys. **46** (2005), no. 5, 052107/1-29.

[BCE06] R. Balan, P. Casazza, D. Edidin, *On signal reconstruction without phase*, Appl. Comput. Harmon. Anal. **20** (2006), 345–356.

[BBRV02] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, *A new proof for the existence of mutually unbiased bases*, Algorithmica **34** (2002), no. 4, 512–528, Quantum computation and quantum cryptography.

[Bod07] B. G. Bodmann, *Optimal linear transmission by loss-insensitive packet encoding*, Appl. Comput. Harmon. Anal. **22** (2007), 274–285.

[BP05] B. G. Bodmann and V. I. Paulsen, *Frames, graphs and erasures*, Linear Algebra Appl. **404** (2005), 118–146.

[BSTW] P. O. Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan *Mutually unbiased bases and orthogonal decompositions of Lie algebras*, E-print: arXiv.org/quant-ph/0506089, to appear in Quantum Information and Computation, 2007.

[CCKS97] 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. (3) **75** (1997), no. 2, 436–480.

[CF06] P. G. Casazza and M. Fickus, *Fourier transforms of finite chirps*, EURASIP J. Appl. Signal Process. (2006), no. Frames and overcomplete representations in signal processing, communications, and information theory, Art. ID 70204, 1-7.

[CK03] P. Casazza and J. Kovačević, *Equal-norm tight frames with erasures*, Adv. Comp. Math. **18** (2003), 387–430.

[CS73] P. J. Cameron and J. J. Seidel, *Quadratic forms over $GF(2)$*, Indag. Math. **35** (1973), 1–8.

[DGS77] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6** (1977), no. 3, 363–388.

[Fin04] J. Finkelstein, Pure-state informationally complete and "really" complete measurements, Phys. Rev. A **70** (2004), 052107/1-3.

[FSC05] S. T. Flammia, A. Silberfarb and C. M. Caves, Minimal informationally complete measurements for pure states, Found. Phys. **35**, no. 12 (2005), 1985-2006.

[GR05] C. Godsil and A. Roy, Equiangular lines, mutually unbiased bases and spin models, 2005, E-print: arxiv.org/quant-ph/0511004.

[GKK01] V. K. Goyal, J. Kovačević, and J. A. Kelner, *Quantized frame expansions with erasures*, Appl. Comp. Harm. Anal. **10** (2001), 203–233.

[HCM06] S. D. Howard, A. R. Calderbank, and W. Moran, *The finite Heisenberg-Weyl groups in radar and communications*, EURASIP J. Appl. Signal Process. (2006), special issue on "Frames and overcomplete representations in signal processing, communications, and information theory," Art. ID 85685, 1-12.

[HP04] R. Holmes and V. I. Paulsen, *Optimal frames for erasures*, Lin. Alg. Appl. **377** (2004), 31–51.

[KDG02] J. Kovačević, P. L. Dragotti, and V. K. Goyal, *Filter bank frame expansions with erasures*, IEEE Trans. Inform. Theory **48** (2002), 1439–1450.

[KR05] A. Klappenecker and M. Rötteler, *Mutually unbiased bases are complex projective 2-designs*, Proc. Int. Symp. on Inf. Theory, IEEE, 2005, pp. 1740–1744.

[LFB87] R. G. Lane, W. R. Freight, and R. H. T. Bates, *Direct Phase Retrieval*, IEEE Trans. ASSP **35**, no. 4 (1987), 520–526.

[LS73] P. W. H. Lemmens and J. J. Seidel, *Equiangular lines*, J. Algebra **24** (1973), 494–512.

[Neu81] A. Neumaier, Combinatorial configurations in terms of distances, Memorandum 81-09 (Wiskunde), Eindhoven Univ.Technol., (1981).

[RBSC04] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys, **45**, no. 6, (2004), 2171-2180.

[Sco06] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, no. 43 (2006), 13507-13530.

[SH03] T. Strohmer and R. Heath, *Grassmannian frames with applications to coding and communcations*, Appl. Comp. Harm. Anal. **14** (2003), 257–275.

[vLS66] J. H. van Lint and J. J. Seidel, *Equilateral point sets in elliptic geometry*, Indag. Math. **28** (1966), 335–348.

[VW05] R. Vale and S. Waldron, *Tight frames and their symmetries*, Constr. Approx. **21** (2005), no. 1, 83–112.

[WF89] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Physics **191** (1989), no. 2, 363–381.