HAL
open science

Signal reconstruction from the magnitude of subspace components

Christine Bachoc, Martin Ehler

To cite this version:

Christine Bachoc, Martin Ehler. Signal reconstruction from the magnitude of subspace components. 2013. hal-00880340

HAL Id: hal-00880340

https://hal.science/hal-00880340v1

Preprint submitted on 5 Nov 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SIGNAL RECONSTRUCTION FROM THE MAGNITUDE OF SUBSPACE COMPONENTS

CHRISTINE BACHOC AND MARTIN EHLER

Abstract. We consider signal reconstruction from the norms of subspace components generalizing standard phase retrieval problems. In the deterministic setting, a closed reconstruction formula is derived when the subspaces satisfy certain cubature conditions, that require at least a quadratic number of subspaces. Moreover, we address reconstruction under the erasure of a subset of the norms; using the concepts of p-fusion frames and list decoding, we propose an algorithm that outputs a finite list of candidate signals, one of which is the correct one. In the random setting, we show that a set of subspaces chosen at random and of cardinality scaling linearly in the ambient dimension allows for exact reconstruction with high probability by solving the feasibility problem of a semidefinite program.

1. Introduction

Frames have become a powerful tool in signal processing that can offer more flexibility than orthogonal bases, cf. [35]. Many signal processing problems in engineering such as X-ray crystallography and diffraction imaging require signal reconstruction from the magnitude of its frame coefficients, cf. [7, 12] and references therein. Classical reconstruction algorithms are based on iterated projection schemes [30, 32], see also [8]. By making additional assumptions on the underlying frame, exact solutions are presented in [6, 7], see [38, 40] for relations to quantum measurements. Lower bounds on the number of required measurements are discussed in [7]. Recently, reconstruction from frame coefficients without phase has been numerically addressed via semidefinite programming, see [12, 14] and [16, 43]. For phase retrieval in the continuous setting, see, for instance, [37], but, here, we focus on the discrete finite dimensional setting.

Frame coefficients can be thought of as projections onto 1-dimensional subspaces. In image reconstruction from averaged diffraction patterns by means of incoherent addition of k wavefields [29], the original signal must be recovered from the norms of its k-dimensional subspace components. Notably, the latter is a common problem in crystal twinning [25].

Here, we pose the following questions: Can we reconstruct the original signal from the norms of its k-dimensional subspace components by means of a closed formula? Also, can we develop strategies to reduce the number of required subspace components? We shall provide affirmative answers for a deterministic choice and a random choice of subspaces.

Deterministic setting: Given k-dimensional linear subspaces $\{V_j\}_{j=1}^n$ in $\mathbb{R}^d$, we aim to reconstruct the signal $x \in \mathbb{R}^d$ from $\{\|P_{V_j}(x)\|\}_{j=1}^n$, where P_{V_j} denotes the orthogonal projector onto V_j. If there are positive weights $\{\omega_j\}_{j=1}^n$ such that

$\{(V_j, \omega_j)\}_{j=1}^n$ yields a cubature of strength 4, then we shall obtain a closed reconstruction formula for xx^* enabling us to extract $\pm x$. Thus, we extend the 1-dimensional results in [6] to k-dimensional projections. Note that the authors in [6] require cubatures for the projective space whose weights are $\omega_j = 1/n$, i.e., so-called projective designs. In practice, however, the choice of subspaces may underlie restrictions that prevent them from being a design. Therefore, our results are a significant improvement for 1-dimensional projections already.

To address subspace erasures, we suppose that we are only given the values of $n - p$ norms and we need to reconstruct the missing p norms. Notice that our input are not the subspace components but their norms, as opposed to signal reconstruction under the erasures discussed in [11, 34, 36]. If there are positive weights $\{\omega_j\}_{j=1}^n$ such that $\{(V_j, \omega_j)\}_{j=1}^n$ forms a tight p-fusion frame as recently introduced in [5], then we are able to reconstruct the erased p norms at least up to permutation. We can then reconstruct $\pm x$ from the entire set of n magnitude subspace components. In other words, we found conditions on subspaces, so that we can compute a finite list of candidate signals, one of which is the correct one. The latter is a form of list decoding as introduced in [28].

The limit of this deterministic approach stands in the required number of subspaces. Indeed, it is known that the cardinality of a cubature formula of strength 4 scales at least quadratically with the ambient dimension d. In the random setting, it will be possible to reduce the number of subspaces to linear size:

Random setting: We shall extend to k-dimensional subspaces the results obtained for $k = 1$ in a recent series of papers [14, 24, 13]. In [14] it was shown that semidefinite programming yields signal recovery with high probability when the 1-dimensional subspaces are chosen at random and that the cardinality of the subspaces can scale linearly in the ambient dimension up to a logarithmic factor. Numerical stability in the presence of noise was also verified. The underlying semidefinite program was shown in [24] to afford (with high probability) a unique feasible solution, and the logarithmic factor was removed in [13].

Our proof for k-dimensional subspaces (see Theorem 5.1) is guided by the approach in [13, 14] but some steps are more involved and require additional tools. For instance, the case $k = 1$ relies on random vectors whose entries are i.i.d. Gaussian modeling the measurements. For $k > 1$, we must deal with measurement matrices having orthogonal rows, so that entries from one row are stochastically dependent on those in any other row. Hence, the extension from $k = 1$ to $k > 1$ is not obvious and requires special care. For instance, our Proposition 5.8 is a novel ingredient reflecting such difficulties.

Moreover, we present numerical experiments indicating that the choice $k > 1$ can lead to better recovery results than $k = 1$.

Although we present our results for real signals and subspaces exclusively, the agenda can also be followed in the complex setting. We shall discuss the required modifications at the end of the present paper.

Outline: In Section 2, we recall fusion frames, state the phase retrieval problem, and introduce tight p-fusion frames and cubature formulas. We present the closed reconstruction formula in Section 3 and our reconstruction algorithm in presence of erasures in Section 4. The random subspace selection is addressed in Section 5. Numerical experiments are presented in Section 6, and we discuss the complex setting in Section 7.

2. Fusion frames, phase retrieval, and cubature formulas

2.1. **Fusion frames and the problem of reconstruction without phase.** Let $\mathcal{G}_{k,d} = \mathcal{G}_{k,d}(\mathbb{R})$ denote the *real Grassmann space*, i.e., the k-dimensional subspaces of $\mathbb{R}^d$. Each $V \in \mathcal{G}_{k,d}$ can be identified with the orthogonal projector onto V, denoted by P_V. Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ and let $\{\omega_j\}_{j=1}^n$ be a collection of positive weights. Then $\{(V_j, \omega_j)\}_{j=1}^n$ is called a *fusion frame* if there are positive constants A and B such that

$$A\|x\|^2 \leq \sum_{j=1}^n \omega_j \|P_{V_j}(x)\|^2 \leq B\|x\|^2, \text{ for all } x \in \mathbb{R}^d, \tag{1}$$

cf. [15]. The condition (1) is equivalent to

$$A \leq \sum_{j=1}^n \omega_j \langle P_x, P_{V_j}\rangle \leq B, \text{ for all } x \in S^{d-1}, \tag{2}$$

where P_x is short for $P_{x\mathbb{R}}$ and $\langle P_x, P_{V_j}\rangle := \operatorname{trace}(P_x P_{V_j})$ is the standard inner product between self-adjoint operators. If $A = B$, then $\{(V_j, \omega_j)\}_{j=1}^n$ is called a *tight fusion frame*, and any signal $x \in S^{d-1}$ can be reconstructed from its subspace components by the simple formula

$$x = \frac{1}{A} \sum_{j=1}^n \omega_j P_{V_j}(x). \tag{3}$$

If, however, instead of $\{P_{V_j}(x)\}_{j=1}^n$ we only observe the norms $\{\|P_{V_j}(x)\|\}_{j=1}^n$ and, worse, we even lose some of these norms, can we still reconstruct x? Clearly, x can be determined up to its sign at best. In the present paper, we find conditions on $\{(V_j, \omega_j)\}_{j=1}^n$ together with a computationally feasible algorithm that enable us to determine $\pm x$.

2.2. **Tight p-fusion frames.** Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ and let $\{\omega_j\}_{j=1}^n$ be a collection of positive weights and p a positive integer. Then $\{(V_j, \omega_j)\}_{j=1}^n$ is called a *p-fusion frame* in [5] if there exist positive constants A_p and B_p such that

$$A_p\|x\|^{2p} \leq \sum_{j=1}^n \omega_j \|P_{V_j}(x)\|^{2p} \leq B_p\|x\|^{2p}, \text{ for all } x \in \mathbb{R}^d, \tag{4}$$

see also [27] for related concepts. If $A_p = B_p$, then $\{(V_j, \omega_j)\}_{j=1}^n$ is called a *tight p-fusion frame*. As with (1) and (2), the condition (4) is equivalent to

$$A_p \leq \sum_{j=1}^n \omega_j \langle P_x, P_{V_j}\rangle^p \leq B_p, \text{ for all } x \in S^{d-1}. \tag{5}$$

If $\{(V_j, \omega_j)\}_{j=1}^n$ is a tight p-fusion frame, then it is also a tight ℓ-fusion frame for all integers $1 \leq \ell \leq p$, and the tight ℓ-fusion frame bounds are

$$A_\ell = \frac{(k/2)_\ell}{(d/2)_\ell} \sum_{j=1}^n \omega_j, \tag{6}$$

where we used $(a)_\ell = a(a+1)\cdots(a+\ell-1)$, cf. [5]. We also refer to [5] for constructions and general existence results.

2.3. **Cubature formulas.** The real orthogonal group $O(\mathbb{R}^d)$ acts transitively on $\mathcal{G}_{k,d}$, and the Haar measure on $O(\mathbb{R}^d)$ induces a probability measure σ_k on $\mathcal{G}_{k,d}$. Let $L^2(\mathcal{G}_{k,d})$ denote the complex valued functions on $\mathcal{G}_{k,d}$, whose squared module is integrable with respect to σ_k. The complex irreducible representations of $O(\mathbb{R}^d)$ are associated to partitions $\mu = (\mu_1, \dots, \mu_d)$, $\mu_1 \geq \dots \geq \mu_d \geq 0$, denoted by V_d^μ, cf. [33]. Let $l(\mu)$ be the number of nonzero entries in μ so that

$$L^2(\mathcal{G}_{k,d}) = \bigoplus_{l(\mu)\leq k} H_{k,d}^{2\mu}, \quad \text{where } H_{k,d}^{2\mu} \simeq V_d^{2\mu}, \tag{7}$$

see [33]. The space of polynomial functions on $\mathcal{G}_{k,d}$ of degree bounded by $2p$ is

$$\mathrm{Pol}_{\leq 2p}(\mathcal{G}_{k,d}) := \bigoplus_{l(\mu)\leq k,\ |\mu|\leq p} H_{k,d}^{2\mu}, \tag{8}$$

and we additionally define the subspace

$$\mathrm{Pol}^1_{\leq 2p}(\mathcal{G}_{k,d}) := \bigoplus_{l(\mu)\leq 1,\ |\mu|\leq p} H_{k,d}^{2\mu}. \tag{9}$$

These spaces are explicitly given by

$$\mathrm{Pol}_{\leq 2p}(\mathcal{G}_{k,d}) = \mathrm{span}\{V \mapsto \langle P_{x_1}, P_V\rangle \cdots \langle P_{x_p}, P_V\rangle : x_1, \dots, x_p \in S^{d-1}\},$$
$$\mathrm{Pol}^1_{\leq 2p}(\mathcal{G}_{k,d}) = \mathrm{span}\{V \mapsto \langle P_x, P_V\rangle^p : x \in S^{d-1}\},$$

cf. [5, Remark 5.4, proof of Theorem 5.3]. Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ and $\{\omega_j\}_{j=1}^n$ be a collection of positive weights normalized such that $\sum_{j=1}^n \omega_j = 1$. Then $\{(V_j, \omega_j)\}_{j=1}^n$ is called a *cubature of strength* $2p$ *for* $\mathcal{G}_{k,d}$ if

$$\int_{\mathcal{G}_{k,d}} f(V) d\sigma_k(V) = \sum_{j=1}^n \omega_j f(V_j) \quad \text{for all } f \in \mathrm{Pol}_{\leq 2p}(\mathcal{G}_{k,d}). \tag{10}$$

Grassmannian designs, i.e., cubatures with constant weights, have been studied in [1, 2, 3, 4]. For existence results on cubatures and the relations between p and n, we refer to [23]. It was verified in [5] that $\{(V_j, \omega_j)\}_{j=1}^n$ is a tight p-fusion frame if and only if

$$\int_{\mathcal{G}_{k,d}} f(V) d\sigma_k(V) = \sum_{j=1}^n \omega_j f(V_j) \quad \text{for all } f \in \mathrm{Pol}^1_{\leq 2p}(\mathcal{G}_{k,d}).$$

Thus, any cubature of strength $2p$ is a tight p-fusion frame. The converse implication does not hold in general except for p or k equals 1.

3. Signal reconstruction in the case of a cubature of strength 4

Let $\mathscr{H}$ denote the collection of symmetric matrices in $\mathbb{R}^{d\times d}$. If $\{P_{V_j}\}_{j=1}^n$ spans $\mathscr{H}$, then standard results in frame theory imply that $S : \mathscr{H} \to \mathscr{H}$ given by $X \mapsto \sum_{j=1}^n \langle X, P_{V_j}\rangle P_{V_j}$ is invertible and

$$xx^* = \sum_{j=1}^n \|P_{V_j}(x)\|^2 S^{-1}(P_{V_j}), \quad \text{for all } x \in \mathbb{R}^d.$$

By imposing stronger conditions on $\{P_{V_j}\}_{j=1}^n$, the operator S can be inverted explicitly. To that end, we establish the following result that generalizes the case $k = 1$ treated in [6]. We point out that we allow for cubatures as opposed to projective designs in [6] that require the cubature weights to be constant:

Proposition 3.1. *Let $\{(V_j, \omega_j)\}_{j=1}^n$ be a cubature of strength 4 for $\mathcal{G}_{k,d}$. If $x \in S^{d-1}$, then*

$$P_x = a_1 \sum_{j=1}^n \omega_j \|P_{V_j}(x)\|^2 P_{V_j} - a_2 I, \tag{11}$$

where $a_1 = \frac{d(d+2)(d-1)}{2k(d-k)}$ and $a_2 = \frac{kd+k-2}{2(d-k)}$.

Proof. For any $x, y \in S^{d-1}$, the function $V \mapsto \langle P_x, P_V\rangle\langle P_y, P_V\rangle$ belongs to $\mathrm{Pol}_{\leq 4}(\mathcal{G}_{k,d})$. Applying the cubature formula yields

$$\sum_{j=1}^n \omega_j \langle P_x, P_{V_j}\rangle\langle P_y, P_{V_j}\rangle = \int_{\mathcal{G}_{k,d}} \langle P_x, P_V\rangle\langle P_y, P_V\rangle d\sigma_k(V). \tag{12}$$

The function

$$G : (\mathbb{R}x, \mathbb{R}y) \mapsto \int_{\mathcal{G}_{k,d}} \langle P_x, P_V\rangle\langle P_y, P_V\rangle d\sigma_k(V) \tag{13}$$

belongs to $L^2(\mathcal{G}_{1,d} \times \mathcal{G}_{1,d})$ and is zonal. For each variable, it has the form $\mathbb{R}x \mapsto \langle P_x, A(y)\rangle$, where $A(y) = \int_{\mathcal{G}_{k,d}} \langle P_y, P_V\rangle P_V d\sigma_k(V)$, and $\mathbb{R}y \mapsto \langle P_y, A(x)\rangle$, respectively. Since $A(y)$ is self-adjoint and hence a linear combination of projections, $G(\cdot, \mathbb{R}y)$ and $G(\mathbb{R}x, \cdot)$ belong to $\mathrm{Pol}_{\leq 2}(\mathcal{G}_{1,d})$. The zonal functions on the projective space are polynomials in the variable $\langle P_x, P_y\rangle = (x, y)^2$, so that G must be of the form $\alpha_1(x, y)^2 + \alpha_2$. Thus, (12) yields

$$\sum_{j=1}^n \omega_j \langle P_x, P_{V_j}\rangle\langle P_y, P_{V_j}\rangle = \alpha_1\langle P_x, P_y\rangle + \alpha_2\langle I, P_y\rangle. \tag{14}$$

Since (14) holds for every y, we derive

$$\sum_{j=1}^n \omega_j \langle P_x, P_{V_j}\rangle P_{V_j} = \alpha_1 P_x + \alpha_2 I. \tag{15}$$

Taking traces in (15) leads to $k\sum_{j=1}^n \omega_j\langle P_x, P_{V_j}\rangle = \alpha_1 + d\alpha_2$, and the property of tight 1-fusion frames gives $\sum_{j=1}^n \omega_j\langle P_x, P_{V_j}\rangle = A_1 = k/d$, so we obtain

$$\alpha_1 + d\alpha_2 = k^2/d. \tag{16}$$

Taking $x = y$ in (14) implies $\sum_{j=1}^n \omega_j\langle P_x, P_{V_j}\rangle^2 = \alpha_1 + \alpha_2$, and the tight 2-fusion frame property leads to $\sum_{j=1}^n \omega_j\langle P_x, P_{V_j}\rangle^2 = A_2 = k(k+2)/(d(d+2))$, so that we obtain

$$\alpha_1 + \alpha_2 = k(k+2)/(d(d+2)). \tag{17}$$

Solving for α_1 and α_2 in (16) and (17) yields the required identity with $a_1 = 1/\alpha_1$ and $a_2 = \alpha_2/\alpha_1$. □

Remark 3.2. Since any $X \in \mathscr{H}$ can be written as a sum of weighted orthogonal projectors, (11) can be extended to

$$X = a_1 \sum_{j=1}^n \omega_j \langle X, P_{V_j}\rangle P_{V_j} - a_2 \,\mathrm{trace}(X) I. \tag{18}$$

For $x \in \mathbb{R}^d$ and $X = xx^*$, the tight-1 fusion frame property yields $\operatorname{trace}(X) = \|x\|^2 = \frac{d}{k}\sum_{j=1}^n \omega_j \|P_{V_j}(x)\|^2$, so that the entire right-hand side of (18) can be computed from $\{\|P_{V_j}(x)\|^2\}_{j=1}^n$ and hence $\pm x$ can be recovered.

We can conclude from (18) that $\{\omega_j P_{V_j}\}_{j=1}^n$ and $\{Q_j\}_{j=1}^n$, where $Q_j = a_1 P_{V_j} - a_2 \frac{d}{k} I$, are pairs of dual frames for $\mathscr{H}$, i.e.,

$$X = \sum_{j=1}^n \langle X, \omega_j P_{V_j}\rangle Q_j, \quad \text{for all } X \in \mathscr{H}.$$

Moreover, if V is a random subspace, uniformly distributed in $\mathcal{G}_{k,d}$, i.e., distributed according to σ_k, then the proof of Proposition 3.1 yields that

$$a_1 \mathbb{E}(\langle X, P_V\rangle P_V) - a_2 \operatorname{trace}(X) I = X, \tag{19}$$

for all $X \in \mathscr{H}$. Thus, if $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ are independent copies of V, then the law of large numbers implies

$$\frac{a_1}{n}\sum_{j=1}^n \langle X, P_{V_j}\rangle P_{V_j} - a_2 \operatorname{trace}(X) I \to X \quad \text{almost surely.} \tag{20}$$

However, n must be chosen large to obtain an accurate representation of X. In Sections 5 and 6, we shall see that the random choice of subspaces can be efficient when the algebraic reconstruction formula is replaced with a semidefinite program.

4. Algorithm for signal reconstruction from magnitudes of incomplete subspace components

In this section, we consider the situation where $x \in S^{d-1}$ and we aim to reconstruct $\pm x$ from only $n-p$ elements of the set $\{\|P_{V_j}(x)\|^2\}_{j=1}^n$. Without loss of generality, we assume that the first p norms have been erased, so we want to recover $\pm x$ from the knowledge of $\{\|P_{V_j}(x)\|\}_{j=p+1}^n$.

In a first step, we attempt to compute the missing values

$$t_j := \|P_{V_j}(x)\|^2, \quad 1 \le j \le p.$$

This will be made possible by the property that $\{(V_j, \omega_j)\}_{j=1}^n$ is a tight p-fusion frame with $\sum_{j=1}^n \omega_j = 1$. The second step is dedicated to reconstructing $\pm x$ from $\{\|P_{V_j}(x)\|^2\}_{j=1}^n$.

4.1. **Step 1: reconstruction of the erased norms.** The tight p-fusion frame $\{(V_j, \omega_j)\}_{j=1}^n$ is also a tight ℓ-fusion frame for $1 \le \ell \le p$, cf. [5, Proposition 5.1], so that (6) yields

$$\sum_{j=1}^n \omega_j \|P_{V_j}(x)\|^{2\ell} = A_\ell = \frac{(k/2)_\ell}{(d/2)_\ell}, \quad 1 \le \ell \le p.$$

Therefore, $(t_1, \dots, t_p)$ is a solution of the algebraic system of equations

$$\sum_{j=1}^p \omega_j T_j^\ell = \frac{(k/2)_\ell}{(d/2)_\ell} - \sum_{j=p+1}^n \omega_j \|P_{V_j}(x)\|^{2\ell}, \quad 1 \le \ell \le p, \tag{AE}$$

in the unknowns $(T_1, \dots, T_p)$. To start with, let us consider the special case of equal weights; then, (AE) gives the values of the symmetric powers $\sum_{j=1}^p t_j^\ell$, for

$\ell = 0, \ldots, p$, which, as polynomial expressions, generate the ring of symmetric polynomials up to degree p. Vieta's formula yields

$$\prod_{i=1}^{p}(T - t_i) = \sum_{j=0}^{p}(-1)^j e_j T^{p-j}, \quad \text{where } e_0 = 1 \text{ and } e_j = \sum_{1 \le i_1 < \ldots < i_j \le p} t_{i_1} \cdots t_{i_p},$$

and Newton's identity leads to

$$e_j = \frac{1}{j}\sum_{\ell=1}^{j}(-1)^{\ell-1} e_{j-\ell} \sum_{j=1}^{p} t_j^{\ell}, \quad \text{for } j = 1, \ldots, p.$$

Therefore, we can compute the coefficients of $\prod_{i=1}^{p}(T - t_i)$ as a polynomial in T and solve for its roots; we see that $(t_1, \ldots, t_p)$ is determined up to a permutation so that we obtain at most $p!$ distinct solutions to (AE).

If the weights are not equal, one can still show that (AE) has at most $p!$ solutions. The issue is to verify that the associated affine variety is zero-dimensional. Results from intersection theory and the refined Bézout theorem, cf. [31, 41] and [10], then imply that the variety's cardinality is at most the product of the degrees of the p polynomials, i.e., there are at most $p!$ solutions:

Proposition 4.1. *Let $\{b_\ell\}_{\ell=1}^{p}$ be complex numbers and define*

$$f_\ell(T) = \sum_{j=1}^{p} \omega_j T_j^{\ell} - b_\ell, \quad \ell = 1, \ldots, p.$$

If $\{\omega_j\}_{j=1}^{p}$ are positive numbers, then the affine variety $\mathcal{V} := \{T \in \mathbb{C}^p : f_1(T) = 0, \ldots, f_p(T) = 0\}$ is zero-dimensional.

Proof. We proceed by induction on p. The assertion is certainly true for $p = 1$. Next, we observe that the Jacobian determinant satisfies

$$\det\Big(\frac{\partial(f_1, \ldots, f_p)}{\partial(T_1, \ldots, T_p)}\Big) = \omega_1 \cdots \omega_p \cdot p! \cdot \prod_{1 \le i < j \le p}(T_j - T_i),$$

where we used the well-known formula for the Vandermonde determinant. For $i < j$, let $\Delta_{i,j} := \{T \in \mathbb{C}^d : T_i = T_j\}$, denotes the diagonals. The Jacobian determinant is apparently nonzero for $T \notin \bigcup_{i<j} \Delta_{i,j}$. Therefore, every $T \in \mathcal{V} \setminus \bigcup_{i<j} \Delta_{i,j}$ is a nonsingular point of $\mathcal{V}$, and the dimension of $\mathcal{V}$ at T is $p - p = 0$, cf. [20, Theorem 9.9] and [10, Lemma 11.5.1]. It remains to consider the intersection of $\mathcal{V}$ with $\Delta_{i,j}$. To fix ideas, let us consider the case $i = 1$, $j = 2$. The intersection $\mathcal{V} \cap \Delta_{1,2}$ is given by the system of equations

$$(\omega_1 + \omega_2) T_2^{\ell} + \sum_{j=3}^{p} \omega_j T_j^{\ell} = b_\ell, \quad \ell = 1, \ldots, p.$$

Because $\omega_1 + \omega_2 > 0$, by induction the first $p - 1$ of these equations have only finitely many solutions. Thus, $\mathcal{V} \cap \Delta_{1,2}$ is finite, too. □

Remark 4.2. The above proof shows that the positivity assumption on the weights in Proposition 4.1 can be replaced with $\omega_{j_1} + \ldots + \omega_{j_i} \neq 0$, for all $1 \le j_1 < \ldots < j_i \le p$ and $i = 1 \ldots, p$.

We have proved that the system of algebraic equations (AE) has at most $p!$ complex solutions. In order to compute these solutions, standard algorithmic methods can be applied [19, 20]. The construction of a Gröbner basis of the ideal $\mathcal{I}$ generated by the p equations allows to compute the algebraic operations in the quotient ring $\mathbb{R}[T_1, \dots, T_p]/\mathcal{I}$, which is finite dimensional and of dimension at most $p!$. The computation of the solutions then boils down to linear algebra in this space.

4.2. **Step 2: reconstruction from the magnitude of subspace components.** In this second step, we try to compute P_x from each of the possible candidates for $\{\|P_{V_j}(x)\|^2\}_{j=1}^n$ derived from a solution $(t_1, \dots, t_p)$ of (AE). For this, we assume that $\{(V_j, \omega_j)\}_{j=1}^n$ is also a cubature of strength 4, and we apply formula (11) where we replace $\|P_{V_j}(x)\|^2$ by t_j for $1 \le i \le p$.

To summarize, we have proved:

Theorem 4.3. *Let $\{(V_j, \omega_j)\}_{j=1}^n$ be a tight p-fusion frame that is also a cubature of strength 4 for $\mathcal{G}_{k,d}$. If $x \in S^{d-1}$, then Algorithm 1 outputs a list L of at most $2p!$ elements of S^{d-1} containing x.*

Algorithm 1 *List reconstruction*

Input: $\{t_j := \|P_{V_j}(x)\|^2\}_{j=p+1}^n$.
Output: L, $x \in L$.

1: *Initialize* $L = \emptyset$.
2: *Compute the set $\mathcal{S}$ of solutions of the algebraic system of equations in the unknowns $T_1, \dots, T_p$:*

$$\text{(AE)} \qquad \sum_{j=1}^p \omega_j T_j^\ell = \frac{(k/2)_\ell}{(d/2)_\ell} - \sum_{j=p+1}^n \omega_j t_j^\ell, \quad 1 \le \ell \le p.$$

3: *For every $(t_1, \dots, t_p) \in \mathcal{S}$, and α, β defined in Proposition 3.1, compute*

$$P = a_1 \sum_{j=1}^n \omega_j t_j P_{V_j} - a_2 I.$$

4: *If P is a projection of rank 1, compute a unit vector ξ spanning its image and add $\pm\xi$ to L.*
5: ***return*** L

We note that the actual output list L can be much shorter than $2p!$ because many solutions of the algebraic system of equations will not lead to a candidate for the signal x. In the first place, we can exclude those solutions of (AE) that are not real or have negative entries. Moreover, one can expect that, for most solutions of (AE), the symmetric operator P in step 3 is not a rank-one projector. Also, the solutions $(t_1, \dots, t_p)$ of (AE) that do not satisfy $|t_i^{1/2} - t_j^{1/2}|^2 \le \|P_{V_i} - P_{V_j}\|^2$, for every $1 \le i < j \le n$, can be removed because they violate the consistency conditions

$$|\|P_{V_i}(x)\| - \|P_{V_j}(x)\||^2 \le \|P_{V_i}(x) - P_{V_j}(x)\|^2 \le \|P_{V_i} - P_{V_j}\|_\infty^2,$$

where $\|P_{V_i} - P_{V_j}\|_\infty$ denotes the operator norm of $P_{V_i} - P_{V_j}$.

Remark 4.4. For $p = 2$, the assumptions in Theorem 4.3 reduce to $\{(V_j, \omega_j)\}_{j=1}^n$ being a cubature of strength 4 for $\mathcal{G}_{k,d}$. Even for $k = 1$, our result extends [6] since we only need $n - 2$ elements of the collection $\{\|P_{V_j}(x)\|^2\}_{j=1}^n$ as opposed to all n elements in [6]. This additional flexibility is not for free: We must assume that $x \in S^{d-1}$, and, instead of the two possibilities $\pm x$ in [6], we obtain a list L of 4 elements, one of which is x.

5. Replacing the algebraic reconstruction formula with semidefinite programming

We assume in Proposition 3.1 that the weighted subspaces form a cubature of strength 4 for $\mathcal{G}_{k,d}$. However, any real cubature of strength 4 requires at least $\frac{1}{2}d(d+1)$ subspaces, see [23]. Hence, the cardinality scales at least quadratically in the ambient dimension d. In this section, we replace the algebraic reconstruction formula with a feasibility problem of a semidefinite program similar to the approach in [14, 24], where the case $k = 1$ was discussed.

Recall that $\mathscr{H}$ denotes the collection of symmetric matrices in $\mathbb{R}^{d\times d}$. For $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$, we define the operator

$$\mathcal{F}_n : \mathscr{H} \to \mathbb{R}^n, \quad X \mapsto \frac{d}{k}(\langle X, P_{V_j}\rangle)_{j=1}^n. \tag{21}$$

For $x \in \mathbb{R}^d$, let $f := \frac{d}{k}(\|P_{V_j}(x)\|^2)_{j=1}^n = \mathcal{F}_n(xx^*) \in \mathbb{R}^n$, and we now aim to reconstruct $\pm x$ from f. By assuming that the union of the subspaces $\{V_j\}_{j=1}^n$ spans $\mathbb{R}^d$, clearly, xx^* is a solution of

$$\min_{X\in\mathscr{H}}(\mathrm{rank}(X)), \quad \text{subject to} \quad \mathcal{F}_n(X) = f,\ X \succeq 0. \tag{22}$$

The notation $X \succeq 0$ stands for X being positive semidefinite. Rank minimization is in general NP-hard, and in convex optimization it is standard to replace (22) with

$$\min_{X\in\mathscr{H}}(\mathrm{trace}(X)), \quad \text{subject to} \quad \mathcal{F}_n(X) = f,\ X \succeq 0, \tag{23}$$

a semidefinite program, for which efficient algorithms based on interior point methods are available. The NEOS Server [21] provides online solvers for semidefinite programs. We know that the solution of (22) has rank 1, so there is more structure to it and, as in [24], we can consider the underlying feasibility problem, i.e.,

$$\text{find } X \in \mathscr{H}, \quad \text{subject to} \quad \mathcal{F}_n(X) = f,\ X \succeq 0. \tag{24}$$

For $k = 1$, there is a constant $c > 0$, such that the random choice of at least cd subspaces yields that, with high probability, xx^* is the only solution to (24), i.e., the only feasible point of (22) and (23), cf. [13, 14, 24]. Here, we extend the result to $k > 1$:

Theorem 5.1. *There are constants $c_1, c_2 > 0$ such that, if $n \geq c_1 d$ and $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ are chosen independently identically distributed according to σ_k, then, for all $x \in \mathbb{R}^d$, the matrix xx^* is the unique solution to* (24) *with probability at least $1 - e^{-c_2 n}$.*

Note that the probability of exact recovery in Theorem 5.1 holds simultaneously over all input signals $x \in \mathbb{R}^d$, and the constants are independent of the ambient dimension d but may depend on the subspace dimension k.

To verify Theorem 5.1, we shall first derive deterministic conditions serving uniqueness in (24). Later, we shall verify that these conditions are satisfied with high probability when the subspaces are chosen in the appropriate random fashion.

A simple rescaling allows us to restrict the considerations to $x \in S^{d-1}$. Let $T := T_x := \{xy^* + yx^* : y \in \mathbb{R}^d\} \subset \mathscr{H}$, and, for $Z \in \mathbb{R}^{d\times d}$, denote Z_T its orthogonal projection onto T and $Z_{T^\perp}$ its orthogonal projection onto the orthogonal complement of T. The term $\|\cdot\|_1$ denotes the nuclear norm and $\|\cdot\|_\infty$ the operator norm:

Theorem 5.2. *Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ and $f = (\|P_{V_j}(x)\|^2)_{j=1}^n$. Assume that $0 < A_k, B$ and $\gamma < A_k/B$ are fixed numbers, such that the following three points are satisfied:*

(a) *For all positive semidefinite matrices $X \in \mathscr{H}$,*

$$\frac{1}{n}\|\mathcal{F}_n(X)\|_{\ell_1} \le B\|X\|_1. \tag{25}$$

(b) *For all $X \in T$,*

$$A_k\|X\|_\infty \le \frac{1}{n}\|\mathcal{F}_n(X)\|_{\ell_1}. \tag{26}$$

(c) *There exists Y in the range of $\mathcal{F}_n^*$ such that*

$$\|Y_T\|_1 \le \gamma, \qquad Y_{T^\perp} \succeq I_{T^\perp}. \tag{27}$$

Then xx^* is the unique solution to (24).

The matrix Y in (27) was called a dual certificate in [14]. To verify Theorem 5.2, we can straightforwardly follow the lines of the proof in [13, 24] while keeping track of the constants, so we omit the explicit proof, see also [14, 17].

Remark 5.3. If $\{V_j\}_{j=1}^n$ is a design of strength 4, then the conditions in Theorem 5.2 can be satisfied. Indeed, we can choose $B = 1$ and there is $A_k > 0$ satisfying (26) that is even allowed to depend on d in this case. Since $\mathcal{F}_n^*$ is onto, the certificate $Y = 2I - 2P_x$ is admissible and γ can be zero.

In the subsequent sections, we shall verify that the conditions of Theorem 5.2 are satisfied with high probability when the subspaces $\{V_j\}_{j=1}^n$ are selected at random.

5.1. **Nuclear norm estimates on $\|\mathcal{F}_n(X)\|_{\ell_1}$ for $X \succeq 0$.** We shall verify that $\mathcal{F}_n$ is close to an isometry with high probability:

Theorem 5.4. *Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ be independently chosen random subspaces with identical distribution σ_k. For $0 < r < 1$ fixed, there are constants $c(r), C(r) > 0$, such that, for all positive semidefinite matrices X and $n \ge c(r)d$,*

$$(1-r)\|X\|_1 \le \frac{1}{n}\|\mathcal{F}_n(X)\|_{\ell_1} \le (1+r)\|X\|_1 \tag{28}$$

holds with probability at least $1 - e^{-C(r)n}$.

By using the spectral decomposition of X, we see that condition (28) is equivalent to

$$(1-r)\frac{nk}{d}\|x\|^2 \le \sum_{j=1}^n \|P_{V_j}(x)\|^2 \le (1+r)\frac{nk}{d}\|x\|^2, \quad \text{for all } x \in \mathbb{R}^d.$$

In other words, $\{V_j\}_{j=1}^n$ is a fusion frame that is not too far from being tight. The present section is dedicated to verify that we can follow the lines in [14] to prove Theorem 5.4 after having established few analogies between $k=1$ and $k>1$.

Lemma 5.5. *If V is a random subspace distributed according to σ_k on $\mathcal{G}_{k,d}$, then, for any $x \in S^{d-1}$,*

$$\sup_{p\geq 1} p^{-1}\big(\mathbb{E}(\frac{d}{k}\|P_V(x)\|^2)^p\big)^{1/p} \leq 1. \tag{29}$$

Note that Lemma 5.5 says that $\frac{d}{k}\|P_V(x)\|^2$ is a sub-exponential random variable with a bound in (29) that does not depend on d.

Proof of Lemma 5.5. The distribution of $\|P_V(x)\|^2$ does not depend on the particular choice of $x \in S^{d-1}$ and is beta distributed with parameters $(\frac{k}{2}, \frac{d-k}{2})$. Thus, its moments are given by

$$\mathbb{E}\|P_V(x)\|^{2p} = \frac{(k/2)_p}{(d/2)_p} = \frac{k(k+2)\cdots(k+2p-2)}{d(d+2)\cdots(d+2p-2)}, \tag{30}$$

which coincide with the tight p-fusion frame bounds (6) when the weights are constant. An induction over p yields (29). □

The following result extends findings on the smallest and largest singular values $s_{\min}(P)$ and $s_{\max}(P)$ of a random matrix P with independent sub-exponential rows in [42, Theorem 5.39]. Here, we consider independent blocks but there are dependent rows within each block:

Proposition 5.6. *Let $P := \sqrt{\frac{d}{k}}\big(P_{V_1}, \ldots, P_{V_n}\big)^* \in \mathbb{R}^{nd\times d}$, in which $\{V_j\}_{j=1}^n$ are identically and independently distributed according to σ_k on $\mathcal{G}_{k,d}$. Then, for every $t \geq 0$, we have with probability at least $1-2\exp(-ct^2)$*

$$\sqrt{n} - C\sqrt{d} - t \leq s_{\min}(P) \leq s_{\max}(P) \leq \sqrt{n} + C\sqrt{d} + t,$$

where $c, C > 0$ are absolute constant.

Since we know that $\frac{d}{k}\|P_V(e_1)\|^2$ is sub-exponential, we can follow the lines of the proof of [42, Theorem 5.39] to verify Proposition 5.6. We point out that the proof involves nets. A (spherical) ε-net $\mathcal{N}_\varepsilon$ is a finite subset of S^{d-1} such that to any element $x \in S^{d-1}$, there is an element in $\mathcal{N}_\varepsilon$ at distance less than or equals ε. The latter with [42, Lemma 5.36], [42, Lemma 5.4], [42, Corollary 5.17], and [42, Lemma 5.2] are the required tools to complete the proof. We omit the details and point out that a related result is obtained in [22].

Since the required extension by means of Proposition 5.6 is available, we can follow the lines in [14] and derive Theorem 5.4.

5.2. **Operator norm estimates on $\|\mathcal{F}_n(X)\|_{\ell_1}$ for symmetric rank-2 matrices.** We shall verify the condition (26):

Theorem 5.7. *There is a constant $u_k > 0$, only depending on k, such that the following holds: for $0 < r < 1$ fixed, there exist constants $c(r), C(r) > 0$, such that, for all $n \geq c(r)d$ and $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ independently chosen random subspaces with identical distribution σ_k, the inequality*

$$\frac{1}{n}\|\mathcal{F}_n(X)\|_{\ell_1} \geq u_k(1-r)\|X\|_\infty,$$

for all symmetric rank-2 matrices X, holds with probability at least $1 - e^{-C(r)n}$.

Note that the probability in the estimate in Theorem 5.7 is uniform in X. To verify Theorem 5.7, we need a preparatory result:

Proposition 5.8. *Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ be independently chosen random subspaces with identical distribution σ_k. There is a constant $u_k > 0$ such that, for all $-1 \leq t \leq 1$ and $z_1, z_2 \in S^{d-1}$ with $z_1 \perp z_2$,*

$$\frac{d}{k}\mathbb{E}\big|\|P_V(z_1)\|^2 - t\|P_V(z_2)\|^2\big| \geq u_k.$$

Proof. The sphere is two-point homogeneous and σ_k is invariant under orthogonal transformation so that we can restrict the analysis to the first two canonical basis vectors e_1 and e_2. Since the integral is always nonzero, we only need to take care of the limit $d \to \infty$. We first see that

$$\begin{aligned}\frac{d}{k}\mathbb{E}\big|\|P_V(e_1)\|^2 - t\|P_V(e_2)\|^2\big| &= \frac{d}{k}\int_{\mathcal{G}_{k,d}} \big|\|P_V(e_1)\|^2 - t\|P_V(e_2)\|^2\big| d\sigma_k(V) \\ &= \frac{d}{k}\int_{\mathcal{V}_{2,d}} \big|\sum_{i=1}^k m_{i,1}^2 - t\sum_{i=1}^k m_{i,2}^2\big| d\nu_2(M),\end{aligned}$$

where $\mathcal{V}_{2,d} = \{M = (m_{i,j}) \in \mathbb{R}^{d\times 2} : M^*M = I\}$ denotes the Stiefel-manifold endowed with the standard probability measure ν_2. If M is a random matrix, distributed according to ν_2, then, according to [26, Proposition 7.5], the upper $k \times 2$ block of M multiplied by d converges in distribution (for $d \to \infty$) towards a random $k \times 2$ matrix whose entries are standard normal i.i.d.. Let us denote the underlying probability measure on $\mathbb{R}^{k\times 2}$ by $\mathcal{N}(0, I_k \otimes I_2)$. The convergence in distribution implies that, for $d \to \infty$,

$$d\mathbb{E}\big|\|P_V(e_1)\|^2 - t\|P_V(e_2)\|^2\big| \to \int_{\mathbb{R}^{k\times 2}} \big|\|N(e_1)\|^2 - t\|N(e_2)\|^2\big| d\mathcal{N}(0, I_k \otimes I_2)(N).$$

Since the right-hand side is bigger than 0, for all $-1 \leq t \leq 1$, compactness and continuity arguments suffice to conclude the proof. □

Note that the constant u_k can be further specified by computing the corresponding integral in the proof of Proposition 5.8.

Proof of Theorem 5.7. It is sufficient to consider $\|X\|_\infty = 1$, so that $X = P_{z_1} - tP_{z_2}$, where $z_1, z_2 \in S^{d-1}$ and $z_1 \perp z_2$ and $t \in [-1, 1]$. We observe

$$\frac{1}{n}\|\mathcal{F}_n(X)\|_1 = \frac{1}{n}\sum_{j=1}^n \frac{d}{k}|\|P_{V_j}(z_1)\|^2 - t\|P_{V_j}(z_2)\|^2| = \frac{1}{n}\sum_{j=1}^n \xi_j,$$

where $\xi_j = \frac{d}{k}|\|P_{V_j}(z_1)\|^2 - t\|P_{V_j}(z_2)\|^2|$. Since $|t|$ is bounded, Lemma 5.5 implies that ξ_j is sub-exponential. Therefore, the Bernstein inequality as stated in [42] yields

$$\mathbb{P}(|\frac{1}{n}\|\mathcal{F}_n(X)\|_1 - \mathbb{E}\xi| \geq \varepsilon) \leq 2\exp(-cn\min(\frac{\varepsilon^2}{4}, \frac{\varepsilon}{2})),$$

where $c > 0$ is an absolute constant. Proposition 5.8 yields $\mathbb{E}\xi_j \geq u_k$, and, for $\varepsilon < 2$, we derive

$$\frac{1}{n}\|\mathcal{F}_n(X)\|_1 \geq u_k - \varepsilon,$$

with probability at least $1 - 2\exp(-C_1 n\varepsilon^2)$, where $C_1 = c/4$. The choice $\varepsilon = u_k r$ establishes the required estimate at least for fixed $X \in T$ with probability at least $1 - 2\exp(-C_2 n r^2)$, where $C_2 = C_1 u_k^2$. The remaining part of the proof is the same covering argument as in [14], so we omit this.

□

5.3. **The dual certificate Y.** To derive the dual certificate Y, we will use Proposition 3.1 from the deterministic setting and the Remark 3.2. Let $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ be independently chosen random subspaces with identical distribution σ_k. The choice $Y_1 := 2I - 2P_x$ would satisfy both conditions in (27) but may not lie in the range of

$$\mathcal{F}_n^* : \mathbb{R}^n \to \mathscr{H}, \qquad (\lambda_j)_{j=1}^n \mapsto \frac{d}{k}\sum_{j=1}^n \lambda_j P_{V_j}.$$

Thus, we aim to determine an appropriate sequence $(\lambda_j)_{j=1}^n$ such that $\frac{d}{k}\sum_{j=1}^n \lambda_j P_{V_j}$ "approximates" Y_1. First, let us rewrite $Y_1 = (k+2)I - (2P_x + kI)$ and observe that $\frac{d}{k}\mathbb{E}P_{V_j} = I$ and (19) imply

$$\frac{d^2}{k}\mathbb{E}\|P_{V_j}(x)\|^2 P_{V_j} = aP_x + bI, \tag{31}$$

where $a = \frac{2d(d-k)}{(d+2)(d-1)}$ and $b = \frac{d(kd+k-2)}{(d+2)(d-1)}$. Indeed, (19) makes the connection between the deterministic and the random setting as considered here. When d tends to infinity, then $a \to 2$ and $b \to k$. Thus, we replace Y_1 with

$$Y_2 := (k+2)I - (aP_x + bI) = \frac{d}{k}\mathbb{E}((k+2-d\|P_V(x)\|^2)P_V).$$

The sample mean converges towards the population mean, so

$$Y_3 := \frac{d}{nk}\sum_{j=1}^n ((k+2-d\|P_{V_j}(x)\|^2)P_{V_j})$$

approximates Y_2, and we observe that Y_3 lies in the range of $\mathcal{F}_n^*$. In view of tail bound estimates, it will be advantageous to use an additional cut-off similar to the one in [14]: keeping in mind that (30) yields $\frac{d^2}{k}\mathbb{E}\|P_{V_j}(x)\|^4 = k+2$, we define the dual certificate by

$$Y := \frac{d}{nk}\sum_{j=1}^n \lambda_j P_{V_j}, \quad \text{where} \quad \lambda_j = \alpha - d\|P_{V_j}(x)\|^2 1_{E_j}, \tag{32}$$

$\alpha = \frac{d^2}{k}\mathbb{E}(\|P_{V_j}(x)\|^4 1_{E_j})$, and $E_j = \{\sqrt{\frac{d}{k}}\|P_{V_j}(x)\| \le 2\beta_\gamma\}$ for some constant $\beta_\gamma > 0$. The latter definitions will be used throughout the entire remaining part of this paper.

5.3.1. *Dual certificate: Y_T.* We shall verify that the dual certificate defined by (32) satisfies the first condition in (27):

Theorem 5.9. *Let $x \in S^{d-1}$ be fixed. There are constants $c, C > 0$ such that, for $n \ge cd$,*

$$\|Y_T\|_1 \le \gamma \tag{33}$$

with probability at least $1 - e^{-Cn}$.

Proof. First, we suppose that $x = e_1$ and take care of the general case later. We observe that $\|Y_T\|_1 \leq \sqrt{2}\|Y_T\|_{HS} \leq 2\sqrt{2}\|y\|^2)$, where $y \in \mathbb{R}^d$ is the first column of Y and $\|\cdot\|_{HS}$ denotes the Frobenius norm. We split $P_{V_j} = Q_j Q_j^*$, such that $Q_j \in \mathbb{R}^{d\times k}$ with orthonormal columns. By using

$$Z = \sqrt{\frac{d}{k}}(Q_1, \dots, Q_n) \in \mathbb{R}^{d\times kn}, \qquad h = \sqrt{\frac{d}{k}} \begin{pmatrix} \lambda_1 Q_1^* e_1 \\ \vdots \\ \lambda_n Q_n^* e_1 \end{pmatrix} \in \mathbb{R}^{kn},$$

and $h_j = \sqrt{\frac{d}{k}}\lambda_j Q_j^* e_1 \in \mathbb{R}^k$, for $j = 1, \dots, n$, we see that $\|y\|^2 = \frac{1}{n^2}\|Zh\|^2$. According to Lemma 5.5, $\|h_j\|^2 = \lambda_j^2 \frac{d}{k}\|P_{V_j}(e_1)\|^2$ is sub-exponential, and [42, Corollary 5.17] implies

$$\mathbb{P}\big(\|h\|^2 - \mathbb{E}\|h\|^2 \geq n\big) \leq 2e^{-C_1 n}, \tag{34}$$

for some constant $C_1 > 0$. Since $\alpha \leq k + 2$, we observe that there is a constant $C_2 > 0$ such that $\mathbb{E}\|h\|^2 \leq C_2 n$. Thus, the above estimate (34) implies that there is a constant C_3 such that

$$\mathbb{P}\big(\|h\|^2 \geq n\big) \leq 2e^{-C_3 n}. \tag{35}$$

For $n > \log(2)/C_3$, the factor 2 can be put into a constant in the exponential, say $C > 0$.

For $q \in \mathbb{R}^{kn}$ with $\|q\| = 1$ and $q = (q_j)_{j=1}^n$, where $q_j \in \mathbb{R}^k$, we obtain

$$\|Zq\|^2 \leq \frac{d}{k}\sum_{j=1}^n \|Q_j q_j\|^2 = \frac{d}{k}\sum_{j=1}^n \|q_j\|^2 = d/k, \tag{36}$$

where we have used that the columns of Q_j are orthonormal. By combining (35) with (36), we obtain

$$\|y\|^2 = \frac{1}{n^2}\|Zh\|^2 = \frac{1}{n^2}\|h\|^2\|Z\frac{h}{\|h\|}\|^2 \leq \frac{d}{kn}$$

with probability at least $1 - e^{-Cn}$. Thus, for sufficiently large $c > 0$, the condition $n \geq cd$ implies (33).

To conclude the proof, we need to allow general $x \in S^{d-1}$. Note that there exists an orthogonal matrix U such that $x = Ue_1$. We observe that $T_x = UT_{e_1}U^*$ and $P_{UV_j} = U^* P_{V_j} U$. Therefore, the definition $Y_x := UY_{e_1}U^*$, where Y_{e_1} is the dual certificate w.r.t. e_1, is in the range of the map $\tilde{\mathcal{F}}_n$ that corresponds to $\{UV_j\}_{j=1}^n$. The latter subspaces are also i.i.d. according to σ_k. Since $(Y_x)_{T_x} = UY_{T_{e_1}}U^*$, we also derive $\|(Y_x)_{T_x}\|_1 = \|Y_{T_{e_1}}\|_1$.

□

5.3.2. *Dual certificate: $Y_{T^\top}$.* Let us verify that the dual certificate Y in (32) satisfies the second condition in (27). Indeed, we prove a slightly stronger result:

Theorem 5.10. *Let $x \in S^{d-1}$ be fixed. For all $0 < \varepsilon < 1/2$, there is $\delta \geq 3/2$ and constants $c, C > 0$ such that, for $n \geq cd$,*

$$\|Y_{T^\perp} - \delta I_{T^\perp}\|_\infty \leq \varepsilon \tag{37}$$

with probability at least $1 - e^{-Cn}$.

Note that (37) implies $Y_{T^\perp} \succeq I_{T^\perp}$.

Proof. As in the proof of Theorem 5.9, we first consider $x = e_1$. Let us split $Y = Y^{(0)} - Y^{(1)}$ into

$$Y^{(0)} = \frac{1}{n}\sum_{j=1}^{n} \alpha \frac{d}{k} P_{V_j}, \qquad Y^{(1)} = \frac{1}{n}\sum_{j=1}^{n} d\|P_{V_j}(e)\|^2 1_{E_j} \frac{d}{k} P_{V_j}.$$

First, we shall estimate $\|Y^{(0)}_{T^\perp} - \alpha I_{T^\perp}\|_\infty$, later also $\|Y^{(1)}_{T^\perp} - b_0 I_{T^\perp}\|_\infty$ for some special number b_0. We observe that $\mathbb{E}Y^{(0)} = \alpha I$. By using $P := \sqrt{\frac{d}{k}}\big(P_{V_1}, \dots, P_{V_n}\big)^*$ as in Proposition 5.6 and squaring the estimates there, we see that

$$(\sqrt{n} - C_1\sqrt{d} - t)^2 \le s^2_{\min}(P) \le s^2_{\max}(P) \le (\sqrt{n} + C_1\sqrt{d} + t)^2$$

with probability at least $1 - 2e^{-c_1 t^2}$. Since $\frac{\alpha}{n} P^* P = Y^{(0)}$, the latter implies at least for sufficiently small $t/\sqrt{n}$:

$$\|Y^{(0)} - \alpha I\|_\infty \le \alpha(C_1^2 d + t^2 + 2\sqrt{nd} + 2\sqrt{n}t + 2C_1 t\sqrt{d})$$

with the same probability. For all $\varepsilon_1 > 0$, there is c_2 sufficiently large and $\varepsilon_2 > 0$ sufficiently small such that $t = \varepsilon_2\sqrt{n}$ yields

$$\|Y^{(0)} - \alpha I\|_\infty \le \alpha\varepsilon_1,$$

for all $n \ge c_2 d$ with probability $1 - e^{-c_3 n}$. In particular, we have

$$\|Y^{(0)}_{T^\perp} - \alpha I_{T^\perp}\|_\infty \le \alpha\varepsilon_1 \tag{38}$$

with the same probability.

Let us now take care of $Y^{(1)}_{T^\perp}$. Due to the unitary invariance of σ_k, (31) for $X = P_{e_1}$ yields

$$\mathbb{E}(d\|P_{V_j}(e_1)\|^2 1_{E_j} \frac{d}{k} P_{V_j}) = a_0 P_{e_1} + b_0 I,$$

for some constants $a_0, b_0 > 0$ that depend on β_γ. Therefore, we have $\mathbb{E}Y^{(1)}_{T^\perp} = b_0 I$. The random matrix

$$X_j = \frac{d^2}{k}\|P_{V_j}(e_1)\|^2 1_{E_j}(P_{V_j})_{T^\perp} - b_0 I_{T^\perp}$$

is bounded, say by K. We find a constant $C_2 > 0$ such that $\|\mathbb{E}X_j^* X_j\|_\infty \le C_2$ implying $\|\sum_{j=1}^n \mathbb{E}X_j^* X_j\|_\infty \le nC_1$. According to [42, Theorem 5.29], we have, for all $t > 0$,

$$\mathbb{P}\big(\|\frac{1}{n}\sum_{j=1}^{n} X_j\|_\infty \ge \frac{t}{n}\big) \le 2de^{\frac{-t^2/2}{nC_2 + Kt/3}}.$$

By choosing $\varepsilon_2 > 0$ and $t = \varepsilon_3 n$, we derive

$$\mathbb{P}\big(\|\frac{1}{n}\sum_{j=1}^{n} X_j\|_\infty \ge \varepsilon_2\big) \le 2de^{-c_4 n} \le e^{-c_5 n},$$

for all $n \ge c_6 \ln(d)$. Thus, we obtain

$$\|Y^{(1)}_{T^\perp} - b_0 I_{T^\perp}\|_\infty \le \varepsilon_2, \tag{39}$$

with probability $1 - e^{-c_5 n}$, for all $n \ge c_6 \ln(d)$.

Combining (38) and (39) implies

$$\|Y_{T^\perp} - (\alpha - b_0) I_{T^\perp}\| \le \alpha\varepsilon_1 + \varepsilon_2$$

with probability at least $1 - e^{-Cn}$, for all $n \geq cd$. We can now choose $\varepsilon_1, \varepsilon_2$ sufficiently small, such that $\alpha\varepsilon_1 + \varepsilon_2 \leq \varepsilon$. The term α is bounded by $k+2$. According to Vershynin's lecture note on nonasymptotic random matrix theory (Lemma 9 in Lecture 4 on dimension reduction), we have, for all $\beta_\gamma \geq 1/2$ that $\mathbb{P}\big(E_j^c\big) \leq 2e^{k/2}e^{-k\beta_\gamma}$. Since $\mathbb{E}(\frac{d^4}{k^2}\|P_{V_j}(e_1)\|^8)$ is bounded independently of d, see (30), the term $k+2-\alpha = \mathbb{E}(\frac{d^2}{k}\|P_{V_j}(e_1)\|^4 1_{E_j^c})$ can be made arbitrarily small by choosing β_γ sufficiently large. Thus, we can derive $\alpha \geq k+5/3$. Similar arguments yield that b_0 gets closer to b when we increase β_γ. With $b \leq k$ we can assume that $b_0 \leq k + 1/6$, so that $\delta = \alpha - b_0 \geq 3/2$.

We still need to address general vectors $x \in S^{d-1}$. With the notation and arguments at the end of the proof of Theorem 5.9, we observe that $\|(Y_x)_{T_x^\perp} - \delta I_{T_x^\perp}\|_\infty = \|(Y_{e_1})_{T_{e_1}^\perp} - \delta I_{T_{e_1}^\perp}\|_\infty$, which concludes the proof.

□

5.4. **Proof of Theorem 5.1.** We can now assemble all of our findings to verify that the conditions in Theorem 5.2 hold with the required probability:

Proof of Theorem 5.1. We first fix $x \in S^{d-1}$. Then we choose $r \in (0,1)$ and $\gamma < u_k\frac{1-r}{1+r}$, where $u_k \in (0,1)$ as in Proposition 5.8. Let c_i and C_i, $i = 1, \dots, 4$, be suitable positive constants. Theorem 5.4 yields that Condition (25) holds with probability of failure at most $e^{-C_1 n}$, for all $n \geq c_1 d$. Theorem 5.7 implies that Condition (26) holds with probability of failure at most $e^{-C_2 n}$, for all $n \geq c_2 d$. According to Theorem 5.9, the first condition in (27) holds with probability of failure at most $e^{-C_3 n}$, for all $n \geq c_3 d$. Theorem 5.10 yields that the second condition in (27) is satisfied with probability of failure at most $e^{-C_4 n}$, for all $n \geq c_4 d$.

Finally, there are constants $c, C > 0$ such that, for all $n \geq cd$, we can estimate $\sum_{i=1}^4 e^{-C_i n} \leq e^{-Cn}$, so that all conditions in Theorem 5.2 are satisfied with probability at least $1 - e^{-Cn}$. In order to turn the latter into a uniform estimate in x, we take an ϵ-net $\mathcal{N}_\epsilon$ on the sphere of cardinality less or equals $(1+\frac{2}{\epsilon})^d$, cf. [42, Lemma 5.2]. Since $(1+\frac{2}{\epsilon})^d e^{-Cn} \leq e^{-\tilde{C}n}$, for all $n \geq \tilde{c}d$ when $\tilde{C}$ is sufficiently small and $\tilde{c}$ sufficiently large, we have a uniform estimate for the net $\mathcal{N}_\epsilon$. Now, to any arbitrary $x \in S^{d-1}$, we find $x_0 \in \mathcal{N}_\epsilon$ with $\|x - x_0\| \leq \epsilon$. By following the lines in [13], one can derive that the certificate for x_0 also works for x, so that we can conclude the proof of Theorem 5.1. □

5.5. **Stability.** In many applications of interest, we may have access to the exact subspaces $\{V_j\}_{j=1}^n$ but the actual measurements are noisy, so that we need to reconstruct the signal from observation of the form

$$f_j = \|P_{V_j}(x)\|^2 + \omega_j, \quad j = 1, \dots, n, \tag{40}$$

where ω_j is some distortion term. If we replace the feasibility problem of the semidefinite program with the constrained ℓ_1-minimization

$$\arg\min_{X \in \mathscr{H}} \|\mathcal{F}_n(X) - f\|_{\ell_1}, \quad \text{subject to} \quad X \succeq 0, \tag{41}$$

then we obtain the same stability properties as in [13]:

Theorem 5.11. *There are constants $c_0, c_1, c_2 > 0$ such that, if $n \geq c_1 d$ and $\{V_j\}_{j=1}^n \subset \mathcal{G}_{k,d}$ are chosen independently identically distributed according to σ_k,*

then, for all $x \in \mathbb{R}^d$ *and* f *given by* (40)*, the solution* $\hat{X}$ *to* (41) *obeys*

$$\|\hat{X} - xx^*\|_{HS} \leq c_0 \frac{\|\omega\|_{\ell_1}}{n} \tag{42}$$

with probability at least $1 - e^{-c_2 n}$.

To verify Theorem 5.11, we can follow the lines of the proof of the corresponding Theorem 1.3 in [13], so we omit the details. There, it was also pointed out that (42) implies

$$\min\big(\|\hat{x} - x\|, \|\hat{x} + x\|\big) \leq c_0 \min\big(\|x\|, \frac{\|\omega\|_{\ell_1}}{n\|x\|}\big),$$

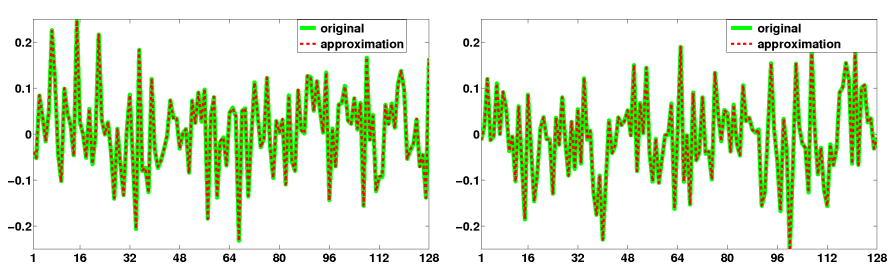
where $\hat{x} = \sqrt{\alpha} x_0$ and α is the largest eigenvalue of $\hat{X}$ with normalized eigenvector x_0. Hence, we also have a bound on the deviation to the exact signal when the measurements are noisy and $k > 1$.

6. Numerical experiments

We shall present some numerical experiments illustrating Theorem 5.1 and the choice of k. Let $x \in S^{d-1}$ and observe that $V \in \mathcal{G}_{k,d}$ is uniformly distributed if and only if $P_V = Z(Z^*Z)^{-1}Z^*$ for some $Z \in \mathbb{R}^{d\times k}$ with independent standard normal entries, cf. [18, Theorem 2.2.2]. Thus, we can easily generate pseudo-random orthogonal projectors $\{P_{V_j}\}_{j=1}^n$. Since $\|P_{V_j^\perp}(x)\|^2 + \|P_{V_j}(x)\|^2 = 1$, we shall restrict us to $k \leq d/2$. We follow the numerical experiments in [14], where the measurement vector is $f = (\|P_{V_j}(x)\|^2)_{j=1}^n$. As in [14], we use the software package Templates for First-Order Conic Solvers (TFOCS) [9]. If $\hat{X}$ is the solution, then we define $\pm\hat{x} \in S^{d-1}$ as the normalized eigenvector corresponding to the largest eigenvalue of $\hat{X}$. If x is not supposed to lie on the sphere, then we can use the largest eigenvalue to rescale the normalized eigenvector.

6.1. Examples of signal reconstruction.

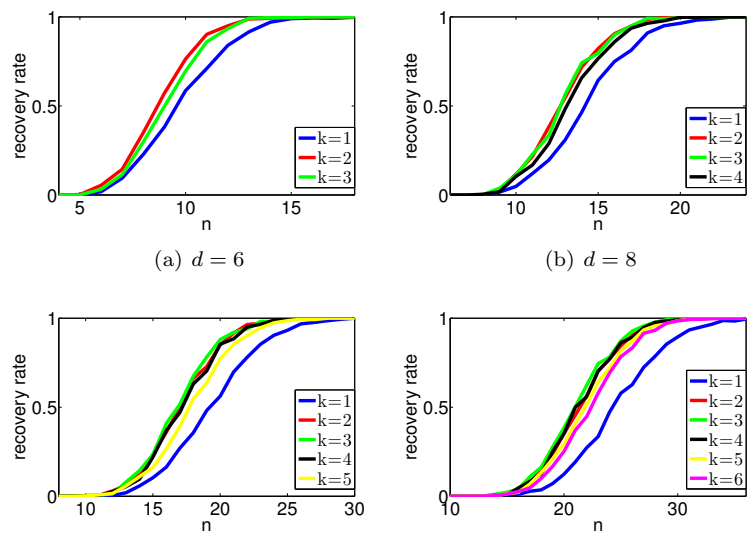
We illustrate Theorem 5.1 by following a numerical test from [12]. As in [12] for $k = 1$, the computed approximation is visually indistinguishable from the test signal when $k = 10$ and $k = 20$, where $d = 128$ and $n = 6d$, cf. Fig. 1.



(a) $k = 10$ (b) $k = 20$

Figure 1. We choose the original signal x uniformly distributed on the sphere S^{d-1}. As in [12], where $k = 1$ was used, the approximation is computed for $d = 128$ and $n = 6d$. Here, also for $k > 1$, we see that original and computed signal are visually indistinguishable.

6.2. **Optimal choice of k.** We investigate on the optimal choice of k. Indeed, for $d = 6, 8, 10, 12$, we check on the reconstruction rate in dependence of the number of subspaces n when k varies between 1 and $d/2$. We see in Figure 2 that, for small n, the proposed algorithm yields higher recovery rates when k is selected bigger than 1, and the choice $k = \lceil d/4 \rceil$ appears to be optimal. Here, the recovery rate is computed as the number of reconstructions deviating less than 10^{-2} from the original signal divided by the number of repeats (1000).



(a) $d = 6$ (b) $d = 8$

(c) $d = 10$ (d) $d = 12$

FIGURE 2. When the subspace number n is small but the subspace dimension k can be selected freely, then $k = 1$ is clearly not the optimal choice. It appears that $k = \lceil d/4 \rceil$ yields the best results.

7. Brief outline of the complex case

If we deal with complex signals $x \in \mathbb{C}^d$ and complex k-dimensional subspaces $\{V_j\}_{j=1}^n$, then there is again a canonical notion of cubature, cf. [39], and the complex analogue of Proposition 3.1 holds with adjusted constants $a_1 = \frac{(d-1)d(d+1)}{k(d-k)}$ and $a_2 = \frac{kd-1}{d-k}$.

For random subspaces, Theorem 5.1 can also be derived in the complex setting. The underlying Theorem 5.2 holds the same way for complex signals and subspaces, so that we need to verify the respective conditions as in the real case. If the subspaces are chosen i.i.d. from the Haar measure on the complex Grassmann space, then $\frac{d}{k}\|P_{V_j}(x)\|^2$ is unitarily invariant in x and sub-exponential since $\mathbb{E}\|P_{V_j}(x)\|^{2p} = \frac{(k)_p}{(d)_p}$, cf. [5]. Thus, the analogue of Lemma 5.5 holds. Proposition 5.8 can be extended to the complex case, because the underlying result from [26, Proposition 7.5] has a complex version too. The formula (31) still holds, only the constants a and b need adjustments, so that the dual certificate Y can be defined the same way as in (32).

Acknowledgements

The authors would like to thank Thomas Bauer for valuable advice on the proof of Proposition 4.1 and Pierre Thibault for discussions on diffraction imaging. The authors are also thankful to Frank Vallentin and Christian Reiher for discussions on the proof of Theorem 5.1. M. E. has been funded by the Vienna Science and Technology Fund (WWTF) through project VRG12-009.

References

[1] C. Bachoc, *Designs, groups and lattices*, J. Theor. Nombres Bordeaux (2005), 25–44.

[2] ———, *Linear programming bounds for codes in Grassmannian spaces*, IEEE Trans. Inf. Th. **52** (2006), no. 5, 2111–2125.

[3] C. Bachoc, E. Bannai, and R. Coulangeon, *Codes and designs in Grassmannian spaces*, Discrete Mathematics **277** (2004), 15–28.

[4] C. Bachoc, R. Coulangeon, and G. Nebe, *Designs in Grassmannian spaces and lattices*, J. Algebraic Combinatorics **16** (2002), 5–19.

[5] C. Bachoc and M. Ehler, *Tight p-fusion frames*, Appl. Comput. Harmon. Anal. **35** (2013), no. 1, 1–15.

[6] R. Balan, B. G. Bodmann, P. G. Casazza, and D. Edidin, *Painless reconstruction from magnitudes of frame coefficients*, J. Fourier Anal. Appl. **15** (2009), no. 4, 488–501.

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

[8] H. H. Bauschke, P. L. Combettes, and D. R. Luke, *Phase retrieval, error reduction algorithm, and Fienup variants: A view from convex optimization*, J. Opt. Soc. Amer. A **19** (2002), 1334–1345.

[9] S. Becker, E. J. Candès, and M. Grant, *Templates for convex cone problems with applications to sparse signal recovery*, Mathematical Programming Computation **3** (2011), no. 3, 165–218.

[10] J. Bochnak, M. Coste, and M. Roy, *Real algebraic geometry*, Springer-Verlag, 1998.

[11] B. G. Bodmann and V. I. Paulsen, *Frames, graphs and erasures*, Lin. Alg. Appl. **404** (2005), 118–146.

[12] E. J. Candès, Y. Eldar, T. Strohmer, and V. Voroninski, *Phase retrieval via matrix completion*, arXiv:1109.0573v2 (2011).

[13] E. J. Candès and X. Li., *Solving quadratic equations via PhaseLift when there are about as many equations as unknowns*, Foundations of Computational Mathematics (2013).

[14] E. J. Candès, T. Strohmer, and V. Voroninski, *PhaseLift: Exact and stable signal recovery from magnitude measurements via convex programming*, Communications on Pure and Applied Mathematics, DOI:10.1002/cpa.21432 **66** (2013), no. 8, 1241–1274.

[15] P. G. Casazza, G. Kutyniok, and S. Li, *Fusion frames and distributed processing*, Appl. Comput. Harmon. Anal. **25** (2008), no. 1, 114–132.

[16] A. Chai, M. Moscoso, and G. Papanicolaou, *Array imaging using intensity-only measurements*, Inverse Problems **27** (2011), no. 015005.

[17] V. Chandrasekaran, B. Recht, P. A. Parrilo, and A. S. Willsky, *The convex geometry of linear inverse problems*, arXiv:1012.0621v3 (2012).

[18] Y. Chikuse, *Statistics on special manifolds*, Lecture Notes in Statistics, Springer, New York, 2003.

[19] A. M. Cohen, H. Cuypers, and H. Sterk (eds.), *Some tapas of computer algebra*, Algorithms and Computation in Mathematics, vol. 4, Springer, 1999.

[20] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, 1996.

[21] J. Czyzyk, M. Mesnier, and J. Moré, *The NEOS server*, IEEE Computational Science & Engineering **5** (1998), no. 3, 68–75.

[22] S. Dasgupta and A. Gupta, *An elementary proof of a theorem of Johnson and Lindenstrauss*, Random Structures & Algorithms **22** (2003), no. 1, 60–65.

[23] P. de la Harpe and C. Pache, *Cubature formulas, geometrical designs, reproducing kernels, and Markov operators*, Infinite groups: geometric, combinatorial and dynamical aspects (Basel), vol. 248, Birkhäuser, 2005, pp. 219–267.

[24] L. Demanet and P. Hand, *Stable optimizationless recovery from phaseless linear measurements*, ArXiv (2012).

[25] J. Drenth, *Principles of protein x-ray crystallography*, Springer, 2010.
[26] M. L. Eaton, *Group invariance applications in statistics*, Regional Conference Series in Probability and Statistics, Institute of Mathematical Statistics, 1989.
[27] M. Ehler and K. Okoudjou, *Minimization of the probabilistic p-frame potential*, J. Stat. Plann. Inference **142** (2012), no. 3, 645–659.
[28] P. Elias, *Error-correcting codes for list decoding*, IEEE Trans. Inform. Theory **37** (1991), no. 1, 5–12.
[29] V. Elser and R. P. Millane, *Reconstruction of an object from its symmetry-averaged diffraction pattern*, Acta Crystallographica Section A **64** (2008), no. 2, 273–279.
[30] J. R. Fienup, *Phase retrieval algorithms: a comparison*, Applied Optics **21** (1982), no. 15, 2758–2769.
[31] W. Fulton, *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 2, Springer-Verlag, 1984.
[32] R. W. Gerchberg and W. O. Saxton, *A practical algorithm for the determination of the phase from image and diffraction plane pictures*, Optik **35** (1972), no. 2, 237–246.
[33] R. Goodman and N. R. Wallach, *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications, vol. 68, Cambridge University Press, 1998.
[34] R. B. Holmes and V. Paulsen, *Optimal frames for erasures*, Lin. Alg. Appl. **377** (2004), 31–51.
[35] J. Kovačević and A. Chebira, *Life beyond bases: The advent of frames (part i)*, IEEE Signal Processing Mag. **24** (2007), no. 4, 86–104.
[36] G. Kutyniok, A. Pezeshki, R. Calderbank, and T. Liu, *Robust dimension reduction, fusion frames, and Grassmannian packings*, Appl. Comput. Harmon. Anal. **26** (2009), no. 1, 64–76.
[37] D. Langemann and M. Tasche, *Phase reconstruction by a multilevel iteratively regularized Gauss–Newton method*, Inverse Problems **24** (2008), no. 3.
[38] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric informationally complete quantum measurements*, J. Math. Phys. **45** (2004), 2171–2180.
[39] A. Roy, *Bounds for codes and designs in complex subspaces*, Journal of Algebraic Combinatorics **31** (2010), no. 1, 1–32.
[40] A. J. Scott, *Tight informationally complete quantum measurements*, Journal of Physics A-Mathematical and General **39** (2006), no. 43, 13507–13530.
[41] F. Sottile, *From enumerative geometry to solving systems of polynomial equations*, vol. 2, Springer-Verlag, 2001.
[42] R. Vershynin, *Introduction to the non-asymptotic analysis of random matrices*, Compressed sensing, Theory and Applications (Y. Eldar and G. Kutyniok, eds.), Cambridge University Press, 2012, pp. 210–268.
[43] I. Waldspurger, A. d'Aspremont, and S. Mallat, *Phase recovery, maxcut and complex semidefinite programming*, arXiv:1206.0102v2 (2012).

(C. Bachoc) Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
E-mail address: `Christine.Bachoc@math.u-bordeaux1.fr`

(M. Ehler) University of Vienna, Department of Mathematics, Oskar-Morgenstern-Platz 1 A-1090 Vienna
E-mail address: `martin.ehler@univie.ac.at`