

# Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements

Aidan Roy<sup>1,\*</sup> and A. J. Scott<sup>2,†</sup>

<sup>1</sup>*Institute for Quantum Information Science,  
University of Calgary, Calgary, Alberta T2N 1N4, Canada*

<sup>2</sup>*Centre for Quantum Computer Technology,  
Centre for Quantum Dynamics, School of Science,  
Griffith University, Brisbane, Queensland 4111, Australia*

We introduce the problem of constructing weighted complex projective 2-designs from the union of a family of orthonormal bases. If the weight remains constant across elements of the same basis, then such designs can be interpreted as generalizations of complete sets of mutually unbiased bases, being equivalent whenever the design is composed of  $d + 1$  bases in dimension  $d$ . We show that, for the purpose of quantum state determination, these designs specify an optimal collection of orthogonal measurements. Using highly nonlinear functions on abelian groups, we construct explicit examples from  $d + 2$  orthonormal bases whenever  $d + 1$  is a prime power, covering dimensions  $d = 6, 10$ , and  $12$ , for example, where no complete sets of mutually unbiased bases have thus far been found.

## 1. INTRODUCTION

Fundamental to the fabrication of quantum information processing devices [1], such as quantum teleporters, key distributors, cloners, gates, and indeed, quantum computers, is the ability to precisely determine an unknown quantum state. Quality assurance requires a complete characterization of these devices, which can be accomplished through knowledge of the output states for a judicious choice of input states.

The determination of an unknown state of a quantum system is achieved by a sequence of measurements on identically prepared copies of the system. If the outcome statistics for the measurements uniquely identify each member from the set of all quantum states, then an estimate of these statistics will reveal the particular state under examination. This process is called *quantum state tomography* [2].

One method of tomography is to perform identical measurements on each system copy; in this case, complete state determination requires that the outcome statistics for this single repeated measurement be described by an informationally complete positive-operator-valued measure (IC-POVM) [3, 4]. In the original tomographic paradigm [5, 6, 7, 8], however, the measurements differ: each one is orthogonal and prescribed by a member of an informationally complete set of quantum observables [9, 10, 11, 12]. The standard example for this latter scenario is provided by a complete set of mutually unbiased bases (MUBs) [13, 14]. That is, a maximal set of  $d + 1$  orthonormal bases,  $\{|e_j^a\rangle\}_{j=0}^{d-1} \subset \mathbb{C}^d$ ,  $a = 0, \dots, d$ , having a

---

\*Electronic address: aroy@qis.ucalgary.ca

†Electronic address: andrew.scott@griffith.edu.au

constant overlap of  $1/d$  between elements of different bases:

$$|\langle e_j^a | e_k^b \rangle|^2 = \begin{cases} \delta_{jk}, & a = b; \\ 1/d, & a \neq b. \end{cases} \quad (1.1)$$

In dimension 2, for example, the 3 bases correspond to “spin” measurements along the  $x$ ,  $y$ , and  $z$  axes of the Bloch sphere.

Explicit constructions of complete sets of MUBs are known for all prime-power dimensions  $d = p^n$  [13, 14, 15, 16, 17, 18, 19, 20, 21]. There is currently no supporting evidence, however, for their existence in other dimensions [22, 23, 24, 25, 26, 27]. Indeed, even in dimension 6, only sets of 3 MUBs have thus far been found [28, 29, 30], which falls well short of the 7 needed for the complete determination of a quantum state in this dimension. It is thus timely to search for alternative sets of bases that are also suitable for quantum state determination, but retain important properties of MUBs in this role.

In this article we investigate weighted complex projective 2-designs that are formed by the union of a family of orthonormal bases. General complex projective  $t$ -designs and their variants have recently attracted attention from the perspective of quantum information theory [3, 4, 31, 32, 33, 34, 35, 36, 37, 38, 39]. Within the context of quantum state determination, weighted 2-designs in  $\mathbb{C}P^{d-1}$  that are formed by the union of a family of orthonormal bases for  $\mathbb{C}^d$  can be interpreted as generalizations of complete sets of MUBs, provided that the weight remains constant across elements of the same basis. In such cases, they specify a series of orthogonal measurements whose outcome statistics are together described by a tight IC-POVM [4]. The smallest number of bases that can be used to construct a weighted 2-design in  $\mathbb{C}P^{d-1}$  is  $d + 1$ ; when exactly  $d + 1$  bases are used, these designs are equivalent to complete sets of MUBs. If an additional basis is allowed, however, we find that weighted 2-designs can be constructed from a family of  $d + 2$  orthonormal bases whenever  $d + 1$  is a prime power, covering dimensions  $d = 6, 10$ , and  $12$ , for example, where no complete sets of MUBs have thus far been found. Explicitly, in dimension 6, by appending the standard basis  $\{|e_j^0\rangle := |e_j\rangle\}_{j=0}^5$  to the 7 bases with elements

$$|e_j^a\rangle := \frac{1}{\sqrt{6}} \sum_{k=0}^5 e^{2\pi i j k / 6} e^{2\pi i a 3^k / 7} |e_k\rangle \quad (a = 1, \dots, 7), \quad (1.2)$$

we obtain a family of 8 orthonormal bases whose union forms a weighted complex projective 2-design. All members of the standard basis are appointed the weight  $w_0 = 1/42$ , while all members of the remaining bases are appointed the weight  $w_a = 1/49$ .

Most importantly, returning to the task of quantum state tomography, by measuring copies of a quantum system in the standard basis at a frequency ratio of  $7 : 6$  relative to each other basis, we retain the same minimal error rate in our estimate of the system state as that for a complete set of MUBs (if one were to be found). In fact, we show that families of orthonormal bases that form weighted complex projective 2-designs specify collections of orthogonal measurements which are (uniquely) optimal for quantum state tomography.

The article is organized as follows. In the next section we give a precise definition of a weighted  $t$ -design in  $\mathbb{C}P^{d-1}$ . In Sec. 3 we translate this notion to the class of  $t$ -designs formed by the union of a family of orthonormal bases, proving existence in every dimension, and then revealing equivalence to complete sets of MUBs in the special case of 2-designs constructed from  $d + 1$  bases. In Sec. 4 we present new constructions of weighted 2-designs

in terms of highly nonlinear functions on abelian groups. In fact, constructions using only  $O(d^2)$  bases are shown to be sufficient, which can be reduced to  $d + 1$  whenever  $d$  is a prime power (using a complete set of MUBs), or  $kd + 2$  whenever  $kd + 1$  is a prime power, for any positive integer  $k$ . We discuss weighted complex projective 2-designs in the role of state determination in Sec. 5, showing that such designs that are constructed from families of bases are optimal in this role in two specific scenarios: quantum state estimation as measurement-based cloning, and quantum state tomography by orthogonal measurements. Finally, in Sec. 6 we summarize our results.

## 2. WEIGHTED COMPLEX PROJECTIVE $t$ -DESIGNS

The extension of spherical  $t$ -designs [40] to projective spaces was first considered by Neumaier [41], but for the most part studied by Hoggar [42, 43, 44, 45], and, Bannai and Hoggar [46, 47]. For a unified treatment of designs in terms of metric spaces consult the work of Levenshtein [48, 49, 50] (see also Ref.'s [51, 52, 53, 54, 55, 56, 57, 58]). Our interest lies with the complex projective space  $\mathbb{C}P^{d-1}$  of lines passing through the origin in  $\mathbb{C}^d$ . In this case each  $x \in \mathbb{C}P^{d-1}$  may be represented by a unit vector  $|x\rangle \in \mathbb{C}^d$  (modulo a phase), or more appropriately, by the rank-one projector  $\pi(x) := |x\rangle\langle x|$ . We will use both representations in this article. Roughly speaking, a complex projective  $t$ -design is then a finite subset of  $\mathbb{C}P^{d-1}$  with the property that the discrete average of a polynomial of degree  $t$  or less over the design equals the uniform average. Many equivalent definitions can be made in these terms (see e.g. Ref.'s [41, 42, 48, 57, 58]). In the general context of compact metric spaces, for example, Levenshtein [49, 50] calls the pair  $(\mathcal{D}, w)$ , where  $\mathcal{D}$  a finite subset of  $\mathbb{C}P^{d-1}$  and  $w$  is positive-valued function on  $\mathcal{D}$  with the normalization  $\sum_{x \in \mathcal{D}} w(x) = 1$ , a *weighted  $t$ -design* if

$$\sum_{x, y \in \mathcal{D}} w(x)w(y)f(|\langle x|y\rangle|^2) = \iint_{\mathbb{C}P^{d-1}} d\mu(x)d\mu(y)f(|\langle x|y\rangle|^2) \quad (2.1)$$

for any real polynomial  $f$  of degree  $t$  or less, where  $\mu$  denotes the unique unitarily invariant probability measure on  $\mathbb{C}P^{d-1}$  induced by the Haar measure on  $U(d)$ . When  $w(x) = 1/|\mathcal{D}|$  we recover the more common notion of an “unweighted”  $t$ -design. In the current context, however, it is appropriate to consider the more general notion, and then make an alternative explicit definition which is specialized to complex projective spaces. With this in mind, let  $\Pi_{\text{sym}}^{(t)}$  denote the projector onto the totally symmetric subspace of  $(\mathbb{C}^d)^{\otimes t}$ , which has dimension  $\binom{d+t-1}{t}$ , and recall that

$$\int_{\mathbb{C}P^{d-1}} d\mu(x) \pi(x)^{\otimes t} = \binom{d+t-1}{t}^{-1} \Pi_{\text{sym}}^{(t)}. \quad (2.2)$$

Since the LHS is invariant under all unitaries  $U^{\otimes t}$ , which act irreducibly on the totally symmetric subspace of  $(\mathbb{C}^d)^{\otimes t}$ , Eq. (2.2) follows from a straightforward application of Schur’s Lemma. The following definition of a weighted  $t$ -design is now equivalent to the one given above (we will defer the proof until the end of this section).

A countable set  $\mathcal{S}$  endowed with a weight function  $w : \mathcal{S} \rightarrow (0, 1]$ , normalized such that  $\sum_{x \in \mathcal{S}} w(x) = 1$ , will be called a *weighted set* and denoted by the pair  $(\mathcal{S}, w)$ .

**Definition 2.1.** A finite weighted set  $(\mathcal{D}, w)$ ,  $\mathcal{D} \subset \mathbb{C}P^{d-1}$ , is called a *weighted  $t$ -design* (of dimension  $d$ ) if

$$\sum_{x \in \mathcal{D}} w(x) \pi(x)^{\otimes t} = \int_{\mathbb{C}P^{d-1}} d\mu(x) \pi(x)^{\otimes t} = \binom{d+t-1}{t}^{-1} \Pi_{\text{sym}}^{(t)}. \quad (2.3)$$

Seymour and Zaslavsky have shown that (unweighted)  $t$ -designs in  $\mathbb{C}P^{d-1}$  exist for any  $t$  and  $d$  [52]. Notice that the normalization of  $w$  is already implied by the trace of Eq. (2.3). If we instead “trace out” only one subsystem of these  $t$ -partite operators, we can immediately deduce that every weighted  $t$ -design is also a weighted  $(t-1)$ -design. A weighted 1-design is known as a *tight frame* in the context of frame theory [59], in which case the unnormalized states  $|\tilde{x}\rangle := \sqrt{w(x)d}|x\rangle$  are the frame vectors, and Eq. (2.3) is the tight frame condition:  $\sum_{x \in \mathcal{D}} |\tilde{x}\rangle\langle\tilde{x}| = I$ . In this form it is immediately apparent that we must have  $|\mathcal{D}| \geq d$  for a weighted 1-design, with equality only if the frame vectors  $|\tilde{x}\rangle$  form an orthonormal basis for  $\mathbb{C}^d$ , i.e.  $w(x) = 1/d = 1/|\mathcal{D}|$  and  $|\langle x|y\rangle|^2 = \delta(x, y)$  for all  $x, y \in \mathcal{D}$ . The 2-design case is treated in the following theorem (see e.g. Ref. [4, Theorem 4] for a proof).

**Theorem 2.2.** *Let  $(\mathcal{D}, w)$  be a weighted 2-design of dimension  $d$ . Then  $|\mathcal{D}| \geq d^2$  with equality only if  $w(x) = 1/|\mathcal{D}|$  and*

$$|\langle x|y\rangle|^2 = \frac{d\delta(x, y) + 1}{d + 1}, \quad (2.4)$$

for all  $x, y \in \mathcal{D}$ .

Within the context of quantum information theory, a set of  $d^2$  lines obeying Eq. (2.4) is called a *symmetric IC-POVM (SIC-POVM)* [3] (see also Ref.’s [21, 25, 28, 60, 61, 62, 63, 64, 65]). In general, the weighted complex projective 2-designs form a class of IC-POVMs which can be considered optimal in the role of state determination [4].

Theorem 2.2 is in fact a special case from known results within the theory of  $t$ -designs. In general, the number of design points must satisfy [42, 46, 48, 51]

$$|\mathcal{D}| \geq \binom{d + \lceil t/2 \rceil - 1}{\lceil t/2 \rceil} \binom{d + \lfloor t/2 \rfloor - 1}{\lfloor t/2 \rfloor}, \quad (2.5)$$

with equality only if the design has uniform weight [48], i.e.  $w(x) = 1/|\mathcal{D}|$ . A design which achieves this bound is called *tight*<sup>1</sup>. Tight  $t$ -designs in  $\mathbb{C}P^1$  are equivalent to tight spherical  $t$ -designs on the Euclidean 2-sphere. Such designs exist only for  $t = 1, 2, 3, 5$  (see e.g. Ref. [66]). When  $d \geq 3$  it is known that tight  $t$ -designs in  $\mathbb{C}P^{d-1}$  exist only for  $t = 1, 2, 3$  [44, 46, 47]. It is trivial that tight 1-designs exist in all dimensions. Tight 2-designs are conjectured to also exist in all dimensions [3, 31]. Analytical constructions, however, are known only for  $d \leq 10$  and  $d = 12, 13, 19$  [3, 28, 31, 60, 61, 67]. Tight 3-designs may exist only in even dimensions. Examples are known for  $d = 2, 4, 6$  [42]. Like in the specific 2-design case, more can be said about the structure of the tight  $t$ -designs. Given their rarity for higher values of  $t$ , however, we will defer further results in this direction to the work of Bannai and Hoggar [42, 43, 44, 45, 46, 47]. The task of finding  $t$ -designs is facilitated by the following theorem.

---

<sup>1</sup> The term “tight” is used differently in the contexts of frames and  $t$ -designs. A tight frame saturates the so-called frame bound [Eq. (2.6) with  $t = 1$ ] whereas a tight  $t$ -design saturates Eq. (2.5). Tight  $t$ -designs, being 1-designs, are tight frames, but the converse need not be true.

**Theorem 2.3.** For any finite weighted set  $(\mathcal{S}, w)$ ,  $\mathcal{S} \subset \mathbb{C}P^{d-1}$ , and any  $t \geq 1$ ,

$$\sum_{x,y \in \mathcal{S}} w(x)w(y) |\langle x|y \rangle|^{2t} \geq \binom{d+t-1}{t}^{-1}, \quad (2.6)$$

with equality if and only if  $(\mathcal{S}, w)$  is a weighted  $t$ -design.

*Proof.* Defining  $S := \sum_{x \in \mathcal{S}} w(x) \pi(x)^{\otimes t} - \binom{d+t-1}{t}^{-1} \Pi_{\text{sym}}^{(t)}$  we see that

$$0 \leq \text{tr}(S^\dagger S) = \sum_{x,y \in \mathcal{S}} w(x)w(y) |\langle x|y \rangle|^{2t} - \binom{d+t-1}{t}^{-1}, \quad (2.7)$$

with equality if and only if  $S = 0$ , which is the defining property of a  $t$ -design.  $\square$

This theorem allows us to check whether a weighted set of points in  $\mathbb{C}P^{d-1}$  forms a  $t$ -design by considering only the angles between the supposed design elements. It also shows that  $t$ -designs can be found numerically by parametrizing a weighted set and minimizing the LHS of Eq. (2.6). The lower bound is in fact a straightforward generalization of the Welch bound [68] (the above proof follows Ref. [57]). We conclude this section by presenting two common alternative definitions of complex projective  $t$ -designs. The first was given at the outset [Eq. (2.1)].

**Proposition 2.4.** A finite weighted set  $(\mathcal{D}, w)$ ,  $\mathcal{D} \subset \mathbb{C}P^{d-1}$ , is a weighted  $t$ -design if and only if

$$\sum_{x,y \in \mathcal{D}} w(x)w(y) f(|\langle x|y \rangle|^2) = \iint_{\mathbb{C}P^{d-1}} d\mu(x) d\mu(y) f(|\langle x|y \rangle|^2) \quad (2.8)$$

for all polynomials  $f$  of degree  $t$  or less.

*Proof.* Choosing the monomial  $f(u) = u^t$  in Eq. (2.8) and integrating the RHS we obtain equality in Eq. (2.6). Thus by Theorem 2.3, a finite weighted set  $(\mathcal{D}, w)$  satisfying Eq. (2.8) for  $f(u) = u^t$  is a  $t$ -design. The converse is just as simple. By squaring both sides of Eq. (2.3) and then taking the trace, we see that Eq. (2.8) is satisfied by the monomial  $f(u) = u^t$  when  $(\mathcal{D}, w)$  is a  $t$ -design. The same is true for any monomial of degree less than  $t$ , since a  $t$ -design is also a  $(t-1)$ -design, and thus by linearity, any polynomial of degree  $t$  or less.  $\square$

Let  $\{|e_j\rangle\}_{j=0}^{d-1}$  be the “standard” basis for  $\mathbb{C}^d$ . Define  $\text{Hom}(t, t)$  to be the set of polynomials which are homogeneous of degree  $t$  in the coordinates  $\langle e_j|x \rangle = x_j$  on the unit sphere in  $\mathbb{C}^d$ , and also homogeneous of degree  $t$  in the conjugates of these coordinates,  $\langle x|e_j \rangle = \bar{x}_j$ . For example,  $f(x) = \langle e_0|x \rangle \langle x|e_1 \rangle = x_0 \bar{x}_1$  is in  $\text{Hom}(1, 1)$ .

**Proposition 2.5.** A finite weighted set  $(\mathcal{D}, w)$ ,  $\mathcal{D} \subset \mathbb{C}P^{d-1}$ , is a weighted  $t$ -design if and only if

$$\sum_{x \in \mathcal{D}} w(x) f(x) = \int_{\mathbb{C}P^{d-1}} d\mu(x) f(x) \quad (2.9)$$

for all polynomials  $f \in \text{Hom}(t, t)$ .

*Proof.* Simply note that Eq. (2.9) for each monomial  $f \in \text{Hom}(t, t)$  is given by a matrix component of Eq. (2.3) in the standard basis. The monomials form a basis for  $\text{Hom}(t, t)$ .  $\square$

### 3. WEIGHTED $t$ -DESIGNS FROM BASES

We now address the problem of constructing weighted 2-designs in  $\mathbb{C}P^{d-1}$  from the union of a family of orthonormal bases for  $\mathbb{C}^d$ . If the weight remains constant across elements of the same basis then such designs correspond to tight IC-POVMs [4] which can be realized by a sequence of orthogonal measurements. We will thus make this a requirement.

To be precise, in the general case we seek a family of sets  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1} \subset \mathbb{C}P^{d-1}$ , each specified by an orthonormal basis for  $\mathbb{C}^d$ , i.e.  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$  where  $\langle e_j^a | e_k^a \rangle = \delta_{jk}$ , and appointed a positive weight  $w_a$ , such that their union  $\mathcal{D} = \cup_a \mathcal{B}_a$  forms a weighted  $t$ -design with the weight function  $w(x) = \sum_a w_a 1_{\mathcal{B}_a}(x)$ . The set indicator function,  $1_A(x) := 1$  if  $x \in A$  and 0 otherwise, takes care of any multiplicity in elements across different bases. Notice that the normalization of  $w(x)$  implies normalization of the basis weights:  $\sum_a w_a = 1/d$ . Although we in fact have  $\mathcal{B}_a \subset \mathbb{C}P^{d-1}$ , we will refer to  $\mathcal{B}_a$  as an ‘‘orthonormal basis for  $\mathbb{C}^d$ ,’’ and then the line  $e_j^a \in \mathbb{C}P^{d-1}$  as the  $j$ -th element of the  $a$ -th basis. Revisiting Eq. (2.3) shows that we require

$$\sum_{a=0}^{m-1} w_a \sum_{j=0}^{d-1} \pi(e_j^a)^{\otimes t} = \int_{\mathbb{C}P^{d-1}} d\mu(x) \pi(x)^{\otimes t} = \binom{d+t-1}{t}^{-1} \Pi_{\text{sym}}^{(t)}, \quad (3.1)$$

or equivalently, by Theorem 2.3,

$$\sum_{a,b=0}^{m-1} w_a w_b \sum_{j,k=0}^{d-1} |\langle e_j^a | e_k^b \rangle|^{2t} = \binom{d+t-1}{t}^{-1}. \quad (3.2)$$

Seymour and Zaslavsky [52] have given a non-constructive proof that (unweighted)  $t$ -designs exist in every dimension. Their main result is quite general, and also applies to weighted  $t$ -designs constructed from bases:

**Theorem 3.1.** *Let  $\Omega$  be a path-connected topological space endowed with a measure  $\omega$  that is finite and positive with full support, and, let  $f : \Omega \rightarrow \mathbb{R}^n$  be a continuous, integrable function. Then there exists a finite set  $\mathcal{X} \subseteq \Omega$  such that*

$$\frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} f(x) = \frac{1}{\omega(\Omega)} \int_{\Omega} d\omega(x) f(x). \quad (3.3)$$

The size of  $\mathcal{X}$  may be any number, with a finite number of exceptions.

**Corollary 3.2.** *For each pair of positive integers  $t$  and  $d$ , and for all sufficiently large  $m$ , there exist weighted  $t$ -designs for  $\mathbb{C}P^{d-1}$  which are formed by taking the union of  $m$  orthonormal bases for  $\mathbb{C}^d$  (as described above).*

*Proof.* Let  $\Omega = \text{U}(d)$  and  $\omega = \mu$ , the Haar measure with  $\mu(\text{U}(d)) = 1$ . Applying Theorem 3.1 to

$$f(U) := \frac{1}{d} \sum_j [U\pi(e_j)U^\dagger]^{\otimes t}, \quad (3.4)$$

which maps  $\text{U}(d)$  into  $\text{End}(\mathbb{C}^d)^{\otimes t} \cong \mathbb{R}^n$ , where  $n = 2d^{2t}$  and  $\{e_j\}_{j=0}^{d-1}$  is the standard basis, we know that for all sufficiently large  $m$  there exist sets  $\mathcal{X} = \{U_a\}_{a=0}^{m-1} \subset \text{U}(d)$  with the

property that [Eq. (3.3)]

$$\frac{1}{md} \sum_{a,j} [U_a \pi(e_j) U_a^\dagger]^{\otimes t} = \frac{1}{d} \sum_j \int_{U(d)} d\mu(U) [U \pi(e_j) U^\dagger]^{\otimes t} \quad (3.5)$$

$$= \binom{d+t-1}{t}^{-1} \Pi_{\text{sym}}^{(t)}, \quad (3.6)$$

using Schur's Lemma for the integral. Now setting  $|e_j^a\rangle = U_a |e_j\rangle$  we have our desired result, i.e. Eq. (3.1) with  $w_a = 1/md$ .  $\square$

Our proof of Corollary 3.2 in fact shows that weighted  $t$ -designs formed by the unweighted union of orthonormal bases exist in all dimensions, i.e. we can take  $w_a = 1/md$ . An example of a family of bases with this property is a *complete set of mutually unbiased bases* [13, 14] (see also Ref.'s [15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33]). Two orthonormal bases,  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$  and  $\mathcal{B}_b = \{e_k^b\}_{k=0}^{d-1}$ , are called *mutually unbiased* if

$$|\langle e_j^a | e_k^b \rangle|^2 = \frac{1}{d} \quad (3.7)$$

for all  $0 \leq j, k \leq d-1$ . A *complete set of mutually unbiased bases* (MUBs) is a set of  $m = d+1$  orthonormal bases with the property that each pair are mutually unbiased. This is the maximum possible number. Such sets are known to exist whenever  $d$  is a prime power, but no other examples have been found. It is straightforward to confirm [via Eq. (3.2)] that a complete set of MUBs will form a 2-design when  $w_a = 1/md$  [32, 33]. Our next result (which can be regarded as the analogue of Theorem 2.2 for the current case) shows that such sets are optimal, in that we always need  $m \geq d+1$  bases to construct a weighted 2-design, with equality only if the bases are mutually unbiased.

**Theorem 3.3.** *Let  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1} \subset \mathbb{C}P^{d-1}$  be a family of orthonormal bases for  $\mathbb{C}^d$  whose union  $\mathcal{D} = \cup_a \mathcal{B}_a$  forms a weighted 2-design with weight function  $w(x) = \sum_a w_a 1_{\mathcal{B}_a}(x)$  for some choice of the positive constants  $w_0, \dots, w_{m-1}$ . Then  $m \geq d+1$  with equality only if  $w_a = 1/md$  for all  $a$  and the bases are pairwise mutually unbiased.*

*Proof.* Theorem 2.2 with  $|\mathcal{D}| = md$  immediately shows that we must have  $m \geq d$ , but since Eq. (2.4) can not be satisfied by a family of orthonormal bases, we in fact need  $m \geq d+1$ . In the case of equality, note that by Theorem 2.3 we require [Eq. (3.2) with  $t=2$ ]

$$d \sum_a w_a^2 + \sum_{a \neq b} w_a w_b \sum_{j,k} \lambda_{jk}^2 = \binom{d+1}{2}^{-1}, \quad (3.8)$$

where we have defined the positive numbers  $\lambda_{jk} := |\langle e_j^a | e_k^b \rangle|^2$ . Moreover, Theorem 2.3 implies that the LHS of Eq. (3.8) is minimal with respect to the variables  $w_a$  and  $\lambda_{jk}$  under the appropriate constraints, two of which are  $\sum_a w_a = 1/d$  and

$$\sum_{j,k} \lambda_{jk} = \sum_{j,k} |\langle e_j^a | e_k^b \rangle|^2 = \text{tr}(I \cdot I) = d. \quad (3.9)$$

We will now minimize the LHS of Eq. (3.8) under these two constraints. The minimum of  $\sum_{j,k} \lambda_{jk}^2$  subject to Eq. (3.9) occurs only when  $\lambda_{jk} = 1/d$  for all  $0 \leq j, k \leq d-1$ , i.e., when  $\mathcal{B}_a$  and  $\mathcal{B}_b$  are mutually unbiased. Then the LHS of Eq. (3.8) reduces to

$$d \sum_a w_a^2 + \sum_{a \neq b} w_a w_b = (d-1) \sum_a w_a^2 + \frac{1}{d^2}, \quad (3.10)$$

and here the minimum (under  $\sum_a w_a = 1/d$ ) occurs only when  $w_a = 1/md$  for all  $0 \leq a \leq m-1$ . With this value, Eq. (3.10) reduces to the RHS of Eq. (3.8) when  $m = d+1$ . Equality in Eq. (3.8) thus requires the bases to be pairwise mutually unbiased and  $w_a = 1/md$  whenever  $m = d+1$ .  $\square$

In general, for each positive integer  $t$  and  $d$ , we would like to know the quantity  $M(t, d)$ , which we use to denote the minimum number of orthonormal bases needed to construct a weighted  $t$ -design in  $\mathbb{C}P^{d-1}$ , or less ambitiously, bounds on this quantity. Trivially,  $M(1, d) = M(t, 1) = 1$ . Theorem 3.3 shows that  $M(2, d) \geq d+1$ , with equality when  $d$  is a prime power. This theorem also shows that knowledge of  $M(2, d)$  in general would solve the MUBs problem, i.e., imply the existence (or most likely, nonexistence) of complete sets of MUBs in dimensions which are not prime powers. As we remarked earlier, no such examples have been found. For the first exceptional dimension however,  $d = 6$ , a tight 3-design exists which is formed from the unweighted ( $w_a = 1/md$ ) union of  $m = 21$  bases. We thus know that  $7 \leq M(2, 6) \leq M(3, 6) = 21$  (In fact  $M(3, d) = d(d+1)/2$  when  $d = 2, 4, 6$ , the dimensions of the only known tight 3-designs). However, in the next section we show that, quite remarkably,  $M(2, 6) \leq 8$ , and moreover,  $M(2, d) \leq d+2$  whenever  $d+1$  is a prime power.

#### 4. WEIGHTED 2-DESIGNS FROM BASES: CONSTRUCTIONS

In this section we give analytic constructions of weighted 2-designs using “highly nonlinear functions” on abelian groups. Nonlinear functions on finite fields have been studied extensively in the context of classical cryptography, and several authors [69, 70, 71, 72] have extended those concepts to arbitrary finite abelian groups. Here we work with a class of functions called differentially 1-uniform, so named for their resistance to differential cryptanalysis [73].

Let  $G$  and  $H$  be abelian groups with  $|G| \leq |H| < \infty$ , let  $f$  be a function from  $G$  to  $H$ , and consider the number of solutions in  $x$  to the equation

$$f(x+a) - f(x) = b. \quad (4.1)$$

If  $(a, b) = (0, 0)$  then Eq. (4.1) has  $|G|$  solutions. There are also  $|G|$  solutions whenever  $f$  is linear or affine and  $b = f(a)$ . A function is therefore highly nonlinear if Eq. (4.1) has as few solutions as possible for any choice of  $a$  and  $b$ . Of course we cannot avoid all solutions: letting  $b = f(x+a) - f(x)$  for any fixed  $x$  and  $a$  gives at least one solution. The function  $f$  is called *differentially 1-uniform*, or simply *1-uniform*, if for every  $(a, b) \neq (0, 0)$ , Eq. (4.1) has at most one solution [69].

By way of example, let  $\mathbb{Z}_n$  denote the cyclic abelian group of order  $n$  and define  $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_6$  through the following table.

$$\begin{array}{c|cccc} x & 0 & 1 & 2 & 3 & 4 \\ \hline f(x) & 0 & 1 & 0 & 2 & 2 \end{array}$$

It is straightforward to verify that  $f$  is differentially 1-uniform.

In constructing weighted 2-designs we will need the following characterization.

**Lemma 4.1.** *Let  $G$  and  $H$  be abelian groups. Then the function  $f : G \rightarrow H$  is differentially 1-uniform if and only if the equation*

$$(w, f(w)) + (x, f(x)) = (y, f(y)) + (z, f(z)) \quad (4.2)$$

has exactly  $|G|(2|G| - 1)$  solutions in  $(w, x, y, z)$ .

*Proof.* Let  $d = |G|$  and note that Eq. (4.2) has  $d(2d - 1)$  trivial solutions, namely  $d$  solutions of the form  $(w, x, y, z) = (w, w, w, w)$  and  $2(d^2 - d)$  solutions of the form  $(w, x, y, z) = (w, x, w, x)$  or  $(w, x, y, z) = (w, x, x, w)$  for  $x \neq w$ . Now rewriting Eq. (4.2) in the form

$$(w, f(w)) - (z, f(z)) = (y, f(y)) - (x, f(x)) = (a, b), \quad (4.3)$$

for some  $a$  and  $b$ , we see that  $f$  is 1-uniform if and only if the solutions all satisfy  $w = z$  or  $w = y$ . That is,  $f$  is 1-uniform if and only if the only solutions are the trivial ones.  $\square$

We now come to our main construction.

**Theorem 4.2.** *Suppose there is a differentially 1-uniform function  $f : G \rightarrow H$  for the abelian groups  $G$  and  $H$ . Then there exists a weighted 2-design in  $\mathbb{C}P^{|G|-1}$  which is formed from the union of  $|H| + 1$  orthonormal bases for  $\mathbb{C}^{|G|}$ .*

Setting  $d = |G|$  and  $m = |H| + 1$ , it follows that  $M(2, d) \leq m$  whenever there exists a function  $f : G \rightarrow H$  which is differentially 1-uniform. The designs that Theorem 4.2 refers to are constructed as follows. We first assign the weight

$$w_0 = \frac{1}{d(d+1)} \quad (4.4)$$

to  $\mathcal{B}_0 := \{e_j\}_{j=0}^{d-1}$ , which is the standard basis for  $\mathbb{C}^d$ . All  $m - 1$  remaining bases are appointed the weight

$$w_a = \frac{1}{(m-1)(d+1)} \quad (a > 0), \quad (4.5)$$

and then defined in terms of the characters of  $G$  and  $H$ . For a review of characters of finite abelian groups, consult Ref. [74]. Now for each  $j \in G$ , let  $\chi_j$  be the  $j$ -th character of  $G$ , and similarly for each  $a \in H$ , let  $\psi_a$  be the  $a$ -th character of  $H$ . The  $j$ -th element of basis  $\mathcal{B}_a$  is then

$$|e_j^a\rangle := \frac{1}{\sqrt{d}} \sum_{x \in G} \chi_j(x) \psi_a(f(x)) |e_x\rangle \quad (a > 0), \quad (4.6)$$

using  $0, \dots, d - 1$  to denote the elements of  $G$ , but  $1, \dots, m - 1$  to denote the elements of  $H$  (with  $m - 1$  now the additive identity), and the index 0 always reserved for the standard basis in the latter context. The requirement  $\langle e_j^a | e_k^a \rangle = \delta_{jk}$  now follows from the orthogonality of characters.

*Proof of Theorem 4.2.* Let  $d = |G|$  and  $m = |H| + 1$ . By Theorem 2.3, it suffices to show that

$$\sum_{a, b \in H \cup \{0\}} \omega_a \omega_b \sum_{j, k \in G} |\langle e_j^a | e_k^b \rangle|^4 = \frac{2}{d(d+1)} \quad (4.7)$$

for the above weights [Eq.'s (4.4) and (4.5)], and with  $\mathcal{B}_a$  given by the standard basis when  $a = 0$ , i.e.  $|e_j^0\rangle = |e_j\rangle$ , or defined by Eq. (4.6) otherwise.

When  $a = b = 0$ , we have  $|\langle e_j^0 | e_k^0 \rangle|^4 = |\langle e_j | e_k \rangle|^4 = \delta_{jk}$ . These terms contribute a total of

$$\omega_0^2 \sum_{j, k \in G} |\langle e_j^0 | e_k^0 \rangle|^4 = \frac{1}{d^2(d+1)^2} \sum_{j, k \in G} \delta_{jk} = \frac{1}{d(d+1)^2} \quad (4.8)$$

to the LHS of Eq. (4.7). When  $a = 0$  and  $b \in H$ , we have  $|\langle e_j^0 | e_k^b \rangle|^4 = |\langle e_j | e_k^b \rangle|^4 = 1/d^2$ , and likewise for  $a \in H$  and  $b = 0$ , adding a total of

$$2 \sum_{b \in H} \omega_0 \omega_b \sum_{j, k \in G} |\langle e_j^0 | e_k^b \rangle|^4 = 2 \sum_{b \in H} \frac{1}{d(m-1)(d+1)^2} \sum_{j, k \in G} \frac{1}{d^2} = \frac{2}{d(d+1)^2} \quad (4.9)$$

to the sum.

For the remainder, we must evaluate  $|\langle e_j^a | e_k^b \rangle|^4$  for  $a, b \in H$ . First note that

$$\langle e_j^a | e_k^b \rangle = \frac{1}{d} \sum_{x \in G} \overline{\chi_j(x) \psi_a(f(x))} \chi_k(x) \psi_b(f(x)) \quad (4.10)$$

$$= \frac{1}{d} \sum_{x \in G} \chi_{k-j}(x) \psi_{b-a}(f(x)), \quad (4.11)$$

since the product of two characters, or the complex conjugate of a character, is another character. Multiplying by the conjugate, it follows that

$$d^4 |\langle e_j^a | e_k^b \rangle|^4 = \left( \sum_{x \in G} \chi_{k-j}(x) \psi_{b-a}(f(x)) \right)^2 \left( \sum_{y \in G} \overline{\chi_{k-j}(y) \psi_{b-a}(f(y))} \right)^2 \quad (4.12)$$

$$= \sum_{w, x, y, z \in G} \chi_{k-j}(w+x-y-z) \psi_{b-a}(f(w)+f(x)-f(y)-f(z)). \quad (4.13)$$

Now taking the sum over  $k \in G$  and  $b \in H$ , every character of  $G$  and  $H$  occurs once:

$$d^4 \sum_{\substack{k \in G \\ b \in H}} |\langle e_j^a | e_k^b \rangle|^4 = \sum_{\substack{k \in G \\ b \in H}} \sum_{w, x, y, z \in G} \chi_k(w+x-y-z) \psi_b(f(w)+f(x)-f(y)-f(z)) \quad (4.14)$$

$$= \sum_{w, x, y, z \in G} \sum_{\substack{k \in G \\ b \in H}} \chi_{w+x-y-z}(k) \psi_{f(w)+f(x)-f(y)-f(z)}(b) \quad (4.15)$$

$$= d^2(m-1)(2d-1). \quad (4.16)$$

The last step is explained as follows. The inner summation in the RHS of Eq. (4.15) is zero unless both of the characters  $\chi_{w+x-y-z}$  and  $\psi_{f(w)+f(x)-f(y)-f(z)}$  are trivial, in which case the sum is  $|G| \cdot |H| = d(m-1)$ . But the characters are trivial exactly when  $w+x=y+z$  and  $f(w)+f(x)=f(y)+f(z)$ . By Lemma 4.1, this occurs exactly  $d(2d-1)$  times if and only if  $f$  is 1-uniform. Thus Eq. (4.15) reduces to Eq. (4.16). It follows that the total contribution to Eq. (4.7) of terms with  $a, b \in H$  is

$$\sum_{a, b \in H} \omega_a \omega_b \sum_{j, k \in G} |\langle e_j^a | e_k^b \rangle|^4 = \frac{1}{(m-1)^2(d+1)^2} \sum_{\substack{j \in G \\ a \in H}} \sum_{\substack{k \in G \\ b \in H}} |\langle e_j^a | e_k^b \rangle|^4 \quad (4.17)$$

$$= \frac{1}{(m-1)^2(d+1)^2} \sum_{\substack{j \in G \\ a \in H}} \frac{(m-1)(2d-1)}{d^2} \quad (4.18)$$

$$= \frac{2d-1}{d(d+1)^2}. \quad (4.19)$$

Finally, adding up all contributions [Eq.'s (4.8), (4.9) and (4.19)], we find that Eq. (4.7) is satisfied, and so the union of the given bases forms a weighted 2-design.  $\square$

We now turn to the problem of constructing differentially 1-uniform functions. When  $f : G \rightarrow H$  is 1-uniform, we always have  $|G| \leq |H|$ ; in terms of minimizing the number of bases in a 2-design, the goal is to minimize  $|H|$ . If  $|H| = |G| = d$ , then Theorem 4.2 produces a complete set of MUBs. Differentially 1-uniform functions  $f : G \rightarrow G$  are also called *perfect nonlinear* [71] or *maximally nonlinear* [72], and they are known to exist whenever  $d$  is an odd prime power. In particular, let  $\mathbb{F}_d$  be the finite field of order  $d = p^n$ . Then the function  $f : \mathbb{F}_d \rightarrow \mathbb{F}_d$  is 1-uniform in the following cases [75]:

1.  $f(x) = x^2$  ;
2.  $f(x) = x^{p^{k+1}}$ ,  $n/\gcd(n, k)$  odd ;
3.  $f(x) = x^{\frac{3^k+1}{2}}$ ,  $p = 3$ ,  $k$  odd,  $\gcd(n, k) = 1$  ;
4.  $f(x) = x^{10} - ux^6 - u^2x^2$ ,  $p = 3$ ,  $n$  odd,  $u \in \mathbb{F}_d^*$ ,

where  $\mathbb{F}_d^*$  is the multiplicative group of  $\mathbb{F}_d$ . The first example reproduces the MUBs of Ivanović [13] and Wootters and Fields [14].

When  $d$  is an even prime power,  $d = 2^n$  say, there are no 1-uniform functions from  $\mathbb{F}_d$  to  $\mathbb{F}_d$ . This is because in a field of characteristic 2, solutions to the equation  $f(x+a) - f(x) = b$  come in pairs  $\{x, x+a\}$ . However, there are 1-uniform functions from  $\mathbb{F}_d$  to  $GR(4^n)$ , the Galois ring of order  $d^2$ . For background on Galois rings, see Ref.'s [76] or [77]. Let  $\mathcal{T}$  be the Teichmüller set of  $GR(4^n)$ , and for each  $x \in \mathbb{F}_d$  let  $\hat{x}$  be the unique element of  $\mathcal{T}$  such that  $x \equiv \hat{x} \pmod{2}$ . Then  $f(x) = \hat{x}$  is 1-uniform [77], and so there is a 2-design formed from the union of  $d^2 + 1$  bases for  $\mathbb{C}^d$ . In fact, all of the bases in this construction (except the standard basis) are repeated  $d$  times, which amounts to giving each distinct basis a larger weight. The result is the complete set of  $d + 1$  MUBs described by Klappenecker and Rötteler [18].

When  $d$  is not a prime power, numerical evidence suggests that no complete set of MUBs exists. If this is true, then  $M(2, d) \geq d + 2$  for those values of  $d$ . The following construction shows that  $M(2, d) \leq d + 2$  whenever  $d + 1$  is a prime power.

**Proposition 4.3.** *Let  $d + 1$  be a prime power, and let  $y$  be a generator for  $\mathbb{F}_{d+1}^*$ . Then the function  $f : \mathbb{Z}_d \rightarrow \mathbb{F}_{d+1}$  defined by*

$$f(j) := y^j \tag{4.20}$$

*is differentially 1-uniform.*

*Proof.* Suppose Eq. (4.1) has two solutions for some  $a$  and  $b$ , say

$$y^{j+a} - y^j = y^{k+a} - y^k . \tag{4.21}$$

Factoring, we have

$$(y^j - y^k)(y^a - 1) = 0 , \tag{4.22}$$

which implies that either  $a = 0$  or  $j = k$ . So for  $(a, b) \neq (0, 0)$ , Eq. (4.1) has at most one solution.  $\square$

The weighted 2-designs resulting from Proposition 4.3 are explicitly constructed according to Eq. (4.6) as follows. For  $j \in \mathbb{Z}_d$ , the  $j$ -th character of the group  $\mathbb{Z}_d$  is  $\chi_j(k) := e^{2\pi ijk/d}$ ; for  $a \in \mathbb{F}_{d+1}$ , the  $a$ -th character of  $\mathbb{F}_{d+1}$  is  $\psi_a(x) := e^{2\pi i \text{tr}(ax)/p}$ , where  $d+1 = p^n$  ( $p$  prime) and  $\text{tr } x := x + x^p + \cdots + x^{p^{n-1}}$  is the trace function from  $\mathbb{F}_{d+1}$  to  $\mathbb{F}_p$ . Thus if  $y$  is a primitive element of  $\mathbb{F}_{d+1}$ , then the  $j$ -th vector of basis  $\mathcal{B}_a$  is

$$|e_j^a\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi ijk/d} e^{2\pi i \text{tr}(ay^k)/p} |e_k\rangle. \quad (4.23)$$

It remains to consider upper bounds on  $M(2, d)$  when neither  $d$  nor  $d+1$  is a prime power. In these cases, the following proposition shows that  $M(2, d) \leq kd+2$ , where  $k$  is the smallest positive number such that  $kd+1$  is a prime power. The proof of Proposition 4.4 is the same as that of Proposition 4.3.

**Proposition 4.4.** *Let  $kd+1$  be a prime power, and let  $y$  be an element of multiplicative order  $d$  in  $\mathbb{F}_{kd+1}$ . Then  $f(j) := y^j$  is a differentially 1-uniform function from  $\mathbb{Z}_d$  to  $\mathbb{F}_{kd+1}$ .*

The following table summarizes the resulting best known upper bound on  $M(2, d)$  for dimension  $d \leq 50$ :

$d$	$p^n$	$p^n - 1$	14	20	21	33	34	35	38	39	44	45	50
$M(2, d) \leq$	$d+1$	$d+2$	30	42	44	68	104	72	192	80	90	182	102

A numerical search in dimension  $d = 14$  was unable to locate an example of a weighted 2-design composed of  $m < 30$  orthonormal bases. The method used, however, which is an optimization procedure based on Theorem 2.3, is quite slow for such a large value of  $d$  and should not be trusted.

In general, the upper limit for  $M(2, d)$  obtained from Proposition 4.4 is far from the lower bound of  $d+1$ . Linnik's theorem [78] gives an upper bound on the size of the smallest prime that occurs in the arithmetic progression  $(kd+1)_{k=1}^\infty$ : it implies that  $M(2, d)$  is  $O(d^L)$ , for some constant  $L$ . Heath-Brown [79] has shown that  $L \leq 5.5$ . However, the next construction shows that  $M(2, d)$  is  $O(d^2)$ .

**Proposition 4.5.** *Let  $f : \mathbb{Z}_d \rightarrow \mathbb{Z}_n$  be the function  $f(j) := \binom{j}{2}$ , for  $0 \leq j \leq d-1$ . If  $d > 2$  and  $n \geq \frac{3}{4}(d-1)^2$ , then  $f$  is differentially 1-uniform.*

*Proof.* We work over the integers: let  $\hat{f} : \mathbb{Z}_d \rightarrow \mathbb{Z}$  be the function that maps  $j$  to  $\binom{j}{2}$ , for  $0 \leq j \leq d-1$ . It then suffices to show that for every  $a \in \{1, \dots, d-1\}$  and  $b \in \{0, \dots, n-1\}$ , the equation

$$\hat{f}(j+a) - \hat{f}(j) \equiv b \pmod{n} \quad (4.24)$$

has at most one solution. Fix  $a \in \{1, \dots, d-1\}$ , and consider the differences

$$\hat{f}(j+a) - \hat{f}(j) = \begin{cases} \binom{j+a}{2} - \binom{j}{2}, & j+a \leq d-1; \\ \binom{j+a-d}{2} - \binom{j}{2}, & j+a \geq d. \end{cases} \quad (4.25)$$

First examine the cases in which  $j+a \leq d-1$ . For these values of  $j$ , the differences  $\binom{j+a}{2} - \binom{j}{2}$  are all distinct mod  $n$ . For, if  $\binom{j+a}{2} - \binom{j}{2} \equiv \binom{k+a}{2} - \binom{k}{2} \pmod{n}$ , then simplifying we find that

$$a(j-k) \equiv 0 \pmod{n}, \quad (4.26)$$

which holds only if  $j = k$ , since  $|a(j - k)| \leq a(d - 1 - a) \leq \frac{1}{4}(d - 1)^2 < n$  whenever  $n \geq \frac{3}{4}(d - 1)^2$  and  $0 \leq j, k \leq d - 1 - a$ . Similarly, the differences for which  $j + a \geq d$  are also distinct mod  $n$  for distinct values of  $j$ .

We now show that no difference with  $j + a \leq d - 1$  has the same value mod  $n$  as a difference with  $j + a \geq d$ . The largest value of the former occurs when  $j + a = d - 1$ , and the smallest of the latter occurs when  $j = d - 1$ . So we require

$$n > \left[ \binom{d-1}{2} - \binom{d-a-1}{2} \right] - \left[ \binom{a-1}{2} - \binom{d-1}{2} \right], \quad (4.27)$$

which simplifies to

$$n > da - a^2 + \frac{d^2 - 3d}{2}. \quad (4.28)$$

The largest value of the RHS of Eq. (4.28) occurs at  $a = \lfloor d/2 \rfloor$ , which means the inequality is satisfied for all  $a$  whenever  $n \geq \frac{3}{4}(d-1)^2$ . Finally, the smallest difference with  $j+a \leq d-1$  needs to be greater than the largest difference with  $j+a \geq d$ , i.e.  $\binom{a}{2} - \binom{0}{2} > \binom{0}{2} - \binom{d-a}{2}$ , which is satisfied for all  $a$  whenever  $d > 2$ .  $\square$

It is also of some mathematical interest to construct weighted 2-designs in  $\mathbb{C}P^{d-1}$  which are the union of  $m$  orthonormal bases for  $m$  larger than the minimum  $M(2, d)$ . While these constructions are not so important in the context of quantum state tomography, they may be of use in other applications of designs. Moreover, insight into the general structure of such designs may eventually lead to improved bounds for  $M(2, d)$ . Numerically, it becomes easier to find designs with  $m$  bases as  $m$  increases, and Corollary 3.2 and Proposition 4.5 indicate that such designs will always exist for sufficiently large  $m$ . We now use differentially 1-uniform functions to more precisely quantify ‘‘sufficiently large  $m$ ’’ for certain values of  $d$ .

There is very little literature on highly nonlinear functions  $f : G \rightarrow H$  with  $|G| < |H|$ , as cryptographers have focused on the case  $|G| \geq |H|$ . Nevertheless, 1-uniform functions become easier to find as  $|H|$  increases. In fact, for fixed  $G$ , a random function  $f : G \rightarrow H$  is asymptotically almost surely 1-uniform as  $|H| \rightarrow \infty$ . There are also many recursive constructions. For example: if  $f_1 : G \rightarrow H_1$  is any function and  $f_2 : G \rightarrow H_2$  is 1-uniform, then the function  $f_1 + f_2 : G \rightarrow H_1 \times H_2$  defined by

$$(f_1 + f_2)(x) := (f_1(x), f_2(x)) \quad (4.29)$$

is also 1-uniform. Embedding the codomain of a 1-uniform function into a larger group serves as a general strategy for constructing designs with many bases.

**Lemma 4.6.** *Let  $E : \mathbb{Z}_k \rightarrow \mathbb{Z}_n$  be the function that maps  $(i \bmod k)$  to  $(i \bmod n)$ , for  $0 \leq i \leq k-1$ . If  $f : G \rightarrow \mathbb{Z}_k$  is differentially 1-uniform and  $n \geq 2k-1$ , then  $E \circ f : G \rightarrow \mathbb{Z}_n$  is also differentially 1-uniform.*

*Proof.* We again work over the integers. Let  $\hat{f} : G \rightarrow \mathbb{Z}$  be the function that maps  $x$  to the unique integer  $\hat{f}(x) \in \{0, \dots, k-1\}$  such that  $f(x) \equiv \hat{f}(x) \pmod{k}$ . Since  $f$  is 1-uniform, it follows that for fixed  $a \neq 0$  and  $b \in \mathbb{Z}$ ,

$$\hat{f}(x+a) - \hat{f}(x) = b \quad (4.30)$$

has at most one solution. Moreover, since  $\hat{f}(x)$  is in the range  $[0, k-1]$ , it is clear that  $\hat{f}(x+a) - \hat{f}(x)$  is in  $[-k+1, k-1]$ , a range of size  $2k-2$ . But  $n > 2k-2$ , so it follows that  $\hat{f}(x+a) - \hat{f}(x) = b$  has at most one solution mod  $n$ . Thus  $E \circ f$  is 1-uniform as a function from  $G$  to  $\mathbb{Z}_n$ .  $\square$

The proof of Lemma 4.6 also demonstrates that any cyclic subgroup in the codomain of a 1-uniform function can be embedded into a larger group. More precisely, suppose that  $f_1 : G \rightarrow H_1$  and  $f_2 : G \rightarrow \mathbb{Z}_k$  are functions such that  $f_1 + f_2$  is 1-uniform from  $G$  to  $H_1 \times \mathbb{Z}_k$ . Then for any  $n \geq 2k - 1$ , the function  $f_1 + (E \circ f_2)$  is 1-uniform from  $G$  to  $H_1 \times \mathbb{Z}_n$ . But every group has some cyclic subgroup, so: if  $f : G \rightarrow H$  is 1-uniform, then for every  $n \geq 2|H| - 1$ , there a 1-uniform function  $g : G \rightarrow H'$  such that  $H'$  is a group of order  $n$ .

**Corollary 4.7.** *If  $f : G \rightarrow H$  is differentially 1-uniform, then for every  $m \geq 2|H|$  there is weighted 2-design in  $\mathbb{C}P^{|G|-1}$  which is formed from the union of  $m$  orthonormal bases for  $\mathbb{C}^{|G|}$ .*

Considering cyclic subgroups  $\mathbb{Z}_p$  in the codomains of perfect nonlinear functions or the 1-uniform functions in Proposition 4.3 yields the following.

**Corollary 4.8.** *Suppose  $d = p^n$  with  $p$  an odd prime, or  $d + 1 = p^n$  with  $p$  any prime. Then for every  $m \geq d + p + 1$ , there is a weighted 2-design in  $\mathbb{C}P^{d-1}$  which is formed from the union of  $m$  orthonormal bases for  $\mathbb{C}^d$ .*

## 5. WEIGHTED 2-DESIGNS AS INFORMATIONALLY COMPLETE POVMS

The outcome statistics of a quantum measurement are described by a positive-operator-valued measure (POVM) [80] on a set  $\mathcal{X}$  of measurement outcomes. When  $\mathcal{X}$  is countable the POVM is completely characterized by a set of positive operators,  $\{F(x)\}_{x \in \mathcal{X}}$ , called the ‘‘POVM elements,’’ which together satisfy the normalization constraint  $\sum_{x \in \mathcal{X}} F(x) = I$ . An *informationally complete POVM (IC-POVM)* [3, 4, 9, 10, 11, 12] is one with the property that for each quantum state,  $\rho \in \mathcal{Q}(\mathbb{C}^d) := \{A \in \text{End}(\mathbb{C}^d) \mid A \geq 0, \text{tr}(A) = 1\}$ , the outcome statistics,  $p(x) := \text{tr}[F(x)\rho]$ , uniquely identify the state. A sequence of measurements on copies of a system in an unknown state, enabling an estimate of the statistics, will then reveal the state.

In this article we are dealing primarily with *rank-one* POVMs. It is then appropriate to consider the measurement outcomes as points in complex projective space,  $\mathcal{X} \subseteq \mathbb{C}P^{d-1}$ , and set  $F(x) = \tau(x)\pi(x)$ , where  $\pi(x) := |x\rangle\langle x|$  and the positive weights  $\tau(x)$  inherit the normalization  $\sum_{x \in \mathcal{X}} \tau(x) = d$ . Important examples of such IC-POVMs include symmetric IC-POVMs (SIC-POVMs) [3] and complete sets of mutually unbiased bases (MUBs) [13, 14]. The main purpose of this section is to show that weighted complex projective 2-designs of the type constructed in the previous section, which include complete sets of MUBs as examples, specify optimal IC-POVMs for quantum state tomography by orthogonal measurements. This will be done in Sec. 5.3. We will begin by revisiting some of the results of Ref. [4].

It is clear that weighted 1-designs are equivalent to rank-one POVMs under the association  $\tau(x) = w(x)d$  and  $\mathcal{X} = \mathcal{D}$ . Weighted 2-designs have the additional property of being informationally complete. A productive way of showing this is as follows. Equipped with the Hilbert-Schmidt inner product  $(A|B) := \text{tr}(A^\dagger B)$ , the vector space  $\text{End}(\mathbb{C}^d) \cong \mathbb{C}^{d^2}$  is an inner product space where we think of  $(A|$  as an operator ‘‘bra’’ and  $|B)$  as an operator ‘‘ket’’ (see Caves [81] or Ref. [4] for notational clarification). Addition and scalar multiplication of operator kets then follows that for operators, e.g.  $|aA + bB) = a|A) + b|B)$  for  $a, b \in \mathbb{C}$ . Under the identification  $A \otimes B^\dagger \leftrightarrow |A)(B|$  we can rewrite our definition of a weighted 2-design

[Eq. (2.3) with  $t = 2$  and  $w(x) = \tau(x)/d$ ],

$$\sum_{x \in \mathcal{D}} \tau(x) \pi(x) \otimes \pi(x) = \frac{2\Pi_{\text{sym}}^{(2)}}{d+1} = \frac{1}{d+1} \left( \sum_{j,k} |e_j\rangle\langle e_k| \otimes |e_k\rangle\langle e_j| + I \otimes I \right), \quad (5.1)$$

in superoperator notation as

$$\sum_{x \in \mathcal{D}} \tau(x) |\pi(x)\rangle\rangle \langle\langle \pi(x)| = \frac{\mathbf{I} + |I\rangle\langle I|}{d+1} = \frac{1}{d+1} \left( \sum_{j,k} ||e_j\rangle\langle e_k| \rangle\rangle \langle\langle e_j| \langle e_k| + |I\rangle\langle I| \right), \quad (5.2)$$

where  $\mathbf{I} := \sum_{j,k} ||e_j\rangle\langle e_k| \rangle\rangle \langle\langle e_j| \langle e_k|$  is the identity superoperator under the “left-right” action [81] (meaning superoperators act on operators just like operators on vectors), i.e.  $\mathbf{I}|A\rangle\rangle = |A\rangle\rangle$  for all  $A \in \text{End}(\mathbb{C}^d)$ . The informational completeness of  $\{F(x) = \tau(x)\pi(x)\}_{x \in \mathcal{D}}$  is now immediately apparent from Eq. (5.2). In fact, an explicit state-reconstruction formula follows from the left-right action of this equation on a quantum state:

$$\sum_{x \in \mathcal{D}} \tau(x) |\pi(x)\rangle\rangle \langle\langle \pi(x)| \rho \rangle\rangle = \frac{\mathbf{I}|\rho\rangle\rangle + |I\rangle\langle I| |\rho\rangle\rangle}{d+1} = \frac{|\rho\rangle\rangle + |I\rangle\rangle}{d+1} \quad (5.3)$$

which simplifies to

$$\rho = (d+1) \sum_{x \in \mathcal{D}} p(x) \pi(x) - I, \quad (5.4)$$

where  $p(x) := \text{tr}[F(x)\rho] = \tau(x) \text{tr}[\pi(x)\rho]$  are the measurement outcome statistics.

The map  $\pi$  embeds complex projective space into  $\text{End}(\mathbb{C}^d)$ . If we instead embed  $\mathbb{C}P^{d-1}$  into the real vector space of traceless Hermitian operators  $\text{H}_0(\mathbb{C}^d) := \{A \in \text{End}(\mathbb{C}^d) \mid A^\dagger = A, \text{tr}(A) = 0\} \cong \mathbb{R}^{d^2-1}$ , via the mapping  $x \rightarrow \vartheta(x) := \pi(x) - I/d$ , then Eq. (5.2) takes a revealing form. Recalling the normalization  $\sum_{x \in \mathcal{D}} \tau(x) = d$ , we can rewrite this equation as

$$\sum_{x \in \mathcal{D}} \tau(x) |\pi(x) - I/d\rangle\rangle \langle\langle \pi(x) - I/d| = \frac{\mathbf{I} - |I\rangle\langle I|/d}{d+1} = \frac{\mathbf{\Pi}_0}{d+1}, \quad (5.5)$$

where  $\mathbf{\Pi}_0 := \mathbf{I} - |I\rangle\langle I|/d$  is the projector onto the subspace of traceless operators in  $\text{End}(\mathbb{C}^d)$ . In  $\text{H}_0(\mathbb{C}^d)$ , this of course means

$$\sum_{x \in \mathcal{D}} \tau(x) |\vartheta(x)\rangle\rangle \langle\langle \vartheta(x)| = \frac{\mathbf{I}_{\text{H}_0}}{d+1}, \quad (5.6)$$

where  $\mathbf{I}_{\text{H}_0}$  denotes the identity superoperator for this space. The interpretation afforded by Eq. (5.6), which states that  $\{\vartheta(x)\}_{x \in \mathcal{D}}$  forms a *tight (operator) frame* [59] in  $\text{H}_0(\mathbb{C}^d)$  with respect to the “trace” measure  $\tau$ , is that rank-one IC-POVMs which correspond to weighted 2-designs in  $\mathbb{C}P^{d-1}$  are “as close as possible” [82, 83] to orthonormal bases for  $\text{H}_0(\mathbb{C}^d)$ , when embedded into this space. Weighted complex projective 2-designs have thus been called *tight* rank-one IC-POVMs [4]. This analogy with tight frames is particularly pleasing since under the projection  $|\rho\rangle\rangle \rightarrow \mathbf{\Pi}_0|\rho\rangle\rangle = |\rho - I/d\rangle\rangle$ ,  $\text{H}_0(\mathbb{C}^d)$  is the natural place to study a general quantum state  $\rho \in \text{Q}(\mathbb{C}^d)$ . Indeed,  $\text{Q}(\mathbb{C}^2)$  then corresponds to the Bloch sphere.

### 5.1. Optimal quantum state estimation

Not only do tight rank-one IC-POVMs possess the above elegant structure, they are the optimal choice in the following state-estimation scenario. Consider a measuring instrument in the role of a cloning machine [84, 85, 86, 87, 88] (i.e. a one-to-infinity cloner [89]). The input to this machine is a single copy of an unknown pure state,  $\psi$ , and the output,  $\hat{\rho}(x)$ , is a state chosen to estimate  $\psi$  based on a measurement (with outcome  $x$ ). The fidelity between the input and output states, averaged over the measurement outcomes,

$$f^{(F, \hat{\rho})}(\psi) := \sum_{x \in \mathcal{X}} \text{tr}[F(x)\pi(\psi)] \text{tr}[\hat{\rho}(x)\pi(\psi)] , \quad (5.7)$$

can then be optimized for a worst-case input, only when the measurement is described by a tight IC-POVM (see Ref.'s [4, 34]). More precisely,

$$f_{\text{wc}}^{(F, \hat{\rho})} := \inf_{\psi \in \mathbb{C}P^{d-1}} f^{(F, \hat{\rho})}(\psi) \leq \frac{2}{d+1} , \quad (5.8)$$

with equality if and only if the outcome statistics for the measurement are described by a tight rank-one IC-POVM,  $\{F(x) = \tau(x)\pi(x)\}_{x \in \mathcal{X}}$  where  $\mathcal{X} \subseteq \mathbb{C}P^{d-1}$ , and  $\hat{\rho}(x) = \pi(x)$  is chosen for the output state. In such cases the output fidelity is in fact independent of the input state:  $f^{(F, \hat{\rho})}(\psi) = 2/(d+1)$ .

A measurement in a random basis is one strategy to achieve equality in Eq. (5.8). However a measuring instrument configurable to only  $m$  different bases,  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1}$ , will also suffice, provided  $\mathcal{D} = \cup_a \mathcal{B}_a$  forms a weighted 2-design with weight  $w(x) = \sum_a w_a 1_{\mathcal{B}_a}(x)$ , and the  $a$ -th basis is chosen with probability  $v_a = w_a d$ . This follows from the straightforward fact that rolling an  $m$ -sided die, where the  $a$ -th side occurs with probability  $v_a$ , and then performing an orthogonal measurement in a basis corresponding to the result,  $\mathcal{B}_b$  say, is one way of realizing the POVM  $\{F(x) = \tau(x)\pi(x)\}_{x \in \mathcal{X}}$  with  $\mathcal{X} = \cup_a \mathcal{B}_a$  and  $\tau(x) = \sum_a v_a 1_{\mathcal{B}_a}(x)$ . When  $d$  is prime power we know that only  $m = d+1$  configurations for the orthogonal measurements are needed, each specified by a member of a complete set of MUBs. If  $d$  is not a prime power, but  $d+1$  is, then the constructions of weighted 2-designs in the previous section show that  $m = d+2$  configurations suffice. In general,  $M(2, d)$  configurations are sufficient and necessary under a restriction to orthogonal measurements.

### 5.2. Optimal quantum state tomography by a repeated general measurement

Tight rank-one IC-POVMs are also an outstanding choice for *quantum state tomography* [2]. Suppose that we are instead given  $N$  copies of a system in an unknown general quantum state  $\rho \in \mathcal{Q}(\mathbb{C}^d)$ . A sequence of measurements on these copies, each with a measuring instrument described by the same IC-POVM,  $\{F(x)\}_{x \in \mathcal{X}}$  say, will provide an estimate of the statistics  $p(x) = \text{tr}[F(x)\rho]$ , and hence, identify the state.

State reconstruction for a general IC-POVM is facilitated by a *dual frame* [59] to the frame of POVM elements  $\{F(x)\}_{x \in \mathcal{X}}$ , i.e. a set of operators  $\{Q(x)\}_{x \in \mathcal{X}} \subseteq \text{End}(\mathbb{C}^d)$  satisfying

$$\sum_{x \in \mathcal{X}} |Q(x)\rangle\langle F(x)| = \sum_{x \in \mathcal{X}} \tau(x) |Q(x)\rangle\langle P(x)| = \mathbf{I} , \quad (5.9)$$

where we have introduced the positive-operator-valued density (POVD)  $P(x) := F(x)/\tau(x)$  and  $\tau(x) := \text{tr}[F(x)]$  for a general POVM. Alternatively,  $Q$  is a dual frame to  $P$  with respect to the trace measure  $\tau$ . In the current context we will refer to  $Q$  as a *reconstruction operator-valued density (OVD)* for the IC-POVM  $F$ . The left-right action of the dual frame condition [Eq. (5.9)] on a quantum state  $|\rho\rangle$  provides a state-reconstruction formula:

$$\rho = \sum_{x \in \mathcal{X}} p(x)Q(x). \quad (5.10)$$

There are generally many different choices for  $Q$ . The *canonical dual frame* to  $P$  (with respect to  $\tau$ ),

$$|R(x)\rangle := \mathcal{F}^{-1}|P(x)\rangle, \quad (5.11)$$

is found through the (left-right) inverse of the POVM superoperator,

$$\mathcal{F} := \sum_{x \in \mathcal{X}} \tau(x)|P(x)\rangle\langle P(x)|. \quad (5.12)$$

It is straightforward to confirm that  $\mathcal{F}^{-1}$  exists if and only if the POVM is informationally complete, and that Eq. (5.9) is satisfied for  $Q = R$ . The optimality of this choice was established in Ref. [4] for the current setting and then again by D'Ariano and Perinotti [90] for a similar scenario. In the special case of a tight rank-one IC-POVM, in which case  $F(x) = \tau(x)\pi(x)$  and  $\mathcal{X} \subseteq \mathbb{C}P^{d-1}$ , the canonical dual is  $R(x) = (d+1)\pi(x) - I$ , and Eq. (5.10) reduces to Eq. (5.4).

Now returning to our problem of state reconstruction, if  $y_1, \dots, y_N \in \mathcal{X}$  are the measurement results, then one estimate for the statistics is simply

$$\hat{p}(x) = \hat{p}(x; y_1, \dots, y_N) := \frac{1}{N} \sum_{k=1}^N \delta(x, y_k), \quad (5.13)$$

which under Eq. (5.10) gives

$$\hat{\rho} = \hat{\rho}(y_1, \dots, y_N) := \sum_{x \in \mathcal{X}} \hat{p}(x; y_1, \dots, y_N)Q(x), \quad (5.14)$$

for an estimate of  $\rho$ . We will call  $\hat{\rho}$  a *linear tomographic estimate* of  $\rho$  to distinguish it from more sophisticated choices, such as those from maximum likelihood estimation [91, 92] or Bayesian mean estimation [93, 94, 95, 96, 97].

The Hilbert-Schmidt distance  $d_{\text{HS}}(\rho, \hat{\rho}) := \|\rho - \hat{\rho}\|$ , where  $\|A\| := \sqrt{\text{tr}[AA^\dagger]}$ , provides a measure of the expected error in our estimate:

$$e^{(F,Q)}(\rho) := \mathbf{E}_{y_1, \dots, y_N} \left[ \|\rho - \hat{\rho}(y_1, \dots, y_N)\|^2 \right]. \quad (5.15)$$

Let  $\rho = \rho(\sigma, U) := U\sigma U^\dagger$  for some fixed quantum state  $\sigma \in \mathcal{Q}(\mathbb{C}^d)$ . It has been shown that, for random Hilbert-space orientations  $U$  between the state  $\sigma$  and measuring apparatus, the average Hilbert-Schmidt error can be minimized only when  $\{F(x)\}_{x \in \mathcal{X}}$  is a tight IC-POVM (see Ref. [4, Theorem 18]). That is,

$$e_{\text{av}}^{(F,Q)}(\sigma) := \int_{U(d)} d\mu(U) e^{(F,Q)}(\rho(\sigma, U)) \geq \frac{1}{N} \left( d(d+1) - 1 - \text{tr}(\sigma^2) \right), \quad (5.16)$$

with equality if and only if the outcome statistics for the measurements are described by a tight rank-one IC-POVM,  $\{F(x) = \tau(x)\pi(x)\}_{x \in \mathcal{X}}$  where  $\mathcal{X} \subseteq \mathbb{C}P^{d-1}$ , and  $Q(x) = R(x) = (d+1)\pi(x) - I$  is chosen for the dual frame. The same is true for the worst-case error  $e_{\text{wc}}^{(F,Q)}(\sigma) := \sup_{U \in \text{U}(d)} e^{(F,Q)}(\rho(\sigma, U))$ , and in fact, tight rank-one IC-POVMs form the unique class of POVMs achieving

$$e_{\text{wc}}^{(F,R)}(\sigma) = e_{\text{av}}^{(F,R)}(\sigma) = e^{(F,R)}(\rho(\sigma, U)) = \frac{1}{N} \left( d(d+1) - 1 - \text{tr}(\sigma^2) \right). \quad (5.17)$$

These results show that if we treat a family of  $m$  bases  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1}$ , as a single rank-one IC-POVM,  $\{F(x) = \tau(x)\pi(x)\}_{x \in \mathcal{X}}$  say, by setting  $\mathcal{X} = \cup_a \mathcal{B}_a$  and  $\tau(x) = \sum_a v_a 1_{\mathcal{B}_a}(x)$  for some choice of weights  $v_a$ , then the error in the tomographic process is minimized if and only if the outcome set  $\mathcal{X}$  forms a weighted 2-design with weight  $w(x) = \tau(x)/d$ , and Eq. (5.4) is used for state reconstruction. As we remarked in Sec. 5.1, one way of realizing the IC-POVM is to perform random orthogonal measurements as specified by the bases. In this case basis  $\mathcal{B}_a$  is chosen with probability  $v_a$ . Smaller error rates are achieved, however, if we instead choose  $\mathcal{B}_a$  exactly  $v_a N$  times. The following subsection focuses on this latter scenario.

### 5.3. Optimal quantum state tomography by a series of orthogonal measurements

When quantum state tomography is achieved through a series of orthogonal measurements, each specified by a member of a complete set of MUBs, it is customary to cycle through the bases in turn rather than select them randomly with equal probability. We will now treat this important scenario for a weighted complex projective 2-design composed of  $m$  orthonormal bases,  $\mathcal{X} = \cup_a \mathcal{B}_a$ . Although our results will apply in the general case, where there might be a multiplicity in elements across different bases, for the sake of notational simplicity, we will assume in this subsection that this is not the case. That is, we will assume that  $|\mathcal{X}| = md$ , so that  $w(e_j^a) = w_a$  (or  $\tau(e_j^a) = v_a$ ) under the association  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$ .

For complete state determination we require that the bases are in fact eigenbases, prescribed by members of an informationally complete set of quantum observables [9, 10, 11, 12]. Alternatively, the bases must together form a rank-one IC-POVM,  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$ , for some choice of the positive weights  $v_a$ . We prefer this latter setting since state reconstruction now follows from the results of Sec. 5.2. Note that if the POVM is informationally complete for one choice of the weights, then it is informationally complete for all choices. Thus, with the exception that  $v_a > 0$  and  $\sum_a v_a = 1$ , the weights can be chosen arbitrarily. There will be one particular choice, however, which will ease the analysis. With these considerations in mind, let us now begin.

Suppose that we make a series of orthogonal measurements as specified by a family of bases  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1}$ , which together form a rank-one IC-POVM,  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$ , for some choice of the weights  $v_a > 0$ . Let  $n_a$  denote the number of measurements in basis  $\mathcal{B}_a$ , and let  $N := \sum_a n_a$  be the total number of measurements. Since we know that the IC-POVM in fact describes a series of orthogonal measurements, we will replace our previous estimate of the statistics [Eq. (5.13)] with

$$\hat{p}(e_j^a) = \hat{p}(e_j^a; y_1, \dots, y_N) := \frac{v_a}{n_a} \sum_{k=1}^N \delta(e_j^a, y_k), \quad (5.18)$$

but retain Eq. (5.14) for our estimate of  $\rho$ . Now following Ref. [4], we use this equation and Eq. (5.10) together to rewrite the squared Hilbert-Schmidt distance as

$$\|\rho - \hat{\rho}\|^2 = \sum_{x,y \in \mathcal{X}} (p(x) - \hat{p}(x))(p(y) - \hat{p}(y))(Q(x)|Q(y)) \quad (5.19)$$

$$= \sum_{a,b,j,k} (p(e_j^a) - \hat{p}(e_j^a))(p(e_k^b) - \hat{p}(e_k^b))(Q(e_j^a)|Q(e_k^b)), \quad (5.20)$$

giving an error in the form

$$e^{(\{\mathcal{B}_a, v_a\}, Q)}(\rho) := \mathbf{E}_{y_1, \dots, y_N} \left[ \|\rho - \hat{\rho}(y_1, \dots, y_N)\|^2 \right] \quad (5.21)$$

$$= \sum_{a,j,k} \frac{1}{n_a} (v_a p(e_j^a) \delta_{jk} - p(e_j^a) p(e_k^a)) (Q(e_j^a) | Q(e_k^a)), \quad (5.22)$$

since

$$\mathbf{E}_{y_1, \dots, y_N} \left[ (p(e_j^a) - \hat{p}(e_j^a))(p(e_k^b) - \hat{p}(e_k^b)) \right] = v_a v_b \mathbf{E}_{y_1, \dots, y_N} \left[ (q(e_j^a) - \hat{q}(e_j^a))(q(e_k^b) - \hat{q}(e_k^b)) \right] \quad (5.23)$$

$$= \frac{\delta_{ab} v_a^2}{n_a} (q(e_j^a) \delta_{jk} - q(e_j^a) q(e_k^a)) \quad (5.24)$$

$$= \frac{\delta_{ab}}{n_a} (v_a p(e_j^a) \delta_{jk} - p(e_j^a) p(e_k^a)), \quad (5.25)$$

where  $q(e_j^a) := \text{tr}[\pi(e_j^a)\rho] = p(e_j^a)/v_a$  is the probability of result  $e_j^a$  for the  $a$ -th orthogonal measurement, our estimate for this probability is  $\hat{q}(e_j^a) := \hat{p}(e_j^a)/v_a$  [under Eq. (5.18)], and the expectation is an elementary calculation.

Now suppose that the rank-one IC-POVM  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is in fact a tight IC-POVM. Choosing  $n_a = v_a N$  and  $Q(e_j^a) = R(e_j^a) = (d+1)\pi(e_j^a) - I$  for the dual frame, we find that Eq. (5.22) simplifies to

$$e^{(\{\mathcal{B}_a, v_a\}, R)}(\rho) = \frac{(d+1)^2}{N} \left( 1 - \sum_{a,j} \frac{p(e_j^a)^2}{v_a} \right). \quad (5.26)$$

But for a tight rank-one IC-POVM

$$\sum_{a,j} \frac{p(e_j^a)^2}{v_a} = \sum_{a,j} v_a \text{tr} [\pi(e_j^a) \otimes \pi(e_j^a) \cdot \rho \otimes \rho] \quad (5.27)$$

$$= \frac{2}{d+1} \text{tr} [\Pi_{\text{sym}}^{(2)} \cdot \rho \otimes \rho] \quad (5.28)$$

$$= \frac{1}{d+1} (1 + \text{tr}(\rho^2)), \quad (5.29)$$

using Eq. (5.1) with  $\tau(e_j^a) = v_a$ , achieving the error rate

$$e^{(\{\mathcal{B}_a, v_a\}, R)}(\rho) = \frac{d+1}{N} (d - \text{tr}(\rho^2)). \quad (5.30)$$

Although the dominating contribution of  $d^2/N$  remains the same, a comparison of the two error rates confirms a small improvement:

$$0 \leq e^{(F,R)}(\rho) - e^{\{\mathcal{B}_a, v_a\}, R}(\rho) = \frac{1}{N} \left( d \operatorname{tr}(\rho^2) - 1 \right) \leq \frac{d-1}{N}. \quad (5.31)$$

The difference can be attributed to Eq. (5.22) (as compared to Eq. (76) of Ref. [4]), which takes into account that the bases are now being chosen nonrandomly.

We will now show that the improved error rate [Eq. (5.30)] is in fact the minimum possible for any family of bases  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1}$ , and for any choice of the reconstruction OVD  $\{Q(e_j^a)\}_{a,j}$ , i.e., for any  $Q$  satisfying the dual frame condition

$$\sum_{a,j} |Q(e_j^a)(F(e_j^a))| = \sum_{a,j} v_a |Q(e_j^a)(P(e_j^a))| = \mathbf{I}, \quad (5.32)$$

where  $P(e_j^a) = \pi(e_j^a)$ . Let  $\rho(\sigma, U) := U\sigma U^\dagger$  for some fixed quantum state  $\sigma \in \mathcal{Q}(\mathbb{C}^d)$  and define the average error in the linear tomographic estimate of  $\rho(\sigma, U)$  as

$$e_{\text{av}}^{\{\mathcal{B}_a, v_a\}, Q}(\sigma) := \int_{\mathcal{U}(d)} d\mu(U) e^{\{\mathcal{B}_a, v_a\}, Q}(\rho(\sigma, U)), \quad (5.33)$$

using Eq.'s (5.10), (5.14), (5.18) and (5.21). The following is then the main result of this section.

**Theorem 5.1.** *Let  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1} \subset \mathbb{C}P^{d-1}$  be a family of orthonormal bases for  $\mathbb{C}^d$  with the property that  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is an IC-POVM, under the association  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$ , for some choice of the positive constants  $v_0, \dots, v_{m-1}$ . Then for any fixed quantum state  $\sigma \in \mathcal{Q}(\mathbb{C}^d)$ , the average error in the linear tomographic estimate of  $\rho(\sigma, U)$  after  $N = \sum_a n_a$  orthogonal measurements, with  $n_a > 0$  of those measurements in the basis  $\mathcal{B}_a$ , satisfies*

$$e_{\text{av}}^{\{\mathcal{B}_a, v_a\}, Q}(\sigma) \geq \frac{d+1}{N} \left( d - \operatorname{tr}(\sigma^2) \right), \quad (5.34)$$

for all reconstruction OVDs  $\{Q(e_j^a)\}_{a,j}$ . Furthermore, equality occurs if and only if  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is a tight rank-one IC-POVM for the choice  $v_a = n_a/N$ , and, assuming this choice for state reconstruction,  $Q(e_j^a) = (d+1)\pi(e_j^a) - I + D_a$ , where  $\{D_a\}_a$  is any set of operators satisfying  $\sum_a v_a D_a = 0$ .

In particular, equality holds in Eq. (5.34) for a tight rank-one IC-POVM whenever  $Q$  is the canonical dual frame, namely  $Q(e_j^a) = R(e_j^a) = (d+1)\pi(e_j^a) - I$ .

This theorem is the analogue of Theorem 18 in Ref. [4] and its proof will be similar. We first establish that the canonical dual frame with respect to the trace measure is optimal for state reconstruction. Unlike the scenario considered in the previous subsection, however, where the bases were sampled randomly, the canonical dual is no longer the unique optimum. These facts are a consequence of the following lemma (which is analogous to Lemma 16 of Ref. [4]). Recall the general definition of the canonical dual frame  $R$  [Eq. (5.11)].

**Lemma 5.2.** *Let  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  be an IC-POVM with reconstruction OVD  $\{Q(e_j^a)\}_{a,j}$ , where each  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$  is an orthonormal basis for  $\mathbb{C}^d$ . Then*

$$\sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (Q(e_j^a) | Q(e_k^a)) \geq \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (R(e_j^a) | R(e_k^a)), \quad (5.35)$$

with equality if and only if  $Q(e_k^a) = R(e_k^a) + D_a$ , where  $\{D_a\}_a$  is any set of operators satisfying  $\sum_a v_a D_a = 0$ .

*Proof.* By analogy with the dual frame condition [Eq. (5.32)], first note that

$$\sum_{a,j,k} v_a |Q(e_j^a)\rangle \langle P(e_k^a)| = \sum_{a,j} v_a |Q(e_j^a)\rangle \langle I| = |I\rangle \langle I|, \quad (5.36)$$

since  $\sum_k P(e_k^a) = \sum_k \pi(e_k^a) = I$  and the left-right action of Eq. (5.32) on  $|I\rangle$  shows that  $\sum_{a,j} v_a Q(e_j^a) = I$ . Now  $Q$  and  $R$  are both dual frames, so defining  $D := Q - R$  we have

$$\sum_{a,j,k} v_a |D(e_j^a)\rangle \langle P(e_k^a)| = |I\rangle \langle I| - |I\rangle \langle I| = 0, \quad (5.37)$$

and since  $|R(e_k^a)\rangle := \mathcal{F}^{-1}|P(e_k^a)\rangle$ ,

$$\sum_{a,j,k} v_a |D(e_j^a)\rangle \langle R(e_k^a)| = 0, \quad (5.38)$$

which means

$$\sum_{a,j,k} v_a (D(e_j^a)|R(e_k^a)) = 0. \quad (5.39)$$

This is the analogue of Eq. (89) in the proof of Lemma 16, Ref. [4], which in the current scenario takes the form

$$\sum_{a,j} v_a (D(e_j^a)|R(e_j^a)) = 0. \quad (5.40)$$

Combining, we obtain

$$\sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (D(e_j^a)|R(e_k^a)) = 0. \quad (5.41)$$

Using this relation and the inequality

$$\sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (D(e_j^a)|D(e_k^a)) = \sum_{a,j} v_a (C(e_j^a)|C(e_j^a)) \geq 0, \quad (5.42)$$

where we have set  $C(e_j^a) := D(e_j^a) - \frac{1}{d} \sum_k D(e_k^a)$ , we obtain

$$\begin{aligned} \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (Q(e_j^a)|Q(e_k^a)) &= \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) \left[ (R(e_j^a)|R(e_k^a)) + (R(e_j^a)|D(e_k^a)) \right. \\ &\quad \left. + (D(e_j^a)|R(e_k^a)) + (D(e_j^a)|D(e_k^a)) \right] \end{aligned} \quad (5.43)$$

$$= \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) \left[ (R(e_j^a)|R(e_k^a)) + (D(e_j^a)|D(e_k^a)) \right] \quad (5.44)$$

$$\geq \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (R(e_j^a)|R(e_k^a)), \quad (5.45)$$

which is our desired result. Equality holds if and only if  $C(e_j^a) = 0$  for all  $j$  and  $a$ , or equivalently,  $D(e_j^a) = D_a$ , an operator which is independent of  $j$ . Both  $R(e_k^a)$  and  $Q(e_k^a) = R(e_k^a) + D_a$  must remain dual frames, however, so it is necessary that  $\sum_{a,j} v_a |P(e_j^a)\rangle \langle D_a| = \sum_a v_a |I\rangle \langle D_a| = 0$ , i.e.  $\sum_a v_a D_a = 0$ .  $\square$

The following technical result is also needed to prove Theorem 5.1. Let  $T := \sum_{j,k} |e_j\rangle\langle e_k| \otimes |e_k\rangle\langle e_j|$ , which is called the “swap” since  $T|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$ .

**Lemma 5.3.** *Let  $\mu$  be the Haar measure on  $U(d)$ . Then*

$$\int_{U(d)} d\mu(U) [U\pi(e_j)U^\dagger] \otimes [U\pi(e_k)U^\dagger] = \frac{1 - \delta_{jk}/d}{d^2 - 1} I \otimes I + \frac{\delta_{jk} - 1/d}{d^2 - 1} T. \quad (5.46)$$

*Proof.* We have previously seen that [Eq. (2.2)]

$$\int_{U(d)} d\mu(U) [U\pi(e_j)U^\dagger]^{\otimes 2} = \binom{d+1}{2}^{-1} \Pi_{\text{sym}}^{(2)} = \frac{I \otimes I + T}{d(d+1)}, \quad (5.47)$$

which is Eq. (5.46) for  $j = k$ . Now write  $I = \sum_j \pi(e_j)$  and expand

$$I \otimes I = \int_{U(d)} d\mu(U) [UIU^\dagger] \otimes [UIU^\dagger] \quad (5.48)$$

$$= \int_{U(d)} d\mu(U) \sum_{j,k} [U\pi(e_j)U^\dagger] \otimes [U\pi(e_k)U^\dagger] \quad (5.49)$$

$$= \int_{U(d)} d\mu(U) \left( d [U\pi(e_j)U^\dagger]^{\otimes 2} + d(d-1) [U\pi(e_j)U^\dagger] \otimes [U\pi(e_k)U^\dagger] \right) \quad (5.50)$$

$$= \frac{I \otimes I + T}{d+1} + d(d-1) \int_{U(d)} d\mu(U) [U\pi(e_j)U^\dagger] \otimes [U\pi(e_k)U^\dagger], \quad (5.51)$$

assuming  $j \neq k$  in the last two lines. Solving this equation gives Eq. (5.46) for  $j \neq k$ .  $\square$

*Proof of Theorem 5.1.* First note that since the weights  $v_a$  could always be absorbed into  $Q$  in the RHS of Eq. (5.32), we are free to set  $v_a = n_a/N$  without any loss of generality, and thus do so. Now using Eq. (5.22) we have

$$e_{\text{av}}^{(\{\mathcal{B}_a, v_a\}, Q)}(\sigma) := \int_{U(d)} d\mu(U) e^{(\{\mathcal{B}_a, v_a\}, Q)}(\rho(\sigma, U)) \quad (5.52)$$

$$= \int_{U(d)} d\mu(U) \sum_{a,j,k} \frac{1}{n_a} (v_a p(e_j^a) \delta_{jk} - p(e_j^a) p(e_k^a)) (Q(e_j^a) | Q(e_k^a)) \quad (5.53)$$

$$= \sum_{a,j,k} \frac{v_a}{N} \int_{U(d)} d\mu(U) \left( \text{tr}[\pi(e_j^a) U \sigma U^\dagger] \delta_{jk} - \text{tr}[\pi(e_j^a) U \sigma U^\dagger] \text{tr}[\pi(e_k^a) U \sigma U^\dagger] \right) \cdot (Q(e_j^a) | Q(e_k^a)) \quad (5.54)$$

$$= \sum_{a,j,k} \frac{v_a}{N} \left( \frac{\delta_{jk}}{d} - \int_{U(d)} d\mu(U) \text{tr} \left[ [U^\dagger \pi(e_j^a) U] \otimes [U^\dagger \pi(e_k^a) U] \cdot \sigma \otimes \sigma \right] \right) \cdot (Q(e_j^a) | Q(e_k^a)) \quad (5.55)$$

since  $p(e_j^a) := v_a \text{tr}[\pi(e_j^a) \rho] = v_a \text{tr}[\pi(e_j^a) U \sigma U^\dagger]$  and  $\int_{U(d)} d\mu(U) U \sigma U^\dagger = I/d$ . The remaining integral is the content of Lemma 5.3, and since  $\text{tr}(T \cdot \sigma \otimes \sigma) = \text{tr}(\sigma^2)$ , Eq. (5.55) reduces to

$$e_{\text{av}}^{(\{\mathcal{B}_a, v_a\}, Q)}(\sigma) = \frac{d - \text{tr}(\sigma^2)}{(d^2 - 1)N} \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (Q(e_j^a) | Q(e_k^a)) \quad (5.56)$$

$$\geq \frac{d - \text{tr}(\sigma^2)}{(d^2 - 1)N} \sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (R(e_j^a) | R(e_k^a)), \quad (5.57)$$

applying Lemma 5.2. The sum can be simplified:

$$\sum_{a,j,k} v_a \left( \delta_{jk} - \frac{1}{d} \right) (R(e_j^a) | R(e_k^a)) = \sum_a v_a \left( \sum_j (R(e_j^a) | R(e_j^a)) - \frac{1}{d} \sum_{j,k} (R(e_j^a) | R(e_k^a)) \right) \quad (5.58)$$

$$= \left( \text{Tr}(\mathcal{F}^{-1}) - \frac{1}{d} \sum_{a,j,k} v_a (P(e_j^a) | \mathcal{F}^{-2} | P(e_k^a)) \right) \quad (5.59)$$

$$= \left( \text{Tr}(\mathcal{F}^{-1}) - \frac{1}{d} \sum_a v_a (I | \mathcal{F}^{-2} | I) \right) \quad (5.60)$$

$$= \left( \text{Tr}(\mathcal{F}^{-1}) - \frac{1}{d} (I | I) \right) \quad (5.61)$$

$$= \left( \text{Tr}(\mathcal{F}^{-1}) - 1 \right), \quad (5.62)$$

using Eq.'s (44) and (42) of Ref. [4], i.e.  $\mathcal{F}^{-1} = \sum_{a,j} v_a |R(e_j^a)\rangle\langle R(e_j^a)|$  and  $\mathcal{F}|I\rangle = |I\rangle$ , and also the fact that  $\sum_j P(e_j^a) = \sum_j \pi(e_j^a) = I$ .

We have thus shown that

$$e_{\text{av}}^{\{\mathcal{B}_a, v_a\}, Q}(\sigma) \geq \frac{1}{(d^2 - 1)N} \left( \text{Tr}(\mathcal{F}^{-1}) - 1 \right) \left( d - \text{tr}(\sigma^2) \right), \quad (5.63)$$

with equality if and only if  $Q(e_k^a) = R(e_k^a) + D_a$ , where  $R$  is the canonical dual frame with respect to the trace measure  $\tau(e_j^a) = v_a = n_a/N$ , and  $\sum_a v_a D_a = 0$ . The remainder of the proof now follows from Lemma 17 of Ref. [4], which states that

$$\text{Tr}(\mathcal{F}^{-1}) \geq d(d(d+1) - 1), \quad (5.64)$$

with equality if and only if  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is a tight rank-one IC-POVM.  $\square$

Finally, recalling that  $\rho(\sigma, U) := U\sigma U^\dagger$  for some fixed  $\sigma \in \mathbb{Q}(\mathbb{C}^d)$ , we define the worst-case error in the linear tomographic estimate of  $\rho(\sigma, U)$  as

$$e_{\text{wc}}^{\{\mathcal{B}_a, v_a\}, Q}(\sigma) := \sup_{U \in \mathbb{U}(d)} e^{\{\mathcal{B}_a, v_a\}, Q}(\rho(\sigma, U)), \quad (5.65)$$

again using Eq.'s (5.10), (5.14), (5.18) and (5.21). The worst-case error is always bounded below by the average error, and when the bases form a tight rank-one IC-POVM, the error is in fact independent of  $U$  [see Eq. (5.30)]. We can thus immediately deduce the following corollary to Theorem 5.1.

**Corollary 5.4.** *Let  $\mathcal{B}_0, \dots, \mathcal{B}_{m-1} \subset \mathbb{C}P^{d-1}$  be a family of orthonormal bases for  $\mathbb{C}^d$  with the property that  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is an IC-POVM, under the association  $\mathcal{B}_a = \{e_j^a\}_{j=0}^{d-1}$ , for some choice of the positive constants  $v_0, \dots, v_{m-1}$ . Then for any fixed quantum state  $\sigma \in \mathbb{Q}(\mathbb{C}^d)$ , the worst-case error in the linear tomographic estimate of  $\rho(\sigma, U)$  after  $N = \sum_a n_a$  orthogonal measurements, with  $n_a > 0$  of those measurements in the basis  $\mathcal{B}_a$ , satisfies*

$$e_{\text{wc}}^{\{\mathcal{B}_a, v_a\}, Q}(\sigma) \geq \frac{d+1}{N} \left( d - \text{tr}(\sigma^2) \right), \quad (5.66)$$

for all reconstruction OVDs  $\{Q(e_j^a)\}_{a,j}$ . Furthermore, equality occurs if and only if  $\{F(e_j^a) = v_a \pi(e_j^a)\}_{a,j}$  is a tight rank-one IC-POVM for the choice  $v_a = n_a/N$ , and, assuming this choice for state reconstruction,  $Q(e_j^a) = (d+1)\pi(e_j^a) - I + D_a$ , where  $\{D_a\}_a$  is any set of operators satisfying  $\sum_a v_a D_a = 0$ .

In fact, weighted complex projective 2-designs which are composed of orthonormal bases specify the unique class IC-POVMs (describing a series of orthogonal measurements) that achieve

$$e_{\text{wc}}^{\{\mathcal{B}_a, v_a\}, R}(\sigma) = e_{\text{av}}^{\{\mathcal{B}_a, v_a\}, R}(\sigma) = e^{\{\mathcal{B}_a, v_a\}, R}(\rho(\sigma, U)) = \frac{d+1}{N} \left( d - \text{tr}(\sigma^2) \right). \quad (5.67)$$

## 6. CONCLUSION

In this article we have introduced the problem of constructing weighted 2-designs in  $\mathbb{C}P^{d-1}$  from the union of a family of  $m$  orthonormal bases for  $\mathbb{C}^d$ . If the weight remains constant across elements of the same basis, then such designs can be interpreted as generalizations of complete sets of MUBs, being equivalent whenever  $m = d + 1$  (Theorem 3.3). Although weighted 2-designs can be constructed from orthonormal bases in all dimensions and for all sufficiently large  $m \geq d + 1$  (Corollary 3.2 and Theorem 3.3), the task remains to find examples with  $m$  as close as possible to the lower bound. To this end, we have presented explicit constructions of weighted 2-designs from  $m = kd + 2$  bases whenever  $kd + 1$  is a prime power, for any positive integer  $k$  (Propositions 4.3 and 4.4 with Theorem 4.2), and shown that  $m = O(d^2)$  bases are always sufficient (Proposition 4.5 with Theorem 4.2). Furthermore, our approach, which is based on highly nonlinear functions on abelian groups, sheds new light on the known constructions of complete sets of MUBs. Finally, we have shown that the entire class of weighted complex projective 2-designs which are composed of orthonormal bases specify the unique optimal choice of bases for quantum state tomography by orthogonal measurements (Theorem 5.1 and Corollary 5.4).

Although this article was motivated from the practical standpoint of verifying quantum mechanical devices for information processing, quantum tomography provides one of the most powerful means to explore and test fundamental aspects of quantum theory. Indeed, quantum information processors rely so critically on the soundness of this theory that their very construction will provide new testament to its validity.

## Acknowledgments

The authors would like to thank Chris Godsil and Barry Sanders for their advice and input. AR is supported by NSERC and MITACS. AJS is supported by ARC and the State of Queensland.

- 
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
  - [2] M. Paris and J. Řeháček (Eds.), *Quantum State Estimation* (Springer-Verlag, Berlin, 2004).
  - [3] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, “Symmetric informationally complete quantum measurements,” *J. Math. Phys.* **45**, 2171 (2004).
  - [4] A. J. Scott, “Tight informationally complete quantum measurements,” *J. Phys. A* **39**, 13507 (2006).
  - [5] U. Fano, “Description of states in quantum mechanics by density matrix and operator techniques,” *Rev. Mod. Phys.* **29**, 74 (1957).

- [6] J. L. Park and W. Band, “A general method of empirical state determination in quantum physics: Part I,” *Found. Phys.* **1**, 211 (1971); W. Band and J. L. Park, “A general method of empirical state determination in quantum physics: Part II,” *Found. Phys.* **1**, 339 (1971).
- [7] I. D. Ivanović, “Formal state determination,” *J. Math. Phys.* **24**, 1199 (1983).
- [8] U. Leonhardt, “Quantum-state tomography and discrete Wigner function,” *Phys. Rev. Lett.* **74**, 4101 (1995).
- [9] E. Prugovečki, “Information-theoretic aspects of quantum measurement,” *Int. J. Theor. Phys.* **16**, 321 (1977).
- [10] F. E. Schroeck, “Coexistence of observables,” *Int. J. Theor. Phys.* **28**, 247 (1989).
- [11] P. Busch and P. J. Lahti, “The determination of the past and the future of a physical system in quantum mechanics,” *Found. Phys.* **19**, 633 (1989).
- [12] P. Busch, “Informationally complete sets of physical quantities,” *Int. J. Theor. Phys.* **30**, 1217 (1991).
- [13] I. D. Ivanović, “Geometrical description of quantal state determination,” *J. Phys. A* **14**, 3241 (1981).
- [14] W. K. Wootters and B. D. Fields, “Optimal state-determination by mutually unbiased measurements,” *Ann. Phys.* **191**, 363 (1989).
- [15] W. Alltop, “Complex sequences with low periodic correlations,” *IEEE Trans. Inf. Theory* **26**, 350 (1980).
- [16] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, “ $\mathbb{Z}_4$ -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets,” *Proc. London Math. Soc.* **75**, 436 (1997).
- [17] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, “A new proof for the existence of mutually unbiased bases,” *Algorithmica* **34**, 512 (2002).
- [18] A. Klappenecker and M. Rötteler, “Constructions of mutually unbiased bases,” *Finite fields and applications*, Lecture Notes in Comput. Sci. **2948**, 137 (2004).
- [19] P. Wocjan and T. Beth, “New construction of mutually unbiased bases in square dimensions,” *Quantum Inf. Comput.* **5**, 93 (2005).
- [20] M. Planat, H. C. Rosu and S. Perrine, “A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements,” *Found. Phys.* **36**, 1662 (2006).
- [21] C. Godsil and A. Roy, “Equiangular lines, mutually unbiased bases, and spin models,” arXiv:quant-ph/0511004.
- [22] M. Saniga, M. Planat and H. Rosu, “Mutually unbiased bases and finite projective planes,” *J. Opt. B* **6**, L19 (2004).
- [23] I. Bengtsson and Å. Ericsson, “Mutually unbiased bases and the complementarity polytope,” *Open Syst. Inf. Dyn.* **12**, 107 (2005).
- [24] C. Archer, “There is no generalization of known formulas for mutually unbiased bases,” *J. Math. Phys.* **46**, 022106 (2005).
- [25] W. K. Wootters, “Quantum measurements and finite geometry,” *Found. Phys.* **36**, 112 (2006).
- [26] M. Aschbacher, A. M. Childs and P. Wocjan, “The limitations of nice mutually unbiased bases,” *J. Algebr. Combin.* **25**, 111 (2007).
- [27] P. O. Boykin, M. Sitharam, P. H. Tiep and P. Wocjan, “Mutually unbiased bases and orthogonal decompositions of Lie algebras,” *Quantum Inf. Comput.* **7**, 371 (2007).
- [28] M. Grassl, “On SIC-POVMs and MUBs in dimension 6,” in *Proceedings of the ERATO Conference on Quantum Information Science*, Tokyo, Sept. 2004, p. 60.
- [29] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej and K. Życzkowski, “Mubs and Hadamards of order six,” *J. Math. Phys.*, to appear; arXiv:quant-ph/0610161.

- [30] P. Butterley and W. Hall, “Numerical evidence for the maximum number of mutually unbiased bases in dimension six,” arXiv:quant-ph/0701122.
- [31] G. Zauner, “Quantendesigns - Grundzüge einer nichtkommutativen Designtheorie,” PhD thesis (University of Vienna, 1999).
- [32] H. Barnum, “Information-disturbance tradeoff in quantum measurement on the uniform ensemble,” Dept. of Computer Science Technical Report CSTR-00-013 (University of Bristol, 2000).
- [33] A. Klappenecker and M. Rötteler, “Mutually unbiased bases are complex projective 2-designs,” in Proceedings of the IEEE International Symposium on Information Theory, Adelaide, Australia, Sept. 2005, p. 1740.
- [34] A. Hayashi, T. Hashimoto and M. Horibe, “Reexamination of optimal quantum state estimation of pure states,” Phys. Rev. A **72**, 032325 (2005).
- [35] M. A. Ballester, “Optimal estimation of  $SU(d)$  using exact and approximate 2-designs,” arXiv:quant-ph/0507073.
- [36] C. Dankert, R. Cleve, J. Emerson and E. Livine, “Exact and approximate unitary 2-designs: constructions and applications,” arXiv:quant-ph/0606161.
- [37] D. Gross, K. Audenaert and J. Eisert, “Evenly distributed unitaries: on the structure of unitary designs,” J. Math. Phys., to appear; arXiv:quant-ph/0611002.
- [38] I. H. Kim, “Quantumness, generalized spherical 2-design and symmetric informationally complete POVM,” Quantum Inf. Comput., to appear; arXiv:quant-ph/0608024.
- [39] A. Ambainis and J. Emerson, “Quantum  $t$ -designs:  $t$ -wise independence in the quantum world,” arXiv:quant-ph/0701126.
- [40] P. Delsarte, J. M. Goethals and J. J. Seidel, “Spherical codes and designs,” Geom. Dedicata **6**, 363 (1977).
- [41] A. Neumaier, “Combinatorial configurations in terms of distances,” Dept. of Mathematics Memorandum 81-09 (Eindhoven University of Technology, 1981).
- [42] S. G. Hoggar, “ $t$ -designs in projective spaces,” Europ. J. Combin. **3**, 233 (1982).
- [43] S. G. Hoggar, “Parameters of  $t$ -designs in  $\mathbb{F}P^{d-1}$ ,” Europ. J. Combin. **5**, 29 (1984).
- [44] S. G. Hoggar, “Tight 4 and 5-designs in projective spaces,” Graphs Combin. **5**, 87 (1989).
- [45] S. G. Hoggar, “ $t$ -designs with general angle set,” Europ. J. Combin. **13**, 257 (1992).
- [46] E. Bannai and S. G. Hoggar, “On tight  $t$ -designs in compact symmetric spaces of rank one,” Proc. Japan Acad. **61A**, 78 (1985).
- [47] E. Bannai and S. G. Hoggar, “Tight  $t$ -designs and squarefree integers,” Europ. J. Combin. **10**, 113 (1989).
- [48] V. Levenshtein, “Designs as maximum codes in polynomial metric spaces,” Acta Appl. Math. **29**, 1 (1992).
- [49] V. Levenshtein, “On designs in compact metric spaces and a universal bound on their size,” Discrete Math. **192**, 251 (1998).
- [50] V. Levenshtein, “Universal bounds for codes and designs,” in V. Pless and C. W. Huffman (Eds.), *Handbook of Coding Theory* (Elsevier, Amsterdam, 1998), p. 499.
- [51] C. F. Dunkl, “Discrete quadrature and bounds on  $t$ -designs,” Michigan Math. J. **26**, 81 (1979).
- [52] P. D. Seymour and T. Zaslavsky, “Averaging sets: a generalization of mean values and spherical designs,” Adv. Math. **52**, 213 (1984).
- [53] S. Nikova, “On bounds on the size of designs in complex projective spaces,” in Proceedings of the International Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, May 1995, p. 121.

- [54] P. Boyvalenkov and S. Nikova, “On lower bounds on the size of designs in compact symmetric spaces of rank 1,” *Arch. Math.* **68**, 81 (1997).
- [55] S. Nikova, “Bounds for designs in infinite polynomial metric spaces,” PhD thesis (Eindhoven University of Technology, 1998).
- [56] P. Boyvalenkov, S. Boumova and D. Danev, “Necessary conditions for existence of some designs in polynomial metric spaces,” *Europ. J. Combin.* **20**, 213 (1999).
- [57] H. König, “Cubature formulas on spheres,” in W. Haußmann, K. Jetter and M. Reimer (Eds.), *Advances in Multivariate Approximation* (Wiley-VCH, Berlin, 1999), p. 201.
- [58] J. J. Seidel, “Definitions for spherical designs,” *J. Statist. Plann. Inference* **95**, 307 (2001).
- [59] O. Christensen, *An Introduction to Frames and Riesz Bases* (Birkhäuser, Boston, 2003).
- [60] D. M. Appleby, “Symmetric informationally complete-positive operator valued measures and the extended Clifford group,” *J. Math. Phys.* **46**, 052107 (2005).
- [61] M. Grassl, “Tomography of quantum states in small dimensions,” *Electron. Notes Discrete Math.* **20**, 151 (2005).
- [62] A. Klappenecker, M. Rötteler, I. E. Shparlinski and A. Winterhof, “On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states,” *J. Math. Phys.* **46**, 082104 (2005).
- [63] S. Colin, J. Corbett, T. Durt and D. Gross, “About SIC POVMs and discrete Wigner distributions,” *J. Opt. B* **7**, S778 (2005).
- [64] S. T. Flammia, “On SIC-POVMs in prime dimensions,” *J. Phys. A* **39**, 13483 (2006).
- [65] D. M. Appleby, “Symmetric informationally complete measurements of arbitrary rank,” arXiv:quant-ph/0611260.
- [66] R. H. Hardin and N. J. A. Sloane, “McLaren’s improved snub cube and other new spherical designs in three dimensions,” *Discrete Comput. Geom.* **15**, 429 (1996).
- [67] S. G. Hoggar, “64 lines from a quaternionic polytope,” *Geom. Dedic.* **69**, 287 (1998).
- [68] L. R. Welch, “Lower bounds on the maximum cross correlation of signals,” *IEEE Trans. Inf. Theory* **20**, 397 (1974).
- [69] K. Nyberg, “Differentially uniform mappings for cryptography,” *Advances in cryptology—EUROCRYPT ’93* (Lofthus), *Lecture Notes in Comput. Sci.* **765**, 55 (1994).
- [70] K. J. Horadam, “Differentially 2-uniform cocycles—the binary case,” *Applied algebra, algebraic algorithms and error-correcting codes*, *Lecture Notes in Comput. Sci.* **2643**, 150 (2003).
- [71] C. Carlet and C. Ding, “Highly nonlinear mappings,” *J. Complexity* **20**, 205 (2004).
- [72] A. Pott, “Nonlinear functions in abelian groups and relative difference sets,” *Discrete Appl. Math.* **138**, 177 (2004).
- [73] F. Chabaud and S. Vaudenay, “Links between differential and linear cryptanalysis,” *Advances in cryptology—EUROCRYPT ’94* (Perugia), *Lecture Notes in Comput. Sci.* **950**, 365 (1995).
- [74] W. Ledermann, *Introduction to group characters*, (Cambridge University Press, Cambridge, 1977).
- [75] J. Yuan, C. Carlet, and C. Ding, “The weight distribution of a class of linear codes from perfect nonlinear functions,” *IEEE Trans. Inform. Theory* **52**, 712 (2006).
- [76] B. R. McDonald, *Finite rings with identity*, (Marcel Dekker, New York, 1974).
- [77] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, “The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes,” *IEEE Trans. Inform. Theory* **40**, 301 (1994).
- [78] U. V. Linnik, “On the least prime in an arithmetic progression. I. The basic theorem,” *Rec. Math. [Mat. Sbornik] N.S.* **15(57)**, 139 (1944).

- [79] D. R. Heath-Brown, “Zero-free regions for Dirichlet  $L$ -functions, and the least prime in an arithmetic progression,” *Proc. London Math. Soc.* (3) **64**, 265 (1992).
- [80] P. Busch, P. J. Lahti and P. Mittelstaedt, *The Quantum Theory of Measurement* (Second edition, Springer-Verlag, Berlin, 1996).
- [81] C. M. Caves, “Quantum error correction and reversible operations,” *J. Supercond.* **12**, 707 (1999).
- [82] I. Daubechies, A. Grossmann and Y. Meyer, “Painless nonorthogonal expansions,” *J. Math. Phys.* **27**, 1271 (1986).
- [83] P. G. Casazza, M. Fickus, J. Kovačević, M. T. Leon and J. C. Tremain, “A physical interpretation for finite tight frames,” in C. Heil (Ed.), *Harmonic Analysis and Applications: In Honor of John J. Benedetto* (Birkhäuser, Boston, 2006).
- [84] S. Massar and S. Popescu, “Optimal extraction of information from finite quantum ensembles,” *Phys. Rev. Lett.* **74**, 1259 (1995).
- [85] N. Gisin and S. Massar, “Optimal quantum cloning machines,” *Phys. Rev. Lett.* **79**, 2153 (1997).
- [86] R. Derka, V. Bužek and A. K. Ekert, “Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement,” *Phys. Rev. Lett.* **80**, 1571 (1998).
- [87] J. I. Latorre, P. Pascual and R. Tarrach, “Minimal optimal generalized quantum measurements,” *Phys. Rev. Lett.* **81**, 1351 (1998).
- [88] D. Bruß and C. Macchiavello, “Optimal state estimation for  $d$ -dimensional quantum systems,” *Phys. Lett. A* **253**, 249 (1999).
- [89] J. Bae and A. Acín, “Asymptotic quantum cloning is state estimation,” *Phys. Rev. Lett.* **97**, 030402 (2006).
- [90] G. M. D’Ariano and P. Perinotti, “Optimal data processing for quantum measurements,” *Phys. Rev. Lett.* **98**, 020403 (2007).
- [91] Z. Hradil, “Quantum-state estimation,” *Phys. Rev. A* **55**, R1561 (1997).
- [92] K. Banaszek, G. M. D’Ariano, M. G. A. Paris and M. F. Sacchi, “Maximum-likelihood estimation of the density matrix,” *Phys. Rev. A* **61**, 010304 (1999).
- [93] K. R. W. Jones, “Principles of quantum inference,” *Ann. Phys.* **207**, 140 (1991).
- [94] V. Bužek, R. Derka, G. Adam and P. L. Knight, “Reconstruction of quantum states of spin systems: from quantum Bayesian inference to quantum tomography,” *Ann. Phys.* **266**, 454 (1998).
- [95] R. Schack, T. A. Brun, and C. M. Caves, “Quantum Bayes rule,” *Phys. Rev. A* **64**, 014305 (2001).
- [96] F. Tanaka and F. Komaki, “Bayesian predictive density operators for exchangeable quantum-statistical models,” *Phys. Rev. A* **71**, 052323 (2005).
- [97] R. Blume-Kohout, “Optimal, reliable estimation of quantum states,” arXiv:quant-ph/0611080.