Painless Reconstruction from Magnitudes of Frame Coefficients

**Radu Balan · Bernhard G. Bodmann ·
Peter G. Casazza · Dan Edidin**

Abstract The goal of this paper is to develop fast algorithms for signal reconstruction from magnitudes of frame coefficients. This problem is important to several areas of research in signal processing, especially speech recognition technology, as well as state tomography in quantum theory. We present linear reconstruction algorithms for tight frames associated with projective 2-designs in finite-dimensional real or complex Hilbert spaces. Examples of such frames are two-uniform frames and mutually unbiased bases, which include discrete chirps. The number of operations required for reconstruction with these frames grows at most as the cubic power of the dimension of the Hilbert space. Moreover, we present a very efficient algorithm which gives reconstruction on the order of d operations for a d-dimensional Hilbert space.

Keywords Frames · Reconstruction without phase · Projective 2-designs

Mathematics Subject Classification (2000) Primary 42C15 · Secondary 05B20

R. Balan
Mathematics Department and CSCAMM, University of Maryland, College Park, MD 20742, USA

B.G. Bodmann (✉)
Department of Mathematics, University of Houston, Houston, TX 77204-3008, USA
e-mail: bgb@math.uh.edu

P.G. Casazza · D. Edidin
Department of Mathematics, University of Missouri, Columbia, MO 65211-4100, USA

1 Introduction

This paper is 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.

A previous paper [2] described the importance of this problem to signal processing, in particular to the analysis of speech. Surprisingly, the same problem appears in a slightly different guise under the name of state tomography in quantum theory [32, 33]. A pure quantum state is given by a rank-one projection on a finite-dimensional Hilbert-space, or equivalently, by the vectors in the range of this projection. A state is experimentally accessible only through the magnitudes of its Hilbert-Schmidt inner products with other states. These inner products of projections can be interpreted as the squared magnitudes of the inner products of corresponding normalized *vectors* in the respective range of the projections. Thus, reconstructing a pure quantum state is the same as finding a vector, up to a unimodular constant, from the magnitudes of linear transform coefficients. However, in contrast to a primary goal of quantum state tomography, which consists of minimizing the number of inner products to be measured [17, 18], we aim at a reconstruction algorithm that scales optimally with the dimension of the Hilbert space.

Of particular interest is the case when the coefficients of the unknown vector are obtained from a Windowed Fourier Transform (also known as Short-Time Fourier Transform), or an Undecimated Wavelet Transform (in audio and image signal processing). While [2] presents some necessary and sufficient conditions for reconstruction, the general problem of finding fast/efficient algorithms is wide open. For vectors in real Hilbert spaces, this is easily shown to be equivalent to a combinatorial problem. In [3] this problem is further proved to be equivalent to a (nonconvex) optimization problem. The case when the coefficients are obtained with the Discrete Fourier Transform (DFT) was widely studied in engineering literature during '70s and '80s. In particular, for the DFT of redundancy 2 (or higher), the reconstruction problem is shown to be solved by a spectral factorization problem of a para-hermitian polynomial (see [21]). Unfortunately, this result does not yield a simple algorithm to solve the problem. Instead, [30] proposes a simple algorithm to reconstruct the data vector when a redundant, windowed Fourier transform is used, which encodes a d-dimensional vector linearly in d^2 coefficients.

Using a completely different approach in this paper we obtain a simple algorithm which, interestingly enough, requires also a $N = d^2$ linear coefficients in the complex case and $N = d(d + 1)/2$ in the real case. Our approach is based on the concept of a *projective t-design* which originated in the context of combinatorial designs [31] (see also [22, 29]). Given an N/d-tight frame $F = \{f_1, f_2, \ldots, f_N\}$ such that the projections onto the lines spanned by the frame vectors form a projective 2-design in $P\mathcal{H}$, we obtain a linear reconstruction algorithm of a vector $x \in \mathcal{H}$, up to a unimodular constant. Based on this result, we construct explicit examples of frames that yield linear or quasi-linear reconstruction algorithms. The organization of the paper is as follows. Section 2 contains basic notations and definitions. Section 3 presents the projective t-design approach to the reconstruction problem. In Sect. 4 the reconstruction algorithm for mutually unbiased bases is presented, whereas Sect. 5 presents other types of frames which yield fast reconstruction.

2 Preliminaries

Definition 2.1 Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space. A finite family of vectors $\{f_1, f_2, \ldots, f_N\}$ is called an *A-tight frame*, with frame constant $A > 0$, if all $x \in \mathcal{H}$ can be reconstructed from the sequence of frame coefficients $\{\langle x, f_j \rangle\}_{j=1}^N$ according to

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

If there is $b > 0$ such that $\|f_j\| = b$ for all $j \in \{1, 2, \ldots, N\}$, then we call this family a *uniform A*-tight frame. Such frames are also called equal-norm tight frames.

Choosing an orthonormal basis $\{e_k\}_{k=1}^d$ in $\mathcal{H}$ and equating

$$d = \sum_{k=1}^d \|e_k\|^2 = \frac{1}{A} \sum_{j=1}^N \sum_{k=1}^d |\langle e_k, f_j \rangle|^2 = \frac{1}{A} \sum_{j=1}^N \|f_j\|^2$$

shows that the constant norm b for uniform A-tight frames in Definition 2.1 is given by

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

The uniform N/d-tight frames used in the latter part of this paper have 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 [6, 24]. Such tight frames are also known as equiangular frames [28, 34–36].

Definition 2.2 A family of vectors $F = \{f_j\}_{j=1}^N$ is said to form a 2-*uniform 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 $|\langle f_j, f_k \rangle| = c$.

Equating

$$d = \sum_{k,l=1}^d |\langle e_k, e_l \rangle|^2 = \frac{1}{A^2} \sum_{j,j'=1}^N \sum_{k,l=1}^d \langle e_k, f_j \rangle \langle f_j, e_l \rangle \langle e_l, f_{j'} \rangle \langle f_{j'}, e_k \rangle$$

$$= \frac{1}{A^2} \sum_{j,j'=1}^N |\langle f_j, f_{j'} \rangle|^2$$

and using the explicit value for the square-norms $\|f_j\|^2 = \frac{Ad}{N}$, $j \in \{1, 2, \ldots, N\}$, shows that the constant c in Definition 2.2 is given by

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

The following proposition bounds the number of vectors in a tight 2-uniform frame. The real case appears in a work by Lemmens and Seidel [28, Theorem 3.5] who attribute the result to Gerzon. The proof generalizes painlessly to complex Hilbert spaces.

Proposition 2.3 (Gerzon) *The possible number of vectors in a tight 2-uniform frame on a d-dimensional Hilbert space $\mathcal{H}$ is bounded. In the case of a real $\mathcal{H}$, $N \leq d(d + 1)/2$, in the complex case, $N \leq d^2$.*

Proof The proof presented here is a variation of an argument used by [4] to show an analogous bound for mutually unbiased bases.

Given a two-uniform N/d-tight frame $\{f_1, f_2, \ldots, f_N\}$ for a complex $\mathcal{H}$, then there exists a Hilbert-Schmidt orthogonal system of frame modulations $\{M_j\}_{j=1}^N$ defined by

$$M_k = \sum_{j=1}^{N} \omega^{kj} P_j,$$

with ω a primitive N-th root of unity and P_j the orthogonal projection onto the line spanned by the vector f_j. If $\mathcal{H}$ is real, then one takes the real and imaginary parts of M_k to define real frame modulations. Since the frame modulations are orthogonal, linear combinations of rank-one projections, their span has dimension N and is contained in the span of *all* rank-one projections. The vector space obtained from all rank-one projections is the space of Hermitian operators in the real case and the space of all operators in the complex case (because any operator is the sum of a Hermitian and an anti-Hermitian). The space of Hermitian operators on a real Hilbert space has dimension $d(d + 1)/2$ and the space of all operators on a complex Hilbert space has dimension d^2. We conclude that the dimension of the span of the operators $\{P_j\}_{j=1}^N$ can be at most $d(d + 1)/2$ or d^2 in the real or complex case, respectively. □

It is a deep open problem in frame theory to show that the upper bound stated in Proposition 2.3 is attained for any finite-dimensional complex Hilbert space. For examples of such frames, see [1, 6, 19, 24, 37]. We cite a minimal example for a two-dimensional real or complex Hilbert space.

Example 2.4 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 $f_3 = R^2e_1$. 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 also informally 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 a 2-uniform 2-tight frame with $|\langle f_i, f_j \rangle| = \frac{1}{\sqrt{3}}$ for all $i \neq j$.

Another type of frame we will use 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.

Definition 2.5 Let $\mathcal{H}$ be a real or complex Hilbert space. 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 2.6 (Delsarte, Goethals and Seidel [16, 37]) *There are at most $m = d + 1$ mutually unbiased bases $\{e_k^{(j)} : 1 \le j \le m, 1 \le k \le d\}$ in a d-dimensional complex Hilbert space $\mathcal{H}$.*

Proof This can be seen by considering that the Hilbert space of operators on $\mathcal{H}$ equipped with the Hilbert-Schmidt inner product has dimension d^2. So the dimension of the span of the operators $\{E_k^{(j)}\}$, each $E_k^{(j)}$ being the self-adjoint rank-one projection onto the span of $e_k^{(j)}$, can be at most d^2. Now we consider the Gram matrix $H_{j,k;\,j',k'} = \mathrm{tr}[E_k^{(j)} E_{k'}^{(j')}]$, which is of the form $H = I_m \otimes I_d + (J_m \otimes J_d - I_m \otimes J_d)/d$, where I_m and I_d are the $m \times m$ and $d \times d$ identity matrix, 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 Gram matrix is identified as 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 $\{E_k^{(j)}\}$ is $md - m + 1 \le d^2$, which implies $m \le d + 1$. $\qquad\square$

Example 2.7 Let d be a prime number, ω a primitive d-th root of unity, and denote the canonical basis of $\mathbb{C}^d$ by $\{e_k\}_{k=1}^d$. Then we identify $e_k^{(1)} \equiv e_k$ and for $j \in \{2, 3, \ldots, d + 1\}$ let

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

This defines a family of $d + 1$ mutually unbiased bases that has been called the *discrete chirps* [11, 23]. To verify that these bases are mutually unbiased, one simply computes the square-modulus of inner products [15].

Remark 2.8 A similar construction applies when d is a power of a prime [37]. If d is not prime, then the maximal number of mutually unbiased bases is generally unknown [19]. In the real case, even in the case of prime dimensions, the construction of maximal sets of mutually unbiased bases is even more difficult [7], but at least for d a power of 4 this is possible [8, 14].

3 Reconstruction of a Vector from Absolute Values of its Frame Coefficients

The 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 the construction of the self-adjoint rank-one operator Q_x, given by $Q_x y = (y, x)x$, $y \in \mathcal{H}$ from the magnitudes of the frame coefficients. For this reason, our computations are mostly formulated in terms of the projective space of $\mathcal{H}$.

Definition 3.1 Let $\mathcal{H}$ be a finite-dimensional real or complex Hilbert space and denote by $P\mathcal{H}$ the *projective space* of $\mathcal{H}$ formed by all orthogonal rank-one projections $\{P : P = P^*P\}$ on $\mathcal{H}$. Equivalently, we can identify each projection by its range in $\mathcal{H}$ and think of this projective space as the set of all one-dimensional subspaces of $\mathcal{H}$.

The projective space $P\mathcal{H}$ is naturally embedded in the space $\mathcal{X}$ containing all self-adjoint rank-one operators. We define the space of *homogeneous kth degree polynomials* $\mathrm{Hom}(k)$ to consist of functions on $\mathcal{X}$ that can be expressed in the form

$$h : X \mapsto \mathrm{tr}[X^{\otimes k} H],$$

with H an operator on $\mathcal{H}^{\otimes k}$.

We denote by μ the probability measure on $P\mathcal{H}$ which is invariant under the conjugation of the projections with orthogonal matrices or unitaries in the real or complex case, respectively.

A finite set $\mathbb{X}$ in $P\mathcal{H}$ is called a *projective t-design* [26], $t \in \{1, 2, \ldots\}$, if for every homogeneous polynomial $h \in \mathrm{Hom}(k)$ of degree $0 \leq k \leq t$, we have

$$\int_{P\mathcal{H}} h\, d\mu = \frac{1}{|\mathbb{X}|} \sum_{P \in \mathbb{X}} h(P),$$

where $|\mathbb{X}|$ denotes the size of the set $\mathbb{X}$.

When restricted to $P\mathcal{H}$, some homogeneous polynomials of different degree may coincide. For our purposes, however, it is important that each harmonic polynomial $h \in \mathrm{Hom}(1)$, which can be expressed with a traceless H, is orthogonal to the space of constants, $\mathrm{Hom}(0)$. Therefore, such harmonic polynomials in $\mathrm{Hom}(1)$ are uniquely determined by their restriction to $P\mathcal{H}$. The following proposition demonstrates this fact.

Proposition 3.2 *Given a real or complex Hilbert space $\mathcal{H}$, a 2-design $\mathbb{X}$ in $P\mathcal{H}$, and a traceless, self-adjoint operator H on $\mathcal{H}$, then*

$$H = \frac{\lambda}{|\mathbb{X}|} \sum_{P \in \mathbb{X}} \mathrm{tr}[HP]P,$$

where $\lambda = d(d/2 + 1)$ in the real case and $\lambda = d(d + 1)$ in the complex case.

Proof This identity is equivalent to a set of identities obtained by taking the Hilbert-Schmidt inner product of both sides with all traceless operators. By the polarization identity, we then only need to prove that

$$\frac{1}{\lambda}\text{tr}[H^2] = \frac{1}{|\mathbb{X}|}\sum_{P\in\mathbb{X}}|\text{tr}[HP]|^2$$

holds for every traceless H. We observe that $P \mapsto |\text{tr}[HP]|^2 = \text{tr}[H\otimes HP\otimes P]$ is in Hom(2) and that for a projective 2-design $\mathbb{X}$,

$$\frac{1}{|\mathbb{X}|}\sum_{P\in\mathbb{X}}\text{tr}[H\otimes HP\otimes P] = \int_{P\mathcal{H}}\text{tr}[H\otimes HP\otimes P]d\mu(P).$$

The result is quadratic in H and invariant under conjugation of H with an orthogonal or unitary matrix in the real or complex case, and therefore it has to be of the form $\alpha\text{tr}[H\otimes H] + \beta\text{tr}[H^2]$. Since H is traceless, α is irrelevant. In order to verify that $\beta = \lambda$, we choose $H = Q_x - I/d$ with a normalized vector $x \in \mathcal{H}$.

Then we conclude $\text{tr}[H^2] = (1 - \frac{1}{d})^2 + (d-1)\frac{1}{d^2} = 1 - \frac{1}{d}$ and

$$|\text{tr}[HP]|^2 = |\text{tr}[Q_xP]|^2 - \frac{2}{d}\text{tr}[Q_xP] + \frac{1}{d^2}$$

$$= |\langle Px, x\rangle|^2 - \frac{2}{d}\langle Px, x\rangle + \frac{1}{d^2},$$

which integrates to

$$\int_{P\mathcal{H}}|\text{tr}[HP]|^2d\mu(P) = \frac{d-1}{d^2(\tilde{d}+1)},$$

where $\tilde{d} = d/2$ in the real case and $\tilde{d} = d$ in the complex case. This computation uses Hoggar's result [22, Theorem 2.11], which states that the measure μ on the projective space induces under the map $\Phi : P \mapsto \langle Px, x\rangle$ the image measure m with $dm(z) = A(1-z)^{\tilde{d}-1-\tilde{d}/d}z^{\tilde{d}/d-1}dz$ on $[0, 1]$, where A is chosen to normalize the measure. Now we confirm that the result of the integration equals $\text{tr}[H^2]/\lambda = (1 - \frac{1}{d})/\lambda$.   □

Two known types of examples for projective 2-designs are a maximal equiangular set of lines generated by 2-uniform tight frames and the set of lines generated by a maximal set of mutually unbiased bases in $\mathcal{H}$.

Example 3.3 Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space with a frame $F = \{f_j\}_{j=1}^N$. For each frame vector f_j, let P_j denote the orthogonal projection onto the one-dimensional subspace containing f_j. If the frame F is N/d-tight and 2-uniform, and contains the maximal number of vectors, $N = d(d+1)/2$ in the case of a real Hilbert space $\mathcal{H}$ or $N = d^2$ in the complex case, then the projections $\{P_j\}_{j=1}^N$ form a projective 2-design [26].

If the frame F for a complex Hilbert space $\mathcal{H}$ is obtained from the union of $d+1$ mutually unbiased bases, then it is a complex projective 2-design [26].

With each $x \in \mathcal{H}$, we associate the quadratic form q_x on $\mathcal{H}$, given by $q_x(y) = |\langle x, y \rangle|^2$, and the operator Q_x corresponding to it, $q_x(y) = \langle Q_x y, y \rangle$ for all $y \in \mathcal{H}$. The following theorem gives a reconstruction formula for Q_x that only depends on the magnitudes of the frame coefficients when the frame F is associated with a projective 2-design. In the complex case, the reconstruction formula can be deduced from a derivation by Scott [33, (10)], who examines the general case of complex weighted 2-designs, and attributes these results to Levenshtein. Here, we consider only uniformly weighted 2-designs, but include real and complex Hilbert spaces.

Theorem 3.4 (Levenshtein [27]) *Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space and $F = \{f_1, f_2, \ldots, f_N\}$ a uniform N/d-tight frame such that the orthogonal projections onto the one-dimensional subspaces containing the frame vectors form a projective 2-design in $P\mathcal{H}$. Given a vector $x \in \mathcal{H}$ with associated self-adjoint rank-one operator Q_x, then*

$$Q_x = \frac{\lambda}{N} \sum_{j=1}^{N} |\langle x, f_j \rangle|^2 Q_{f_j} - \nu \|x\|^2 I,$$

where $\lambda = d(d/2 + 1)$, $\nu = 1/2$ in the real case and $\lambda = d(d + 1)$, $\nu = 1$ in the complex case.

Proof By definition, the vectors $\{f_j\}_{j=1}^{N}$ all have unit norm, and each Q_{f_j} is an orthogonal projection contained in $P\mathcal{H}$. Since the frame gives rise to a projective 2-design, the preceding proposition applies and we have

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

Replacing the sum over the 2-design by an integral over $P\mathcal{H}$, and using Hoggar's result [22, Theorem 2.11] again, $\frac{1}{N} \sum_j Q_{f_j} = \int_{P\mathcal{H}} P d\mu(P) = I/d$ simplifies this to the claimed identity. □

Remark 3.5 With the help of the integral formula in the proof, we could re-state the reconstruction identity as

$$Q_x = \frac{\lambda}{N} \sum_{j=1}^{N} \mathrm{tr}[Q_x Q_{f_j}] \left(Q_{f_j} - \frac{\nu d}{\lambda} I \right).$$

By linearity, this holds also if Q_x is replaced by a general operator on $\mathcal{H}$ if it is a complex Hilbert space and by any self-adjoint operator if $\mathcal{H}$ is real. Since $\mathrm{tr}[Q_x Q_{f_j}]$ is a Hilbert-Schmidt inner product, this reconstruction identity can be interpreted as the statement that the operators $\{Q_{f_j}\}_{j=1}^{N}$ form a frame for the (sub)space in $B(\mathcal{H})$ spanned by rank-one projections and the set of operators $\{\frac{\lambda}{N}(Q_{f_j} - \nu d I/\lambda)\}_{j=1}^{N}$ is a dual frame.

From a practical point of view, the above theorem gives an algorithm that allows us to reconstruct x, up to an overall unimodular constant, by considering one non-vanishing column of the matrix Q_x. Thus, the computation requires only $O(Nd)$ operations. For the examples of maximal 2-uniform frames and mutually unbiased bases that yield projective 2-designs, N is of order d^2. This results in $O(d^3)$ operations required for reconstruction.

4 The Reconstruction Formula for Mutually Unbiased Bases

For the maximal family of mutually unbiased bases given by discrete chirps in a complex Hilbert space of prime dimension, the reconstruction formula is especially simple. We could immediately deduce the form from the fact that maximal families of mutually unbiased bases are projective two-designs [26]. However, to keep our exposition self-contained, we derive this special case of Theorem 3.4 with the help of frame modulations.

Definition 4.1 Let $\mathcal{H}$ be a complex Hilbert space of dimension d. Let $\mathbb{J} = \{1, 2, \ldots, d+1\}$ and $\mathbb{K} = \{1, 2, \ldots, d\}$. If the family of vectors $\{e_k^{(j)} : j \in \mathbb{J}, k \in \mathbb{K}\}$ forms $d+1$ mutually unbiased bases in $\mathcal{H}$ and ω is a primitive d-th root of unity, then we denote

$$B_k^{(j)} = \frac{1}{\sqrt{d}} \sum_{l=1}^{d} \omega^{kl} P_l^{(j)},$$

where for each $k \in \mathbb{K}$, $j \in \mathbb{J}$, $P_k^{(j)}$ is the rank-one orthogonal projection onto the span of $e_k^{(j)}$.

Before we derive our algorithm for reconstruction using mutually unbiased bases, we need to show that this class naturally defines an orthonormal basis for $B(\mathcal{H})$.

Lemma 4.2 *Let $\{e_k^{(j)} : j \in \mathbb{J}, k \in \mathbb{K}\}$ form $d+1$ mutually unbiased bases in a d-dimensional complex Hilbert space $\mathcal{H}$, and let ω be a primitive d-th root of unity. Then the operators $\{B_k^{(j)} : j \in \mathbb{J}, k \in \mathbb{K} \setminus \{d\}\} \cup \{\frac{1}{\sqrt{d}} I\}$ form an orthonormal basis in $B(\mathcal{H})$ with respect to the Hilbert-Schmidt inner product.*

Proof First we note that all these operators are normalized with respect to the Hilbert-Schmidt norm and that the trace of all $B_k^{(j)}$, $k \in \{1, 2, \ldots, d-1\}$ is zero. So the operators $\{B_k^{(j)}\}$ are Hilbert-Schmidt orthogonal to the identity. Now consider

$$A_{k,k'}^{(j,j')} = \mathrm{tr}[B_k^{(j)}(B_{k'}^{(j')})^*] = \frac{1}{d} \sum_{l=1}^{d} \sum_{l'=1}^{d} \omega^{kl} \omega^{-k'l'} \mathrm{tr}[P_l^{(j)} P_{l'}^{(j')}].$$

If $j \neq j'$, then

$$A^{(j,j')}_{k,k'} = \frac{1}{d^2} \sum_{l,l'=1}^{d} \omega^{kl-k'l'} = 0$$

and if $j = j'$, then

$$A^{(j,j)}_{k,k'} = \frac{1}{d} \sum_{l,l'=1}^{d} \omega^{kl-k'l'} \delta_{l,l'} = \frac{1}{d} \sum_{l=1}^{d} \omega^{l(k-k')}$$

which either adds to zero if $k \neq k'$ or else to one. Now we have an orthonormal system of $(d+1)(d-1) + 1 = d^2$ operators, and since $\dim(B(\mathcal{H})) = d^2$, this is a basis. $\quad\square$

Now we are ready to present a fast reconstruction algorithm for mutually unbiased bases.

Theorem 4.3 *Given a family of vectors $\{e_k^{(j)}, j \in \mathbb{J}, k \in \mathbb{K}\}$ that form $d+1$ mutually unbiased bases in $\mathbb{C}^d$, a primitive d-th root of unity ω and the associated operators $\{B_k^{(j)}\}$, then for all $x \in \mathbb{C}^d$,*

$$Q_x = \frac{\|x\|^2}{d} I + \frac{1}{\sqrt{d}} \sum_{j=1}^{d+1} \sum_{k=1}^{d-1} \sum_{l=1}^{d} \omega^{-kl} |\langle x, e_l^{(j)}\rangle|^2 B_k^{(j)}.$$

Proof Since $\{\frac{1}{\sqrt{d}}I\} \cup \{B_k^{(j)}\}$ forms an orthonormal basis in $B(\mathbb{C}^d)$, we have

$$Q_x = \frac{1}{d}\mathrm{tr}Q_x + \sum_{j=1}^{d+1} \sum_{k=1}^{d-1} \mathrm{tr}[Q_x (B_k^{(j)})^*] B_k^{(j)}$$

and the claimed identity follows from the definition of $B_k^{(j)}$. $\quad\square$

Corollary 4.4 *Assume without loss of generality that the first set of basis vectors $\{e_k^{(1)}\}_{k=1}^{d}$ is the canonical orthonormal basis of $\mathbb{C}^d$, and denote the coefficients of the vector x in this basis by $\{x_k\}_{k=1}^{d}$. If not all coefficients are zero, say $x_1 \neq 0$, then for $i \in \{1, 2, \ldots, d\}$,*

$$x_i \overline{x_1} = \sum_{j=1}^{d+1} \sum_{l=1}^{d} |\langle x, e_l^{(j)}\rangle|^2 \langle e_1^{(1)}, e_l^{(j)}\rangle \langle e_l^{(j)}, e_i^{(1)}\rangle - \|x\|^2 \delta_{i,1}.$$

Proof Inserting the definition of $B_k^{(j)}$, we have

$$x_i \overline{x_1} = \frac{1}{d}\|x\|^2 \delta_{i,1} + \frac{1}{\sqrt{d}} \sum_{j=1}^{d+1} \sum_{k=1}^{d-1} \sum_{l=1}^{d} \omega^{-kl} |\langle x, e_l^{(j)}\rangle|^2 \mathrm{tr}[B_k^{(j)} E_{i,1}^*]$$

where $E_{i,1}$ is the usual matrix unit. We then compute

$$x_i \overline{x_1} = \frac{1}{d} \|x\|^2 \delta_{i,1} + \frac{1}{d} \sum_{j=1}^{d+1} \sum_{k=1}^{d-1} \sum_{l,l'=1}^{d} \omega^{kl'-kl} |\langle x, e_l^{(j)} \rangle|^2 \langle e_1^{(1)}, e_{l'}^{(j)} \rangle \langle e_{l'}^{(j)}, e_i^{(1)} \rangle.$$

Adding and subtracting the term corresponding to $k = d$,

$$\frac{1}{d} \sum_{j=1}^{d+1} \sum_{l,l'=1}^{d} |\langle x, e_l^{(j)} \rangle|^2 \langle e_1^{(1)}, e_{l'}^{(j)} \rangle \langle e_{l'}^{(j)}, e_i^{(1)} \rangle = \frac{d+1}{d} \|x\|^2 \delta_{i,1}$$

gives

$$x_i \overline{x_1} = \sum_{j=1}^{d+1} \sum_{l=1}^{d} |\langle x, e_l^{(j)} \rangle|^2 \langle e_1^{(1)}, e_l^{(j)} \rangle \langle e_l^{(j)}, e_i^{(1)} \rangle - \|x\|^2 \delta_{i,1}. \qquad \square$$

Using this algorithm for prime-number dimensions and discrete chirps, we get a simple closed form for the reconstruction.

Corollary 4.5 *If d is prime and we use the discrete chirps in Example 2.7 as a maximal set of mutually unbiased bases, then the reconstruction formula becomes*

$$x_n \overline{x_1} = \frac{1}{d} \sum_{j=1}^{d+1} \sum_{l=1}^{d} \omega^{-(j-1)(n^2-1)+l(n-1)} |\langle x, e_l^{(j)} \rangle|^2 - \|x\|^2 \delta_{n,1}.$$

5 Frames for Fast Reconstruction

Although the use of 2-designs allows a reconstruction algorithm with $O(d^3)$ operations, and the efficient numerical implementation of the discrete Fourier transform offers another possibility for an improvement for the special case of chirps, the algorithm still does not scale in the best possible way with the dimension of $\mathcal{H}$. The ideal case is to have reconstruction on the order of d steps for a d-dimensional Hilbert space.

We will now construct uniform tight frames for which there is a fast reconstruction algorithm requiring on the order of d operations.

The construction of the frame we use combines the preceding material with the idea of fusion frames [10, 12, 13], see also [5].

Example 5.1 (Covering with minimal 2-uniform frames) We pick a basis $\{e_i\}_{i=1}^{d}$ in $\mathcal{H}$ and identify the basis vectors with vertices in a complete graph. With each edge $\{i, k\} \subset \{1, 2, \ldots, d\}$, $1 \le i < k \le d$, we associate the subspace $\mathcal{H}_{i,k}$ spanned by the pair $\{e_i, e_k\}$.

Then it is straightforward to check that the orthogonal projections $\{P_{i,k} : \mathrm{ran}(P_{i,k}) = \mathcal{H}_{i,k}, 1 \le i < k \le d\}$ resolve the identity on $\mathcal{H}$,

$$\frac{1}{d-1} \sum_{1 \le i < k \le d} P_{i,k} = I.$$

Consider a 2-uniform $N/2$-tight frame $\{f_j^{(i,k)}\}_{j=1}^N$ as in Example 2.4 for each $\mathcal{H}_{i,k}$. If $\mathcal{H}$ is a real Hilbert space, then $N = 3$; if it is complex, then $N = 4$.

Denote the rank-one orthogonal projection with range containing $f_j^{(i,k)}$ by $Q_j^{(i,k)}$. Since each projection $P_{i,k}$ can be written as the sum $P_{i,k} = \frac{2}{N} \sum_{j=1}^N Q_j^{(i,k)}$, the set $\{f_j^{(i,k)} : 1 \le i < k \le d, 1 \le j \le N\}$ is a $(d-1)N/2$-tight uniform frame for $\mathcal{H}$.

It seems that the number of frame coefficients needed for reconstruction is still quadratic in d. However, we can modify the algorithm in such a way that only a portion of them is used and significantly reduce the number of needed frame coefficients.

Theorem 5.2 *Let $\mathcal{H}$ be a d-dimensional real or complex Hilbert space. Let $\{e_1, e_2, \ldots, e_d\}$ be an orthonormal basis for $\mathcal{H}$. Let $F = \{f_j^{(i,k)} : 1 \le i < k \le d, 1 \le j \le N\}$ be the $(d-1)N/2$-tight frame for $\mathcal{H}$ constructed in the preceding example, with $N = 3$ if the Hilbert space is real and $N = 4$ if it is complex. Given a non-zero vector $x \in \mathcal{H}$ and a spanning tree T for the complete graph on d vertices such that the set $L \subset \{1, 2, \ldots, d\}$ of the leaves of the graph contains each vertex i for which $\langle x, e_i \rangle = 0$. Then Q_x can be reconstructed from the magnitudes of the frame coefficients of the subset $G = \{f_j^{(i,k)} : \{i, k\} \in T, 1 \le j \le N\}$.*

Proof To simplify notation, we abbreviate $v_i = \langle v, e_i \rangle$ for any $v \in \mathcal{H}$ and $i \in \{1, 2, \ldots, d\}$. As before, we denote the orthogonal projection onto the span of $\{e_i, e_k\}$ by $P_{i,k}$. Given the spanning tree T, we reconstruct $Q_{P_{i,k}x}$ with the two-uniform $N/2$-tight frame of $\mathcal{H}_{i,k}$ for each edge $\{i, k\} \in T$. This means, we have $y^{(i,k)} = u_{i,k} P_{i,k} x$ with an unknown unimodular constant $u_{i,k}$ for each edge. In order to determine x up to a unimodular constant u, we have to eliminate $d - 1$ of these unknowns. To this end, we proceed in an iterative manner. Starting with the root of the tree, we pick an edge, say $\{1, 2\}$ and choose an arbitrary unimodular $u_{1,2}$. This fixes $y_1 = u_{1,2} x_1$. Now we proceed along the edges of the spanning tree. At each step, we compute a new coefficient y_i from an adjacent pair of edges $\{i, k\}$ and $\{i, l\}$. This is accomplished by comparing the two reconstructed vectors $y^{(i,k)}$ and $y^{(i,l)}$, where the phase of $y^{(i,k)}$ has already been fixed. We note that $y_i^{(i,k)} \ne 0$ because it is not a leaf. Since we require $y_i = y_i^{(i,k)}$ and $y_i = y_i^{(i,l)}$, this determines $y^{(i,l)}$ and thus $y_l = y_l^{(i,l)}$. According to this procedure, all $y_i, i \in \{1, 2, \ldots, d\}$ are determined. $\qquad \square$

Remark 5.3 The above algorithm needs only the magnitudes of $(d-1)N$ frame coefficients. Since the reconstruction for each 2-dimensional subspace uses a constant number of operations, and there are $d - 1$ edges in a spanning tree, it requires of the order of d operations.

The spanning tree can be constructed iteratively in the course of reconstruction. At each step, we test whether a given pair $\{i, k\}$ leads to coefficients y_i or y_k that are zero. Each vanishing coefficient is declared a leaf in the spanning tree. If we have initially chosen an edge with two zero coefficients we declare the two vertices it contains leaves and start anew with a non-adjacent edge. Since the vector x was by assumption non-zero, there is at least one edge which is associated with a non-zero coefficient. Beginning with this edge, we proceed inductively by picking the next edge such that it is incident with the vertex with a non-vanishing coefficient in the preceding edge. It is straightforward to verify that this construction exhausts all vertices and that the set of leaves contains all vertices associated with vanishing coefficients.

6 Conclusion and Outlook

We have seen that for certain tight frames, there are remarkably simple reconstruction algorithms that only use the magnitudes of the frame coefficients. The main tool giving such simple reconstruction formulas is the use of projective 2-designs. Since examples for such designs have a small set of possible magnitudes for inner products between frame vectors, the general reconstruction formula can be simplified even further.

Furthermore, we have demonstrated that there are frames for which the number of operations required for reconstruction only grows linearly with the dimension of the Hilbert space.

One may consider the task of reconstruction without phase also when coefficients are lost, e.g. in the course of a data transmission [6, 9, 20, 25]. Since 2-uniform tight frames are in certain situations optimal for a small number of lost coefficients, [6], one can expect that reconstruction without phase will perform well even in the presence of lost coefficients. This topic will be pursued in another work.

References

1. Appleby, D.M.: Symmetric informationally complete-positive operator valued measures and the extended Clifford group. J. Math. Phys. **46**(5), 052107 (2005)
2. Balan, R., Casazza, P., Edidin, D.: On signal reconstruction without phase. Appl. Comput. Harmon. Anal. **20**, 345–356 (2006)
3. Balan, R., Casazza, P., Edidin, D.: Equivalence of reconstruction from the absolute value of the frame coefficients to a sparse representation problem. IEEE Signal Process. Lett. **14**, 341–343 (2007)
4. Bandyopadhyay, S., Boykin, P.O., Roychowdhury, V., Vatan, F.: A new proof for the existence of mutually unbiased bases. Algorithmica **34**(4), 512–528 (2002). Quantum computation and quantum cryptography
5. Bodmann, B.G.: Optimal linear transmission by loss-insensitive packet encoding. Appl. Comput. Harmon. Anal. **22**, 274–285 (2007)
6. Bodmann, B.G., Paulsen, V.I.: Frames, graphs and erasures. Linear Algebra Appl. **404**, 118–146 (2005)
7. Boykin, P.O., Sitharam, M., Tiep, P.H., Wocjan, P.: Mutually unbiased bases and orthogonal decompositions of Lie algebras. Quantum Inf. Comput. **7**, 371–382 (2007)
8. Calderbank, A.R., Cameron, P.J., Kantor, W.M., Seidel, J.J.: Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. Lond. Math. Soc. (3) **75**(2), 436–480 (1997)

9. Casazza, P., Kovačević, J.: Equal-norm tight frames with erasures. Adv. Comput. Math. **18**, 387–430 (2003)

10. Casazza, P.G., Kutyniok, G.: Frames of subspaces. In: Wavelets, Frames and Operator Theory. Contemp. Math., vol. 345, pp. 87–113. Am. Math. Soc., Providence (2004)

11. Casazza, P.G., Fickus, M.: Fourier transforms of finite chirps. EURASIP J. Appl. Signal Process. **2006**, 1–7 (2006). Frames and overcomplete representations in signal processing, communications, and information theory

12. Casazza, P.G., Kutyniok, G.: Robustness of fusion frames under erasures of subspaces and of local frame vectors. In: Grinberg, E.L., Larson, D., Jorgensen, P.E.T., et al.(eds.) Radon Transforms, Geometry, and Wavelets, New Orleans, LA, 2006. Contemp. Math., vol. 464, pp. 149–160. Am. Math. Soc., Providence (2008)

13. Casazza, P.G., Kutyniok, G., Li, S.: Fusion frames and distributed processing. Appl. Comput. Harmon. Anal. **25**, 114–132 (2008)

14. Cameron, P.J., Seidel, J.J.: Quadratic forms over $GF(2)$. Indag. Math. **35**, 1–8 (1973)

15. Chaturvedi, S.: Aspects of mutually unbiased bases in odd-prime-power dimension. Phys. Rev. A **65**, 0044301 (2002)

16. Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geom. Dedic. **6**(3), 363–388 (1977)

17. Finkelstein, J.: Pure-state informationally complete and "really" complete measurements. Phys. Rev. A **70**, 052107 (2004)

18. Flammia, S.T., Silberfarb, A., Caves, C.M.: Minimal informationally complete measurements for pure states. Found. Phys. **35**(12), 1985–2006 (2005)

19. Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases and spin models. Eur. J. Comb. **30**, 246–262 (2009)

20. Goyal, V.K., Kovačević, J., Kelner, J.A.: Quantized frame expansions with erasures. Appl. Comput. Harmon. Anal. **10**, 203–233 (2001)

21. Hayes, M.H., Lim, J.S., Oppenheim, A.V.: Signal reconstruction from phase and magnitude. IEEE Trans. Acoust. Speech Signal Process. **28**(6), 672–680 (1980)

22. Hoggar, S.G.: t-designs in projective spaces. Eur. J. Comb. **3**, 233–254 (1982)

23. Howard, S.D., Calderbank, A.R., Moran, W.: The finite Heisenberg-Weyl groups in radar and communications. EURASIP J. Appl. Signal Process. **2006**, 1–12 (2006). Special issue on "Frames and overcomplete representations in signal processing, communications, and information theory"

24. Holmes, R., Paulsen, V.I.: Optimal frames for erasures. Linear Algebra Appl. **377**, 31–51 (2004)

25. Kovačević, J., Dragotti, P.L., Goyal, V.K.: Filter bank frame expansions with erasures. IEEE Trans. Inf. Theory **48**, 1439–1450 (2002)

26. Klappenecker, A., Rötteler, M.: Mutually unbiased bases are complex projective 2-designs. In: Proc. Int. Symp. on Inf. Theory, pp. 1740–1744. IEEE Press, New York (2005)

27. Levenshtein, V.I.: On designs in compact metric spaces and a universal bound on their size. Discrete Math. **192**, 251–271 (1998)

28. Lemmens, P.W.H., Seidel, J.J.: Equiangular lines. J. Algebra **24**, 494–512 (1973)

29. Lyubich, Yu.I.: On tight projective designs. E-print: math/0703526 (2007)

30. Nawab, H., Quatieri, T.F., Lim, J.S.: Signal reconstruction from the short-time Fourier transform magnitude. In: Proceedings of ICASSP'82, vol. 7, pp. 1046–1048 (1982)

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

32. Renes, J.M., Blume-Kohout, R., Scott, A.J., Caves, C.M.: Symmetric informationally complete quantum measurements. J. Math. Phys. **45**(6), 2171–2180 (2004)

33. Scott, A.J.: Tight informationally complete quantum measurements. J. Phys. A Math. Gen. **39**(43), 13507–13530 (2006)

34. Strohmer, T., Heath, R.: Grassmannian frames with applications to coding and communications. Appl. Comput. Harmon. Anal. **14**, 257–275 (2003)

35. van Lint, J.H., Seidel, J.J.: Equilateral point sets in elliptic geometry. Indag. Math. **28**, 335–348 (1966)

36. Vale, R., Waldron, S.: Tight frames and their symmetries. Constr. Approx. **21**(1), 83–112 (2005)

37. Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**(2), 363–381 (1989)