arXiv:2311.13479v1 [quant-ph] 22 Nov 2023

Projective toric designs, difference sets, and quantum state designs

Joseph T. Iosue[*,‡], T. C. Mooney[†,‡], Adam Ehrenberg, and Alexey V. Gorshkov

Joint Center for Quantum Information and Computer Science, NIST/University of Maryland, College Park, Maryland 20742, USA

Joint Quantum Institute, NIST/University of Maryland, College Park, Maryland 20742, USA

November 21, 2023

Abstract

Trigonometric cubature rules of degree t are sets of points on the torus over which sums reproduce integrals of degree t monomials over the full torus. They can be thought of as t-designs on the torus. Motivated by the projective structure of quantum mechanics, we develop the notion of t-designs on the *projective* torus, which, surprisingly, have a much more restricted structure than their counterparts on full tori. We provide various constructions of these projective toric designs and prove some bounds on their size and characterizations of their structure. We draw connections between projective toric designs and a diverse set of mathematical objects, including difference and Sidon sets from the field of additive combinatorics, symmetric, informationally complete positive operator valued measures (SIC-POVMs) and complete sets of mutually unbiased bases (MUBs) (which are conjectured to relate to finite projective geometry) from quantum information theory, and crystal ball sequences of certain root lattices. Using these connections, we prove bounds on the maximal size of dense $B_t \bmod m$ sets. We also use projective toric designs to construct families of quantum state designs. Finally, we discuss many open questions about the properties of these projective toric designs and how they relate to other questions in number theory, geometry, and quantum information.

Contents

[*] jtiosue@umd.edu
[†] tmooney@umd.edu
[‡] These authors contributed equally to this work

1 Introduction

Given a measure space (M, μ) and a set of polynomials on M, a *t-design* on M is a measure space $(X \subset M, \nu)$ satisfying $\int_X f \, \mathrm{d}\nu = \int_M f \, \mathrm{d}\mu$ for all polynomials f of degree $\leq t$ [1–13]. Classic examples are Gaussian quadrature rules [1] and spherical designs [2,3], where the measure space M is the hypercube and hypersphere, respectively. Typically, one is interested in finding designs where X is a discrete measure space such that the integral over X with respect to ν reduces to a weighted sum that is often simpler to compute. However, this is not always possible; in the case of rigged designs (defined below), it is often crucial that X be a non-discrete measure space [14].

Specific forms of t-designs for particular choices of measure spaces M have found a plethora of uses in the field of quantum information theory [15–48]. In particular, complex projective space $\mathbb{CP}^{d-1}$ describes the space of d-dimensional quantum states [49], so t-designs on $M = \mathbb{CP}^{d-1}$ are called *complex-projective* or *quantum state t-designs*. These quantum state designs also relate to other mathematical objects such as symmetric, informationally complete positive operator valued measures (SIC-POVMs) and complete sets of mutually unbiased bases (MUBs), which themselves are conjectured to relate to finite projective geometry. Finite-dimensional quantum state designs can be generalized to designs on infinite-dimensional, or continuous-variable, quantum systems by defining *rigged quantum state t-designs*, which are designs on the space of tempered distributions $M = S(\mathbb{R})'$ [14]. Finally, the (projective) unitary group $\mathrm{PU}(d)$ describes the space of noiseless dynamics of quantum states, and these too admit constructions of *unitary t-designs*. Therefore a better understanding of various kinds of t-designs can also lead to deep insights about quantum information.

Consider the complex sphere Ω_d; that is, the set of unit vectors in $\mathbb{C}^d$. Any vector in Ω_d can be written (non-uniquely) as $|q, \phi\rangle \coloneqq \sum_{n=1}^{d} \sqrt{q_n} \mathrm{e}^{\mathrm{i}\phi_n} |n\rangle$, where $\{|n\rangle\}_{n=1}^{d}$ forms an orthonormal basis, $q = (q_n)_{n=1}^{d}$ is a discrete probability distribution ($\sum_n q_n = 1$), and $\phi = (\phi_n)_{n=1}^{d}$ is a set of phases. Therefore, q belongs to the $(d-1)$-simplex Δ^{d-1} and ϕ to the d-torus T^d. Via this mapping $\Delta^{d-1} \times T^d \to \Omega_d$, one can combine simplex designs and toric designs to form complex spherical designs [10]. Identifying $\mathbb{CP}^{d-1}$ with $\Omega_d/\mathrm{U}(1)$ (that is, quantum states are complex unit vectors with a global phase redundancy), we have a similar mapping $\Delta^{d-1} \times P(T^d) \to \mathbb{CP}^{d-1}$ defined as $(q, [\phi]) \mapsto [|q, \phi\rangle]$, where $P(T^d) = T^d/\mathrm{U}(1)$ is the projective torus (see Definition 3) and $[\cdot]$ denotes equivalence classes in the respective quotient spaces. In a similar way as before, via this mapping one can combine simplex designs and *projective toric designs* (see Definition 4) to form quantum state designs [11, 14].

In what follows, we flesh out and formalize this argument. Specifically, we formalize the notion of projective toric designs—both finite- and infinite-dimensional—and provide various constructions thereof. We discuss the connection between projective toric designs and difference sets [50–52], and use this correspondence to construct more projective toric designs, including some minimal ones. We illustrate the connection to quantum state designs and various other mathematical objects. Using minimal projective toric 2-designs, we construct an infinite family of almost-minimal complex-projective 2-designs. Finally, we discuss many exciting open questions regarding projective toric designs, some of which are deeply connected to long-outstanding conjectures in mathematics, such as some conjectures relating to finite affine and projective spaces.

Relation to prior work. Toric designs have been considered before. Trigonometric cubature rules are such designs on the torus [5–7]. Ref. [10] generalized the idea of trigonometric cubature to more general algebraic tori. Ref. [14] studied designs on projective tori and showed an equivalence to a specific case of Ref. [10], and further showed that such projective toric designs are related to complete sets of MUBs [53]. However we believe the presentation given in Section 2 gives new clarity and focus on the subject. Furthermore, Section 2.1 compiles, to the best of our knowledge, all previously known constructions of projective toric t-designs[1], and indeed generalizes some of these constructions.

The main novel contributions of our work lie in Sections 2.2, 3 and 4. In Section 2.2, we prove a general lower bound on the size of projective toric t-designs for all dimensions and all t by relating these designs to the crystal ball sequence corresponding to the root lattice A_{n-1} [54, 55]. In Section 3, we related difference sets to minimal projective toric designs. We show how the former can be used to construct the latter. Using the connection of difference sets to projective toric designs, we furthermore relate dense difference sets to

[1] Of course, many toric designs are known, and these always project to projective toric designs. Such constructions are not compiled in this manuscript.

the crystal ball sequence mentioned above, and derive new (to the best of our knowledge) bounds on the size of B_t mod m sets (*cf.* Corollary 18). In Section 4, we describe the relationship between projective toric designs and quantum state designs. This relationship was first noted in Refs. [10,14], though we believe that Section 4 greatly clarifies the details of this connection. In Section 4, we also construct an infinite family of *almost-minimal* quantum state 2-designs—that is, quantum state 2-designs of size exactly one more than minimal. While these specific almost-minimal designs have been noted before in Ref. [56], we arrive at the construction via an entirely different route that utilizes projective toric designs. We believe that this route has a much better hope of generalizing to other infinite families and $t > 2$.

Finally, Section 5 compiles a number of new interesting open problems involving projective toric designs, highlighting their connection to a number of other open problems in mathematics.

2 Theory of projective toric designs

We begin with some basic definitions that we will use for the rest of the paper.

Definition 1 (Torus)**.** *Let $T \coloneqq \mathbb{R}/2\pi\mathbb{Z}$. When $n \in \mathbb{N}$, let $I_n \coloneqq \{1, 2, \dots n\}$; when $n = \infty$, let $I_n = I_\infty \coloneqq \mathbb{N}$. For such n, let $T^n \coloneqq \prod_{i\in I_n} T$ with the product topology. Define the projection maps $p_i\colon T^n \to T$ as $(\phi_j)_{j\in I_n} \mapsto \phi_i$. For all $n \in \mathbb{N} \cup \{\infty\}$, let μ_n denote T^n's unit-normalized Haar measure.*

Note that by Tychonoff's theorem, T^∞ is compact. For all n, T^n is therefore a compact abelian group and thus has a unique unit-normalized Haar measure.

By definition, the product topology on T^∞ is the coarsest topology such that the projection maps p_i are continuous. Similarly, we endow T^∞ with the smallest σ-algebra such that the projections p_i are measurable. This σ-algebra is generated by sets of the form $A = \prod_{i\in\mathbb{N}} A_i$, where each A_i is a measurable subset of T and all but finitely many A_i are equal to T. Define a measure μ' on T^∞ by $\mu'(A) = \prod_{i\in\mathbb{N}} \mu_1(A_i)$. From Ref. [57, Thm. 10.6.1] (or Ref. [58] for a shorter proof), this definition of μ' on such subsets uniquely determines μ' on the whole space. Clearly μ' is transitionally-invariant and unit-normalized, and therefore $\mu' = \mu_\infty$.

We now define trigonometric cubature rules [5–7], which are designs on the torus. To match the general terminology of this paper, we prefer to use the term *toric design.*

Definition 2 (Toric design)**.** *A T^n* t-design *(or trigonometric cubature rule of dimension n and degree t [5–7]) is a measure space $(X \subset T^n, \Sigma, \nu)$ such that*

$$\int_X \exp\left(\mathrm{i}\sum_{j=1}^n \alpha_j\phi_j\right) \mathrm{d}\nu(\phi) = \int_{T^n} \exp\left(\mathrm{i}\sum_{j=1}^n \alpha_j\phi_j\right) \mathrm{d}\mu_n(\phi) \tag{1}$$

for all $\alpha \in \mathbb{Z}^n$ satisfying $\sum_{j=1}^n |\alpha_j| \le t$.

We now consider the projective torus, an important object in the study of quantum mechanics because it removes a global phase redundancy (see Section 4).

Definition 3 (Projective torus)**.** *Let $P(T^n)$ denote the* projective torus *$P(T^n) \coloneqq T^n/T$, where here T denotes the inclusion $T \hookrightarrow T^n$ by $T \ni \theta \mapsto (\theta, \theta, \dots) \in T^n$.*

In other words, $P(T^n)$ is the set points in T^n identified up to a constant additive factor. Clearly, for any $f : T^n \to \mathbb{C}$ to descend to a well-defined function on $P(T^n)$ it must be constant on the cosets of the diagonal subgroup; in other words, it must satisfy $f(\mathrm{e}^{\mathrm{i}\phi_1+\mathrm{i}\theta}, \mathrm{e}^{\mathrm{i}\phi_2+\mathrm{i}\theta}, \dots) = f(\mathrm{e}^{\mathrm{i}\phi_1}, \mathrm{e}^{\mathrm{i}\phi_2}, \dots)$ for all $\theta \in T$. Hence, when studying designs on $P(T^n)$, we need only consider monomials on T^n where the degree and conjugate degree are equal. A degree t monomial on $P(T^n)$ therefore lifts to $\exp\left(\mathrm{i}\sum_{k=1}^t(\phi_{a_k} - \phi_{b_k})\right)$ for $a, b \in I_n^t$. We are thus now in a position to define a $P(T^n)$ t-design.

Definition 4 (Projective toric design)**.** *Fix an $n \in \mathbb{N} \cup \{\infty\}$ and $t \in \mathbb{N}$. Let $X \subset P(T^n)$ and (X, Σ, ν) be a measure space. X is called a* $P(T^n)$ t-design *if for all $a, b \in I_n^t$,*

$$\int_X \exp\left(\mathrm{i}\sum_{j=1}^t(\phi_{a_j} - \phi_{b_j})\right) \mathrm{d}\nu(\phi) = \int_{P(T^n)} \exp\left(\mathrm{i}\sum_{j=1}^t(\phi_{a_j} - \phi_{b_j})\right) \mathrm{d}\mu_{n-1}(\phi). \tag{2}$$

Here we denote the unit-normalized Haar measure on $P(T^n)$ as simply μ_{n-1} since $P(T^n) \cong T^{n-1}$. X is called discrete *if ν is a counting measure, and is called* finite *if it is discrete and $|X| < \infty$. If X is finite, then $|X|$ is called the* size *of X.*

Clearly a $P(T^n)$ t-design is also a $(t-1)$-design, since we can let $a_t = b_t$ and have the integrand become an arbitrary degree $(t-1)$ monomial. Additionally, a $P(T^n)$ t-design is also a $P(T^{n-1})$ t-design, as can be seen by picking a subset of indices. We note that in the language of Ref. [10], a $P(T^n)$ designs is a design on the algebraic torus $T(\mathrm{PSU}(n))$. It was shown in Ref. [14] that the two notions coincide[2].

Throughout this work, we will use double braces to denote multisets, whereas single braces will denote sets as usual; that is, $\{\!\{1,2,2\}\!\} = \{\!\{2,1,2\}\!\} \neq \{\!\{1,2\}\!\}$, whereas $\{1,2,2\} = \{1,2\} = \{2,1\}$. Since the integrand in Eq. (2) contains only a finite number of projection maps, we can use Fubini's theorem to compute the integral on the right-hand side. By choosing a set of representatives of $P(T^n)$ to be those phases ϕ for which $p_1(\phi) = \phi_1 = 0$, we can think of $P(T^n)$ as $\{0\} \times T^{n-1}$. In this way, we have that $p_1(\phi) = 0$ for all ϕ. It follows that $X \subset \{0\} \times T^{n-1}$ is a $P(T^n)$ t-design if

$$\int_X \exp\left(\mathrm{i}\sum_{j=1}^{t}(\phi_{a_j} - \phi_{b_j})\right) \mathrm{d}\nu(\phi) = \int_{\{0\}\times T^{n-1}} \exp\left(\mathrm{i}\sum_{j=1}^{t}(\phi_{a_j} - \phi_{b_j})\right) \mathrm{d}\mu_{n-1}(\phi) \tag{3a}$$

$$= \begin{cases} 1 & \text{if } \{\!\{a_i \mid i \in \{1,\dots,t\}\}\!\} = \{\!\{b_i \mid i \in \{1,\dots,t\}\}\!\} \\ 0 & \text{otherwise} \end{cases}. \tag{3b}$$

Suppose that we set each $b_j = 1$. It follows that X must match integration of polynomials on T^{n-1} of degree t and conjugate degree 0 (because $\phi_{b_j} = 0$). Similarly, we can set each $a_j = 1$, and thus X must match integration of degree 0 and conjugate degree t. More generally, we see that it must match on monomials on T^{n-1} of degree (t_1, t_2) whenever $t_1 \leq t$ and $t_2 \leq t$. It follows that a T^{n-1} $(2t)$-design is a $P(T^n)$ t-design, and a $P(T^n)$ t-design is a T^{n-1} t-design. The reverse implications, however do not hold in general.

By linearity, a $P(T^n)$ t-design exactly integrates all polynomials on $P(T^n)$ of degree t or less. It is the projective nature of the polynomials that we are integrating that give projective toric designs their interesting structure that is quite different than the structure of toric designs. For example, as we will see, for finite n, $P(T^n)$ 2-designs must be of size at least $n(n-1)+1$, and indeed this can be saturated for many n; in contrast, it is known that a T^n 4-design requires size at least $2n^2$, 3-design requires at least $4n$ points (which can often be achieved), and 2-design requires at least $2n$ points (and $2n+1$ can often be achieved) [6]. Indeed, the difference between toric designs (*i.e.* trigonometric cubature rules) and projective toric designs is analogous to the difference between (complex) spherical designs and (complex) projective designs.

2.1 Constructions of projective toric designs

In this section, we will present a few simpler constructions in order to get a handle on projective toric designs. Later, in Section 3, we will construct more (and smaller) projective toric t-designs by utilizing difference sets and Sidon sets from additive combinatorics [50]. Throughout this section, we will write points in $P(T^n)$ as representatives in T^n with the first entry set to 0.

Our first example is a $P(T^n)$ 2-design of size n^2 whenever n is prime, and slightly larger when n is not prime. Note that this construction can be generalized to be size n^2 whenever n is a prime power, but we do not do this here. The generalized construction can be seen in the phases in the complete set of MUBs in prime-power dimensions given in Ref. [18].

Theorem 5 (Thm. C.9 of [14])**.** *Let $n \in \mathbb{N}$. Define p to be the smallest prime number strictly larger than $\max(2,n)$ (by the prime number theorem, $p \in \mathcal{O}(n + \log n)$). Let $X \subset T^n$ be the set*

$$X = \left\{ \left(0, 2\pi(q_1+q_2)/p, 2\pi(2q_1+4q_2)/p, \dots, 2\pi((n-1)q_1+(n-1)^2 q_2)/p\right) \mid q_1 \in \mathbb{Z}_p, q_2 \in \mathbb{Z}_p \right\} \tag{4}$$

and v the constant map[3] *$v(\phi) = 1/|X|$. Then X with the counting measure weighted by v is a $P(T^n)$ 2-design.*

[2] We note that Ref. [14] refers to $P(T^n)$ designs as T^n designs.

[3] We corrected a minor error in Thm. C.9 of [14]. Namely, the map v was stated as $v(\phi) = 1/p^2$. This is correct for all $n > 2$, as $|X| = p^2$. However, when $n = 2$, $|X| = p = 3$.

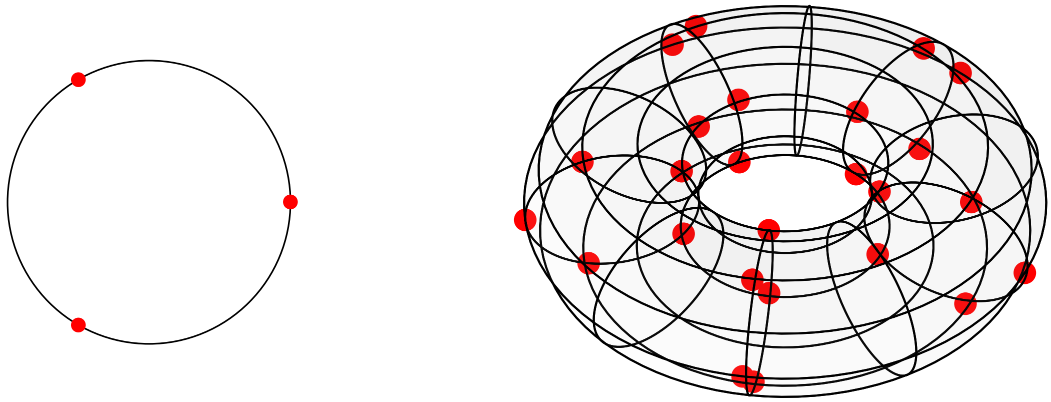

Figure 1: The construction of the 2-design in Theorem 5 for (left) $n = 2$ with $p = 3$ and (right) $n = 3$ with $p = 5$. Note we are representing points in $P(T^n)$ here as points in T^{n-1} by discarding the first coordinate which we fix to 0. The number of points in the design for (left) $n = 2$ is p and for (right) $n = 3$ is $p^2 = 25$.

We can easily write out the construction for $n = 2$, where we have $p = 3$, and therefore $X = \{(0, 0), (0, 2\pi/3), (0, 4\pi/3)\}$ with weight $v(\phi) = 1/3$ is a $P(T^2)$ 2-design. We show the construction in Fig. 1 for this example of $n = 2$ with $p = 3$ as well as for $n = 3$ with $p = 5$.

We can extend this construction to the case when $n = \infty$.

Theorem 6. *Let $X \subset T^\infty$ be the set*

$$X = \left\{\left(0, \vartheta + \varphi, 2\vartheta + 4\varphi, \ldots, j\vartheta + j^2\varphi, \ldots\right) \mid \vartheta, \varphi \in [0, 2\pi]\right\} \tag{5}$$

and ν the unit normalized Lebesgue measure on $[0, 2\pi]^2$ (i.e. $\mathrm{d}\nu = \mathrm{d}\vartheta\,\mathrm{d}\varphi/(2\pi)^2$). Then X is a T^∞ 2-design.

Proof. For any $a, b, c, d \in \mathbb{N}$,

$$\int_X \exp(\mathrm{i}(\phi_a + \phi_b - \phi_c - \phi_d))\,\mathrm{d}\nu(\phi) = \int_{[0,2\pi]^2} \exp\left(\mathrm{i}\vartheta(a + b - c - d) + \mathrm{i}\varphi(a^2 + b^2 - c^2 - d^2)\right) \frac{\mathrm{d}\vartheta\,\mathrm{d}\varphi}{(2\pi)^2} \tag{6a}$$

$$= \begin{cases} 1 & \text{if } a + b = c + d \ \wedge \ a^2 + b^2 = c^2 + d^2 \\ 0 & \text{otherwise} \end{cases} \tag{6b}$$

$$= \begin{cases} 1 & \text{if } \{\!\{a, b\}\!\} = \{\!\{c, d\}\!\} \\ 0 & \text{otherwise} \end{cases}, \tag{6c}$$

where in the last line we used [14, Lem. C.10]. $\square$

We now consider a construction for arbitrary t.

Theorem 7 (Thm. C.8 of [14])**.** *Let $n \in \mathbb{N}$, $t \in \mathbb{N}$, $X \subset T^n$ be the set*

$$X = \left\{(0, 2\pi d_1/(t + 1), 2\pi d_2/(t + 1), \ldots, 2\pi d_{n-1}/(t + 1)) \mid d \in \mathbb{Z}_{t+1}^{n-1}\right\}, \tag{7}$$

and v be the constant map $v(\phi) = (t+1)^{-(n-1)}$. Then X with the counting measure weighted by v is a $P(T^n)$ t-design.

Example 8 ($n = 2$, $t = 3$)**.** We have

$$\begin{aligned} X = \Bigg\{ & (0, 0, 0), \left(0, 0, 2\pi\frac{1}{3}\right), \left(0, 2\pi\frac{1}{3}, 0\right), \left(0, 0, 2\pi\frac{2}{3}\right), \left(0, 2\pi\frac{2}{3}, 0\right), \\ & \left(0, 2\pi\frac{1}{3}, 2\pi\frac{2}{3}\right), \left(0, 2\pi\frac{2}{3}, 2\pi\frac{1}{3}\right), \left(0, 2\pi\frac{1}{3}, 2\pi\frac{1}{3}\right), \left(0, 2\pi\frac{2}{3}, 2\pi\frac{2}{3}\right) \Bigg\}, \end{aligned} \tag{8}$$

with $v(\phi) = 1/9$, is a $P(T^3)$ 2-design. $\diamond$

We now extend this construction to $n = \infty$.

Theorem 9. *Let $t \in \mathbb{N}$ and $X_1 \subset T$ be the discrete probability space $X_1 = \{2\pi d/(t+1) \mid d \in \mathbb{Z}_{t+1}\}$. Let $X = \prod_{i\in\mathbb{N}} X_1$ and its σ-algebra be generated by sets of the form $\prod_{i\in\mathbb{N}} A_i$ where each A_i in the power set $A_i \in \mathcal{P}(X_1)$ and for all but finitely many i we have $A_i = X_1$. Define ν by its action $\nu(A) = \prod_{i\in\mathbb{N}}(|A_i| / |X_1|)$, and note that ν uniquely extends to a measure on X [57, Thm. 10.6.1]. Then X is a T^∞ t-design.*

Proof. Let $m = \max(\max_j a_j, \max_j b_j)$. Since t is finite, we are only ever dealing with a finite number of projection maps p_i in the integrand. Therefore, we can apply Fubini's theorem to separate the integral $\int_X$ into a product of an integral over X_1^m and an integral over the rest of the space. Hence,

$$\int_X \exp\left(\mathrm{i}\sum_{j=1}^{t}(\phi_{a_j} - \phi_{b_j})\right) \mathrm{d}\nu(\phi) = \frac{1}{|\mathbb{Z}_{t+1}^m|}\sum_{d\in\mathbb{Z}_{t+1}^m} \exp\left(\frac{2\pi\mathrm{i}}{t+1}\sum_{j=1}^{t}(d_{a_j} - d_{b_j})\right) \tag{9a}$$

$$= \begin{cases} 1 & \text{if } \{\!\{a_j \mid j \in \{1,\ldots,t\}\}\!\} = \{\!\{b_j \mid j \in \{1,\ldots,t\}\}\!\} \\ 0 & \text{otherwise} \end{cases}. \tag{9b}$$

□

Finally, for completeness, we note the asymptotic existence theorem proven in Ref. [10].

Theorem 10 (Thm. 3.3 and Cor. 5.4 of [10])**.** *Asymptotically in $n \to \infty$ but for finite n, a $P(T^n)$ t-design must have size at least $\frac{n^t(1-o(1))}{\lceil t/2\rceil!\lfloor t/2\rfloor!}$ and there exists t-designs of size $n^t(1 + o(1))$.*

2.2 Minimal projective toric designs

A very natural question that one can ask is *what is the size of the smallest projective toric t-design?* We call such designs *minimal*. Ref. [14, Prop. C.11] proved a lower bound on the size of minimial projective toric 2-designs. In Section 3, we will show that this bound can be saturated in many dimensions. In this section, we generalize the bound and prove a lower bound on the size of minimal projective toric t-designs. In the case when t is even, we conjecture that this bound is tight.

We begin by defining the set

$$P_s^{(n)} := \left\{\mathbf{q} - \mathbf{r} \;\middle|\; \mathbf{q}, \mathbf{r} \in \mathbb{N}_0^n,\; \sum_{i=1}^{n} q_i = \sum_{i=1}^{n} r_i = s\right\}. \tag{10}$$

We show that $|P_s^{(n)}|$ is the s^{th} element of the crystal ball sequence corresponding to the root lattice A_{n-1} [54, 55], and therefore arrive at the explicit formula for $|P_t^{(n)}|$ given in Eq. (11). We begin by defining the crystal ball sequence of A_{n-1}. Let $S_{n-1}(t)$ denote the number of vertices of A_{n-1} a distance t away from some fixed vertex, where we define distance for the lattice A_{n-1} as follows: letting $\mathcal{R} := \{\mathbf{e}_i - \mathbf{e}_j \mid i, j \in \{1,\ldots,n\}\}$ be the roots of A_{n-1}, the distance between $\mathbf{x}, \mathbf{y} \in A_{n-1}$ is the smallest d such that $\mathbf{x} - \mathbf{y} \in d\mathcal{R}$, where $d\mathcal{R} := \mathcal{R} + \mathcal{R} + \cdots + \mathcal{R}$ is the d-fold set sum of $\mathcal{R}$. The sequence $(S_{n-1}(t))_{t\in\mathbb{N}_0}$ is the *coordination sequence* of A_{n-1} [54]. The *crystal ball numbers* are the partial sums $G_{n-1}(s) = \sum_{x=0}^{s} S_{n-1}(x)$ [54]. The explicit formula for $G_{n-1}(t)$ is [54, 55]

$$G_{n-1}(t) = {}_3F_2(1-n, -t, n; 1, 1; 1) = \sum_{i=0}^{t} \binom{n-1}{i}^2 \binom{n-i+t-1}{t-i}, \tag{11}$$

where ${}_3F_2$ denotes the generalized hypergeometric function [59–62].

Lemma 11. $|P_s^{(n)}| = G_{n-1}(s)$.

Proof. Let $\{\mathbf{e}_j\}_{j=1}^n$, and $\mathcal{R}$ be as above. Now, let $\mathcal{R}_j := \{\mathbf{e}_i - \mathbf{e}_j \mid i \in \{1,\ldots,n\}\}$. Let $\mathbf{q}, \mathbf{r} \in \mathbb{N}_0^n$ be defined as in Eq. (10). Note that $\mathbf{q}, \mathbf{r} \in s\mathbf{e}_1 + s\mathcal{R}_1$. Further, note that $\mathcal{R}_1 - \mathcal{R}_1 = \mathcal{R}$. Thus,

$$\mathbf{q} - \mathbf{r} \in s\mathbf{e}_1 + s\mathcal{R}_1 - (s\mathbf{e}_1 + s\mathcal{R}_1) = s\mathcal{R}_1 - s\mathcal{R}_1 = s(\mathcal{R}_1 - \mathcal{R}_1) = s\mathcal{R}. \tag{12}$$

Thus, we have an injection from $P_s^{(n)}$ into $s\mathcal{R}$. Note also that $G_{n-1}(s) = |s\mathcal{R}|$, since $|s\mathcal{R}|$ is precisely the set of all points that are reachable within a path of at most s edges. Thus, we now need only show that this map is actually also a surjection.

To do this, note that for any $\mathbf{x} = \sum_{l=1}^{s}(\mathbf{e}_{i_l} - \mathbf{e}_{j_l}) \in s\mathcal{R}$, we can easily reverse this chain by letting $\mathbf{q} = s\mathbf{e}_1 + \sum_{l=1}^{s}(\mathbf{e}_{i_l} - \mathbf{e}_1)$ and $\mathbf{r} = s\mathbf{e}_1 + \sum_{l=1}^{s}(\mathbf{e}_{j_l} - \mathbf{e}_1)$. Thus, all $\mathbf{x} \in s\mathcal{R}$ also satisfy $\mathbf{x} \in P_s^{(n)}$ and vice versa, meaning that the two sets are equal, and thus that their cardinalities are as well. □

We recall that Ref. [14] showed the equivalence of $P(T^n)$ designs and designs on the algebraic torus $T(\mathrm{PSU}(n))$ as defined in Ref. [10]. Ref. [10] further explored the connection between such designs and the root lattice of $\mathrm{PSU}(n)$, which is A_{n-1}. This gives a hint as to why A_{n-1} shows up in the analysis of projective toric designs.

We now prove a lower bound on the size of projective toric designs. We note that this bound is compatible with the asymptotic bound given in Theorem 10. One can see this by using the asymptotic expansion of the binomial coefficients in Eq. (11).

Proposition 12. *Let $n \in \mathbb{N}$ and (X, Σ, ν) be a finite $P(T^n)$ t-design. Then $|X| \geq G_{n-1}(\lfloor t/2 \rfloor)$, where $G_{n-1}(s)$ is given in Eq. (11).*

Proof. We prove the bound for even t. The bound for odd t is then automatically valid since the minimal size of a $(t+1)$-design is at least as large as the minimal size of a t-design. We therefore restrict our attention to even t for the rest of the proof.

Since X is a finite, discrete measure space, we can rewrite $\int_X (\cdot)\,\mathrm{d}\nu$ as $\sum_{\phi \in X} v(\phi)(\cdot)$. The projective toric t-design condition can be expressed as follows. Let each $\phi \in X$ label a basis element of $V := \mathbb{C}^{|X|}$ so that $\{|\phi\rangle \mid \phi \in X\}$ is an orthonormal basis of V. Then for $\mathbf{k} \in P_{t/2}^{(n)}$, define $|\mathbf{k}\rangle = \sum_{\phi \in X} \sqrt{v(\phi)} \mathrm{e}^{\mathrm{i}\mathbf{k}\cdot\phi} |\phi\rangle$. The t-design condition is equivalently stated as $\langle \mathbf{k}|\mathbf{k}'\rangle = \delta_{\mathbf{k},\mathbf{k}'}$. Hence, $\{|\mathbf{k}\rangle \mid \mathbf{k} \in P_{t/2}^{(n)}\}$ must be orthonormal in V, meaning that $|P_{t/2}^{(n)}| \leq \dim V = |X|$. The proposition then follows from Lemma 11. □

Furthermore, we can prove that a minimal t-design for even t must be uniformly weighted.

Proposition 13. *Let $X \subset P(T^n)$ and let $v \colon X \to (0, \infty)$ define a weighted discrete measure on X. Suppose the measure space defined by X and v is a minimal t-design with t even. Then $v(\theta) = 1/|X|$.*

Proof. This proof essentially follows that of Ref. [6, Thm. 2.2]. The $P(T^n)$ t-design condition is written as $MM^\dagger = \mathbb{I}_{|P_{t/2}^{(n)}| \times |P_{t/2}^{(n)}|}$, where $M_{\mathbf{k},\theta} = \sqrt{v(\theta)}\mathrm{e}^{\mathrm{i}\mathbf{k}\cdot\theta}$. If X is minimal—that is, if $|X| = |P_{t/2}^{(n)}|$—then M is a square matrix so that $MM^\dagger = \mathbb{I}$ if and only if $M^\dagger M = \mathbb{I}$. From the latter condition, it follows that $\delta_{\theta,\theta'} = \sqrt{v(\theta)v(\theta')} \sum_{k \in P_{t/2}^{(n)}} \mathrm{e}^{\mathrm{i}\mathbf{k}\cdot(\theta-\theta')}$. When $\theta = \theta'$, we therefore find that $v(\theta) = 1/|P_{t/2}^{(n)}| = 1/|X|$. □

Finally, we conjecture that the bound given in Proposition 12 is tight for even t.

Conjecture 14. *When t is even, the bound given in Proposition 12 is tight in the sense that there are infinitely many dimensions n for which the bound is saturable.*

In Section 3, we show how minimal t-designs are related to difference sets. Using this connection, we construct an infinite family of minimal 2-designs that indeed saturate the bound given in Proposition 12, and we derive a bound on the size of dense difference sets.

3 Relation to difference sets

We say that $X \subset P(T^n)$ is a *group toric t-design* if X is a t-design and also inherits group structure from $P(T^n)$. We will consider the case when X is a cyclic group for finite n and a circle group for $n = \infty$. Here we will find connections to Sidon sets and difference sets [50].

We begin with the infinite case. Suppose that $X \subset T^\infty$ is a t-design and isomorphic to the circle group U(1). Then there is a single element $z \in \mathbb{Z}^\infty$ such that $X = \{\theta z = (\theta z_1, \theta z_2, \dots) \mid \theta \in [0, 2\pi]\}$. In order for X to be a design, it must be that

$$\int_0^{2\pi} \exp\left(\mathrm{i}\theta \sum_{j=1}^{t} (z_{a_j} - z_{b_j})\right) \frac{\mathrm{d}\theta}{2\pi} = \begin{cases} 1 & \text{if } \{\!\{a_j \mid j \in \{1, \dots, t\}\}\!\} = \{\!\{b_j \mid j \in \{1, \dots, t\}\}\!\} \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

for all $a, b \in \mathbb{N}^t$. It follows that z must satisfy

$$\left(\sum_{j=1}^{t} z_{a_j} = \sum_{j=1}^{t} z_{b_j}\right) \iff \left(\{\!\{a_j \mid j \in \{1, \dots, t\}\}\!\} = \{\!\{b_j \mid j \in \{1, \dots, t\}\}\!\}\right). \tag{14}$$

In other words, the sum of any t elements of z must be unique. If we restrict z to be in $\mathbb{Z}^\infty_{\geq 0}$, then Eq. (14) is exactly the condition for z to be a *B_t set*[4] [50, Def. 4.27]. In the special case of $t = 2$, we need to find a $z \in \mathbb{Z}^\infty_{\geq 0}$ such that $z_a + z_b = z_c + z_d$ if and only if $\{\!\{a, b\}\!\} = \{\!\{c, d\}\!\}$. Such a z is called a *Sidon set* [50].

We have therefore proven the following proposition.

Proposition 15. *Group T^∞ t-designs isomorphic to the circle group are in one-to-one correspondence with B_t sets.*

We next give a simple example of a B_t set.

Example 16 (Exponential B_t set)**.** Let $S \in \mathbb{Z}^\infty$ be defined by $z_a = t^a$. In this case, z_a written in base t is $100\dots0$, a 1 followed by a 0s. It follows easily that every sum is unique up to reordering. ⋄

We now discuss finite n. Suppose that $X \subset P(T^n)$ is a t-design and isomorphic to the cyclic group $\mathbb{Z}_m$. It follows that X is a size m t-design and is generated by a fixed $z \in \mathbb{Z}_m^n$. In order for X to be a design, it must be that

$$\sum_{d=0}^{m-1} \exp\left(\frac{2\pi \mathrm{i} d}{m} \sum_{j=1}^{t} (z_{a_j} - z_{b_j})\right) = \begin{cases} 1 & \text{if } \{\!\{a_j \mid j \in \{1, \dots, t\}\}\!\} = \{\!\{b_j \mid j \in \{1, \dots, t\}\}\!\} \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

for all $a, b \in I_n^t$, where recall that $I_n = \{1, 2, \dots, n\}$. It follows that z must satisfy

$$\left(\sum_{j=1}^{t} z_{a_j} \equiv \sum_{j=1}^{t} z_{b_j} \pmod{m}\right) \iff \left(\{\!\{a_j \mid j \in \{1, \dots, t\}\}\!\} = \{\!\{b_j \mid j \in \{1, \dots, t\}\}\!\}\right). \tag{16}$$

In other words, the sum of any t elements of z must be unique, or equivalently,

$$\left| \left\{ \sum_{j=1}^{t} z_{a_j} \bmod m \mid a \in I_n^t \right\} \right| = \binom{n+t-1}{t}. \tag{17}$$

Eq. (16) is precisely the condition for z to be a *B_t mod m set of size n* [50]. We have therefore shown the following proposition.

Proposition 17. *Group $P(T^n)$ t-designs isomorphic to the cyclic group $\mathbb{Z}_m$ are in one-to-one correspondence with B_t mod m sets of size n.*

Given Proposition 17 and the bound in Proposition 12, we immediately arrive at the following corollary.

Corollary 18. *Any B_t mod m set must have size n satisfying $m \geq G_{n-1}(\lfloor t/2 \rfloor)$, where $G_{n-1}(s)$ is given in Eq. (11). Furthermore, if Conjecture 14 is true, then this bound is tight for even t in the sense that there are infinitely many dimensions n for which the bound is saturable.*

[4] Note that we are considering z to be a tuple and yet calling it a difference "set". It is understood that we are talking about the set $\{z_a \mid a \in \mathbb{N}\}$.

We have been unable to find the bound in Corollary 18 in the existing literature on difference sets. If this bound is indeed new, it illustrates the utility of studying projective toric designs due to the many interesting mathematical objects to which they relate.

In the special case of $t = 2$, $B_{t=2}$ mod m sets are called a *Sidon sets of size n mod m*. Notably, by a simple counting argument, any Sidon set of size n mod m must satisfy $m \geq n(n-1)+1$.[5] Further, for many but not all n, this bound can be saturated, as we will discuss later. When the bound is saturated, we say the Sidon set is *dense*. Hence, for every n for which there is a Sidon set of size n mod $n(n-1)+1$, there is a *minimal* $P(T^n)$ 2-design—that is, a $P(T^n)$ 2-design of size $n(n-1)+1$, hence saturating the lower bound from Proposition 12.

For one example of a dense Sidon set, consider $n = 6$ and $m = G_{n-1}(1) = n(n-1)+1 = 31$. Then one can easily check that $z = (0, 1, 3, 8, 12, 18)$ is a Sidon set and thus gives rise to a $P(T^6)$ 2-design of size 31. A simple numerical search however reveals that there does not exist a Sidon set of size 7 mod $7(7-1)+1 = 43$. Therefore, we have the following corollary.

Corollary 19. *Either there are no $P(T^7)$ 2-designs of size saturating the lower bound given in Proposition 12, or such a saturating design cannot be isomorphic to a cyclic group.*

3.1 Explicit families of designs from Singer sets

There is a general construction of dense Sidon sets—called Singer sets—whenever $n-1$ is a prime power [63]. Thus, we have constructed minimal $P(T^n)$ 2-designs whenever $n-1$ is a prime power, and these designs are isomorphic to the cyclic group $\mathbb{Z}_{n(n-1)+1}$. We review the Singer set construction in Appendix A.

Indeed more generally, we review Singer's construction in Lemma A.2 of B_t mod $\frac{(n-1)^{t+1}-1}{n-2}$ sets of size n whenever $n-1$ is a prime power. Using Proposition 17, we have therefore constructed explicit $P(T^n)$ t-designs of size $\frac{(n-1)^{t+1}-1}{n-2}$ whenever $n-1$ is a prime power, and these designs are isomorphic to the cyclic group $\mathbb{Z}_{\frac{(n-1)^{t+1}-1}{n-2}}$.

4 Relation to quantum state designs

Projective toric designs are closely connected to complex-projective designs [15–26], continuous-variable (CV) rigged designs [14], and complete sets of mutually unbiased bases (MUBs) [53]. These connections arise by concatenating toric and simplex designs in order to generate elements in complex-projective space, which in turn satisfy the design condition. We discuss the connection here.

Denote the complex unit sphere by $\Omega_d = \{z \in \mathbb{C}^d \mid \sum_{i=1}^d |z_i|^2 = 1\}$, which can be identified with S^{2d-1}. Let $\mathbb{CP}^{d-1}$ be complex-projective space $\Omega_d/\mathrm{U}(1)$. Pick an orthonormal basis $\{|n\rangle \mid n \in \{1,\ldots,d\}\}$ of $\mathbb{C}^d$. A polynomial f on Ω_n descends to a well-defined polynomial on $\mathbb{CP}^{d-1}$ if and only if it is invariant under the action of U(1)—that is, $f(\mathrm{e}^{\mathrm{i}\theta}|\psi\rangle) = f(|\psi\rangle)$ for all θ and $|\psi\rangle \in \Omega_d$. It follows that all degree t monomials on $\mathbb{CP}^{d-1}$ are of the form $\prod_{i=1}^t \langle a_i|\psi\rangle\langle\psi|b_i\rangle$ for $a, b \in I_d^t$ (recall that $I_d = \{1, 2, \ldots, d\}$). A $\mathbb{CP}^{d-1}$ t-design is thus a measure space (X, Σ, ν) such that, for all $a, b \in I_d^t$,

$$\int_X \left(\prod_{i=1}^t \langle a_i|\psi\rangle\langle\psi|b_i\rangle\right) \mathrm{d}\nu(\psi) = \int_{\mathbb{CP}^{d-1}} \left(\prod_{i=1}^t \langle a_i|\psi\rangle\langle\psi|b_i\rangle\right) \mathrm{d}\psi = \frac{\Pi_t^{(d)}(a;b)}{\operatorname{Tr}\Pi_t^{(d)}}, \tag{18}$$

where $\Pi_t^{(d)}$ is the projector onto the symmetric subspace of $(\mathbb{C}^d)^{\otimes t}$, $\Pi_t^{(d)}(a;b) := \left(\bigotimes_{i=1}^t \langle a_i|\right) \Pi_t^{(d)} \left(\bigotimes_{i=1}^t |b_i\rangle\right)$, and $\mathrm{d}\psi$ denotes the Fubini-Study volume measure on $\mathbb{CP}^{d-1}$. The last equality is a simple consequence of Schur's lemma and the unitary invariance of $\mathrm{d}\psi$ [22, 24] [14, Ap. C3].

Let $\Delta^{d-1} = \{p \in [0,1]^d \mid \sum_{i=1}^d p_i = 1\}$ denote the $(d-1)$-dimensional simplex. Simplex t-designs have analogous definitions to those of toric and complex-projective designs [4, 8–11]. Any vector $|\psi\rangle \in \Omega_n$ can be represented as $|p,\phi\rangle := \sum_{n=1}^d \sqrt{p_n}\mathrm{e}^{\mathrm{i}\phi_n}|n\rangle$ for some (not necessarily unique) $p \in \Delta^{d-1}$ and $\phi \in T^d$. For a

[5] The Sidon set condition can be restated as stipulating that $z_a - z_c \equiv z_d - z_b$ if and only if $\{\!\{a,b\}\!\} = \{\!\{c,d\}\!\}$. We therefore need $z_a - z_c$ to be unique for all a and c. First choose an $a \in I_n$ and then choose a $c \in I_n$ with $c \neq a$. This gives us $n(n-1)$ distinct values. Further, we have one more value—namely 0—coming from when $a = c$.

complex unit vector $|\psi\rangle \in \Omega_n$, let $[|\psi\rangle]$ denote the equivalence class corresponding to a point in $\mathbb{CP}^{d-1}$. Let $\pi\colon \Delta^{d-1} \times P(T^d) \to \mathbb{CP}^{d-1}$ be defined by $(p,\phi) \mapsto [|p,\phi\rangle]$, where ϕ is any representative of an equivalence class in T^d/T. The pullback of the Fubini-Study volume form along π is precisely the Lebesgue measure on Δ^{d-1} times the Lebesgue measure on $P(T^d)$ (see Appendix B). Together, this implies that the concatenation of a Δ^{d-1} t-design and a $P(T^d)$ t-design yields a $\mathbb{CP}^{d-1}$ t-design [10, 14].

We note that the analogous result holds for the complex sphere Ω_d; namely, concatenation of a Δ^{d-1} t-design and a toric $(2t)$-design (see Definition 2) yields a Ω_d t-design. The reason that we only need a projective toric design in the $\mathbb{CP}^{d-1}$ case, as opposed to a full toric design as in the Ω_d case, is because polynomials on $\mathbb{CP}^{d-1}$ are more restricted than on Ω_d. On Ω_d, $z_1 z_2 \bar{z}_3$ is a valid monomial. On the other hand, this is an invalid monomial on $\mathbb{CP}^{d-1} = \Omega_d/\mathrm{U}(1)$ since it varies under the action of $\mathrm{U}(1)$.

One particularly nice simplex 2-design contains the extremal points $(1,0,\ldots,0),\ldots,(0,0,\ldots,1)$ and the centroid $c = (1/d, 1/d, \ldots, 1/d)$ (see e.g. [14, Thm. C4]). When concatenating the extremal points with a projective toric design, we get the basis vectors $[|n\rangle] \in \mathbb{CP}^{d-1}$. When concatenating the centroid with a finite-sized projective toric design X, we get a collection of points $\{[|c,\phi\rangle] \in \mathbb{CP}^{d-1} \mid \phi \in X\}$. Hence, the total number of points in the resulting complex-projective design is $d + |X|$. Recalling Proposition 12, we have that $|X| \geq d(d-1)+1$. Furthermore, from Section 3, we found an explicit construction using Singer sets of these minimal projective toric designs whenever $d+1$ is a prime power. It follows that the resulting complex-projective 2-design is of size d^2+1. Interestingly, the smallest possible complex-projective 2-design—also called a SIC-POVM—has size d^2. The existence of SIC-POVM's in all dimensions d is still an open problem.

These *almost-minimal* $\mathbb{CP}^{d-1}$ 2-designs that we just constructed using Singer sets—$\mathbb{CP}^{d-1}$ 2-designs of size d^2+1—were first constructed in Ref. [56]. Notably, however, our utilization of projective toric designs indicates a possible path toward extending such constructions to higher t-designs.

Example 20 ($d = 3$)**.** We construct the above almost-minimal $\mathbb{CP}^{d-1}$ 2-design in the case of $d = 3$. Let us utilize the minimal $P(T^3)$ 2-design given by the mod 7 Sidon set $(0,1,3)$. The corresponding projective toric design is given by the phases

$$\left\{ \left(0, \frac{2\pi k}{7}, \frac{2\pi k}{7} \times 3\right) \mid k \in \mathbb{Z}_7 \right\}, \tag{19}$$

where we understand $(0,\theta,\phi) \in T^3$ to be a representative of an equivalence class in $P(T^3)$. Denote by (p_0,p_1,p_2) an element of Δ^2. Consider the Δ^2 2-design given by the centroid $(1/3,1/3,1/3)$ weighted by $3/4$ and the extremal points $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ each weighted by $1/12$. Finally, denote points in $\mathbb{CP}^2$ by $[|\psi\rangle]$ for $|\psi\rangle$ a unit vector in $\mathbb{C}^3$, and fix an orthonormal basis $\{|0\rangle, |1\rangle, |2\rangle\}$. Let

$$X = \{[|0\rangle], [|1\rangle], [|2\rangle]\} \cup \left\{ [|\psi_k\rangle] := \left[\frac{1}{\sqrt{3}} \left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} k/7} |1\rangle + \mathrm{e}^{2\pi \mathrm{i} k \times 3/7} |2\rangle \right) \right] \mid k \in \mathbb{Z}_7 \right\}. \tag{20}$$

Turn X into a discrete measure space by weighting $[|0\rangle], [|1\rangle]$, and $[|2\rangle]$ each by $1/12$ and each $[|\psi_k\rangle]$ by $3/(4 \times 7)$. The resulting measure space is a $\mathbb{CP}^2$ 2-design of size 10. ⋄

In Ref. [14, Ap. F], it was shown that projective toric designs are closely related to complete sets of MUBs. Let $S \subset P(T^n)$ be a set of size $|S| = d^2$. By concatenating S with the simplex 2-design described above (extremal points and centroid), one finds that the set of phases S constitute a complete set of MUBs if and only if they satisfy an (1) orthonormality condition, and a (2) mutually unbiased condition. It was shown in Ref. [14, Ap. F] that the second condition (2) can be replaced with the requirement that S be a toric 2-design.

Finally, Ref. [64] introduced the notion of a continuous variable (CV) t-design. Ref. [14] proved that such designs do not exist and therefore introduced *rigged* CV t-designs. A simplex design can be generalized to the unnormalized infinite-dimensional simplex. It then follows that the concatenation of an infinite-dimensional simplex t-design and a $P(T^\infty)$ t-design yields a rigged CV t-design. We therefore see that designs on the infinite-dimensional projective torus $P(T^\infty)$ are closely related to designs on other infinite-dimensional spaces.

5 Conclusion and open questions

In this work, we have developed the theory of projective toric designs and their relation to various other objects in and areas of mathematics and physics. There is still much unknown and we believe there are still many exciting connections to be made. We now discuss various future research directions relating to projective toric designs.

Minimal projective toric designs In this work, we showed that if X is a $P(T^n)$ 2-design, then $|X| \geq n(n-1)+1$. Furthermore, using Sidon sets, we showed that the bound can be saturated when $n-1$ is a prime power. However, we also showed that the bound cannot always be satisfied using the Sidon set construction; for example, when $n=7$, the Sidon set construction does not yield a minimal projective toric 2-design. We thus have the following open question: do projective toric 2-designs saturating the bound exist for all n?

We showed that if the t-design is a cyclic group, then the constructions are in one-to-one correspondence with B_t mod $|X|$ sets. In the case of e.g. $n=7$ and $t=2$, $n(n-1)+1=43$ is prime so that the only group design could be a cyclic group. Therefore, if one can prove that a minimal design must be a group, then one would prove that the $t=2$ bound cannot be saturated for all n. Must the minimal design be a group?

We further proved that if X is a $P(T^n)$ t-design, then $|X| \geq G_{n-1}(\lfloor t/2 \rfloor)$. We conjectured that the bound is tight when t is even. Can this conjecture be proven? Can the bound be tightened for odd t? Can one construct saturating designs? As we saw in Proposition 12, the lower bound on the size of projective toric 2-designs matches the lower bound on the size of dense modular Sidon sets. We believe that the analogous statement holds for all t. Using the connection between difference sets and projective toric designs, we related dense B_t mod m sets to the root lattice A_{n-1} and proved a bound relating the size n of the set and the value of m. This connection seems to be a fruitful area to continue exploring.

Connection to affine/projective planes A *finite projective plane* is a tuple (P, L) of a finite set of points P and lines $L \subseteq 2^P$ (where 2^P means the power set of set P, i.e. the set of all subsets of P) such that:

1. Any two points are elements of a unique common line
2. Any two lines intersect at a unique point
3. There exist four points in P such that no line contains more than two of them.

Affine planes are defined similarly. A tuple (P, L) can only be a finite projective plane if there exists some $d \in \mathbb{N}$ such that $|P| = |L| = d^2 + d + 1$. However, finite projective planes have only been constructed for d a prime power, and are known to *not* exist if d is both not the sum of two squares and $d \equiv 1$ or 2 mod 4. These numeric similarities, along with deep connections between combinatorial designs and finite geometry, hint at a deeper connection between projective toric designs and finite projective planes. In addition, projective planes appear in the construction of Sidon sets, and are conjectured to correspond to dense ones [65].

Further, a complete set of MUBs yields a finite projective plane, while a SIC-POVM in prime power dimensions yields a finite affine plane [53,66,67]. As mentioned above, MUBs are closely related to projective toric designs, while SIC-POVMs are minimal complex-projective designs. All of this circumstantial evidence begs the question: are there interesting direct connections one can make between projective toric designs and finite planes, either projective or affine?

Connection to other designs Recall that complex projective designs can be constructed by concatenating simplex and projective toric designs. Similarly, rigged continuous variable t-designs can be constructed in an analogous way by using $P(T^\infty)$ designs. One can ask: how much can this result be generalized? Can we use similar constructions for toric varieties and flag varieties? Indeed $\mathbb{CP}^n$ is a toric variety with moment map to the associated polytope being the simplex Δ^n. The moment map allows us to project $\mathbb{CP}^n$ designs to Δ^n designs. Projective toric designs allow us to pullback along the moment map and build $\mathbb{CP}^n$ designs from Δ^n designs. How much more general can this result be made?

New families of quantum state designs Using the families of $P(T^n)$ t-designs constructed in Section 3.1, can we generate new interesting families of quantum state t-designs? To do this, we need to find families of simplex t-designs. In the $t = 2$ case, we used a particularly nice simplex 2-design that allowed us to construct almost-minimal quantum state 2-designs from minimal projective toric 2-designs. Can we find similarly nice simplex t-designs for $t > 2$?

Approximate designs One can consider approximate projective toric t-design, which are points on the projective torus that integrate monomials of degree $\leq t$ up to an error of ε. How does the size of the minimal approximate t-design depend on t and ε? If one takes an ε_1-approximate simplex t-design and ε_2-approximate projective toric design and concatenates them, what is the ε with which we get an ε-approximate complex-projective t-design? In Appendix C, we take the first steps to study such approximate designs. In particular, we define ε-approximate $P(T^n)$ t-designs, and we provide an upper bound on the minimum number of points drawn uniformly randomly from $P(T^n)$ needed to form an ε-approximate $P(T^n)$ t-design with probability $1-\delta$. We show that the resulting bound depends on the crystal ball sequences of the root lattices A_{n-1} [54,55] given in Eq. (11).

Acknowledgements

We thank Alexander Barg, Carl Miller, Wim van Dam, Greg Kuperberg, Kunal Sharma, Jake Bringewatt, and Victor Albert for helpful discussions. JTI thanks the Joint Quantum Institute at the University of Maryland for support through a JQI fellowship. This work was supported in part by the DoE ASCR Accelerated Research in Quantum Computing program (award No. DE-SC0020312), DoE ASCR Quantum Testbed Pathfinder program (awards No. DE-SC0019040 and No. DE-SC0024220), NSF QLCI (award No. OMA-2120757), NSF PFCQC program, AFOSR, ARO MURI, AFOSR MURI, and DARPA SAVaNT ADVENT. Support is also acknowledged from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator.

A Singer sets

In this appendix, we review Singer's construction of Sidon sets of size $p^m + 1$ for cyclic groups of size $(p^m)^2 + (p^m) + 1$ with p a prime [63, p. 380-381] [51, Sec. 3.5] [52]. The existence of these Singer sets implies that there is a projective n-torus 2-design of size $(n-1)^2 + n = n^2 - n + 1$, i.e., a minimal one, whenever $n - 1$ is prime-power. We emphasize that everything in this appendix is review.

The construction of such Sidon sets goes as follows. Let θ be the generator of $\mathbb{F}^\times_{(n-1)^{t+1}}$, and then let

$$T_t := \{0\} \cup \{a \in [(n-1)^{t+1} - 1] \;:\; (\theta^a - \theta) \in \mathbb{F}_{n-1} \subset \mathbb{F}_{(n-1)^{t+1}}\}. \tag{A1}$$

The inclusion $\mathbb{F}_{n-1} \hookrightarrow \mathbb{F}_{(n-1)^{t+1}}$ is done by identifying the generator of $\mathbb{F}^\times_{(n-1)}$ with $\theta^{\frac{(n-1)^{t+1}-1}{n-2}}$, which makes sense as for any finite field $\mathbb{F}_q$, $|\mathbb{F}_q^\times| = q - 1$, and $\mathbb{F}_q^\times$ is cyclic.

Further, note that $\mathbb{F}_{(n-1)^{t+1}}$ is a $(t+1)$-dimensional $\mathbb{F}_{n-1}$-vector space. Thus, $\{\theta^b\}_{b=0}^t$ is a $\mathbb{F}_{n-1}$-basis of $\mathbb{F}_{(n-1)^{t+1}}$. This means that all $\theta^a = \sum_{i=0}^t k_i \theta^i$ for some unique $k_i \in \mathbb{F}_{(n-1)}$. However, if $\frac{(n-1)^{t+1}-1}{n-2} | a$, we know all $i \geq 1$ have $k_i = 0$.

Then, let

$$S_t((n-1), \theta) := \left\{ l \in \mathbb{Z}_{\frac{(n-1)^{t+1}-1}{n-2}} \;:\; l \equiv a \mod \left(\frac{(n-1)^{t+1}-1}{n-2}\right), a \in T_t \right\} \tag{A2}$$

be the residues of T_t mod $\frac{(n-1)^{t+1}-1}{n-2}$. We now recount proofs of some of $S_t((n-1), \theta)$'s properties.

Lemma A.1. *$|S_t((n-1), \theta)| = n$.*

Proof. First we note there are n distinct elements of $\mathbb{F}_{(n-1)^{t+1}}$ of the form $\theta + \gamma_a$, $\gamma_a \in \mathbb{F}_{n-1}$ by the $\mathbb{F}_{n-1}$-linear independence of θ and 1. As all elements of $\mathbb{F}_{(n-1)^{t+1}}$ equal θ^a for some unique $a \in [(n-1)^{t+1} - 1]$, we see that $|T_t| = n$. Now, we must show that every element of T_t has a different residue modulo $\frac{(n-1)^{t+1}-1}{n-2}$.

Suppose $a, a' := a + k\frac{(n-1)^{t+1}-1}{n-2} \in T$, $k \in \mathbb{Z}_{>0}$. Then $r := \theta^{a'}/\theta^{a} = \theta^{k\frac{(n-1)^{t+1}-1}{n-2}} \in \mathbb{F}_{n-1}$. But by definition of T_t, $\theta^a = \theta + \gamma_a$, $\theta^{a'} = \theta + \gamma_{a'}$. But

$$\theta^{a'} = r\theta^a = r\theta + r\gamma_a. \tag{A3}$$

Thus, $r = 1$, meaning $(n-2)|k$, which means that only a can be in $[(n-1)^{t+1}-1]$, and thus that no two elements of T_t can have the same residue modulo $\frac{(n-1)^{t-1}+1}{n-2}$. □

Lemma A.2. *$S_t((n-1), \theta)$ is a B_t (mod $\frac{(n-1)^{t+1}-1}{n-2}$) set.*

Proof. Recall that $\{\theta^i\}_{i=0}^t$ is a $\mathbb{F}_{n-1}$-basis of $\mathbb{F}_{(n-1)^{t+1}}$. In other words, there exist no non-elementwise-zero tuples $(c_i)_{i=0}^t \in \mathbb{F}_{n-1}^{t+1}$ such that

$$\sum_{i=0}^{t} c_i\theta^i = 0. \tag{A4}$$

Equivalently, θ cannot be the root of any polynomial of degree $\leq t$ with $\mathbb{F}_{n-1}$-coefficients.

Now, consider two multisets A, B, $|A| = |B| \leq t$, taking entries from $S_t((n-1), \theta)$. Then, by the definition of $S_t((n-1), \theta)$ and T_t, we see that for all $a \in A \cup B$

$$\theta^a = \alpha_a(\theta + \gamma_a) \tag{A5}$$

for some $\alpha_a \in \mathbb{F}_{n-1}$. Now, consider $\Pi_A := \prod_{a\in A} \theta^a$ and $\Pi_B := \prod_{b\in B} \theta^b$. It is clear that $\Pi_B/\Pi_A \in \mathbb{F}_{n-1}$ and only if

$$\sum_{a\in A} a \equiv \sum_{b\in B} b \mod \frac{(n-1)^{t+1}-1}{n-2}. \tag{A6}$$

Thus, $\Pi_A - \beta_{A,B}\Pi_B = 0$ for some $\beta_{A,B} \in \mathbb{F}_{n-1}$ if and only if Eq. (A6) holds. However, for any $\beta \in \mathbb{F}_{n-1}$, we see that $\Pi_A - \beta\Pi_B$ is a degree-t polynomial equation in θ with $\mathbb{F}_{n-1}$ coefficients, meaning it cannot have any solutions, meaning the B_t (mod $\frac{(n-1)^{t+1}-1}{n-2}$) condition is satisfied. □

A.1 Explicit example of dense modular Sidon set

In this appendix, we work through an explicit example of the construction of the Sidon set $S_{t=2}((n-1), \theta)$ for $n = 5 = 2^2+1$. We begin by constructing T_t. Consider the field $\mathbb{F}_{(n-1)^{t+1}} = \mathbb{F}_{4^3} = \mathbb{F}_{2^6}$. With the irreducible polynomial $f(x) = 1 + x^5 + x^6 \in \mathbb{F}_2[x]$, we work in the polynomial representation $\mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/(f(x))$.

One can check that the generator θ of the multiplicative group $\mathbb{F}_{2^6}^\times$ is x in this representation—in other words, $|\{x^m \bmod f(x) \mid m \in \mathbb{Z}_{63}\}| = 63$. We identify $\mathbb{F}_{n-1} = \mathbb{F}_{2^2} \subset \mathbb{F}_{2^6}$ via generating $\mathbb{F}_{2^2}^\times$ with

$$y = x^{\frac{(n-1)^{t+1}-1}{n-2}} = x^{21}, \tag{A7}$$

so that $\mathbb{F}_{2^2} = \{0\} \cup \{y^k \mid k \in \mathbb{Z}_3\}$. Then

$$T_{t=2} = \{0\} \cup \{a \in \mathbb{Z}_{4^3-1} \setminus \{0\} \mid (x^a - x) \pmod{f(x)} \in \mathbb{F}_{2^2}\}. \tag{A8}$$

Clearly, $1 \in T_{t=2}$. With that out of the way, we can rephrase this as

$$T_{t=2} = \{0,1\} \cup \{a \in \mathbb{Z}_{4^3-1} \setminus \{0,1\} \mid \exists k \in \mathbb{Z}_3\colon\ x^a - x \equiv y^k \pmod{f(x)}\}. \tag{A9}$$

One can straightforwardly numerically verify that $T_2 = \{0, 1, 14, 25, 58\}$. To ensure understanding of the construction, we will work through why $14 \in T_2$. We need to show that $x^{14} - x \equiv y^k \pmod{f(x)}$ for $k = 0, 1$ or 2. It turns out that $k = 2$ satisfies this equation. In particular,

$$(x^{14} - x) \pmod{f(x)} = x^3 + x^4 + x^5 = y^2 \pmod{f(x)} = x^{42} \pmod{f(x)}, \tag{A10}$$

where recall we're working with polynomials over the field $\mathbb{F}_2$. Similarly, for 25,

$$(x^{25} - x) \pmod{f(x)} = 1 + x^3 + x^4 + x^5 = y^1 \pmod{f(x)} = x^{21} \pmod{f(x)}, \tag{A11}$$

and for 58,

$$(x^{58}-x) \pmod{f(x)} = 1 = y^0 \pmod{f(x)}. \tag{A12}$$

Hence, we have found that $T_2 = \{0,1,14,25,58\}$. To get our Sidon set, we compute the residues $S_2 = T_2 \bmod \frac{(n-1)^{t+1}-1}{n-2} = T_2 \bmod 21$, giving

$$S_2 = \{0,1,14,4,16\} = \{0,1,4,14,16\}\,. \tag{A13}$$

One can easily confirm that this is a Sidon set mod 21. In particular, the set of all sums $a+b \bmod 21$ for $a,b \in S_2$ is $\{0,1,2,4,5,7,8,9,11,14,15,16,17,18,20\}$, which has size $15 = \binom{n+t-1}{t} = \binom{6}{2}$, which is the maximal possible size.

B Pullback of the Fubini-Study volume form

It is shown in Ref. [49, Sec. 4.5, 4.7, 7.6] that the volume measure on complex projective space is the product of the flat measure on the simplex and the flat measure on the torus. For completeness, in this appendix, we show the same result via a different method.

Let $[Z_0 : \dots : Z_n]$ be homogeneous coordinates on $\mathbb{CP}^n$. Consider the coordinate patches $C_0, \dots, C_n$ on $\mathbb{CP}^n$, where $C_i = \{[Z_0 : \dots : Z_n] \mid Z_i \neq 0\}$. The volume of $\mathbb{CP}^{d-1} \setminus C_0$ is zero, and therefore for the purposes of volume integration we can restrict our attention to C_0. On C_0, we use the coordinates $z_i \coloneqq Z_i/Z_0$ for $i = 1, \dots, n$. The (unnormalized) Fubini-Study volume form ω can then be written as

$$\omega = \frac{1}{(1+\sum_{i=1}^n |z_i|^2)^{n+1}}\, \mathrm{d}z_1 \wedge \mathrm{d}\bar{z}_1 \wedge \dots \mathrm{d}z_n \wedge \mathrm{d}\bar{z}_n. \tag{B1}$$

We can write $Z_i = \sqrt{p_i}\mathrm{e}^{\mathrm{i}\phi_i}$ for $i = 0, \dots, n$ and $\sum_{i=0}^n p_i = 1$. In other words, p is a point on the simplex $p \in \Delta^n \coloneqq \{p \in [0,1]^n \mid \sum_i p_i \leq 1\}$ (with $p_0 \coloneqq 1 - \sum_{i=1}^n p_i$) and ϕ is a point on the projective torus $\phi \in P(T^{n+1})$ (e.g. we can choose a representative with $\phi_0 = 0$). Therefore, $z_i = \sqrt{\frac{p_i}{p_0}}\mathrm{e}^{\mathrm{i}\phi_i - \mathrm{i}\phi_0}$.

Consider the map $\pi\colon \tilde{\Delta}^n \times P(T^{n+1}) \to C_0$, where $\tilde{\Delta}^n$ is all $p \in \Delta^n$ satisfying $p_0 > 0$. The map is $\pi^i(p,\phi) = \sqrt{\frac{p_i}{p_0}}\mathrm{e}^{\mathrm{i}\phi_i - \mathrm{i}\phi_0}$.

Proposition B.1. *The pullback $\pi^*\omega$ is*

$$\pi^*\omega = (-1)^{n/2}\, \mathrm{d}p_1 \wedge \dots \mathrm{d}p_n \wedge \mathrm{d}\phi_1 \wedge \dots \mathrm{d}\phi_n. \tag{B2}$$

It follows from this proposition that the unit-volume normalized volume measure on $\mathbb{CP}^n$ is equal to the product of the Lebesgue measure on the simplex Δ^n and the Lebesgue measure on $P(T^{n+1})$ (where recall the latter is equal to the Lebesgue measure on T^n).

Proof of the proposition. We can without loss of generality fix $\phi_0 = 0$. We can rewrite

$$\omega = p_0^{n+1}\, \mathrm{d}z_1 \wedge \mathrm{d}\bar{z}_1 \wedge \dots \mathrm{d}z_n \wedge \mathrm{d}\bar{z}_n. \tag{B3}$$

Therefore,

$$\pi^*\omega = p_0^{n+1} \det(J)\, \mathrm{d}p_1 \wedge \dots \mathrm{d}p_n \wedge \mathrm{d}\phi_1 \wedge \dots \mathrm{d}\phi_n, \tag{B4}$$

where

$$J = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{B5}$$

is the Jacobian with

$$A_{ij} = \frac{\partial \pi^i}{\partial \phi_j}, \quad B_{ij} = \frac{\partial \pi^i}{\partial p_j}, \quad C_{ij} = \frac{\partial \bar{\pi}^i}{\partial \phi_j}, \quad D_{ij} = \frac{\partial \bar{\pi}^i}{\partial p_j}. \tag{B6}$$

We can check that

$$\frac{\partial \pi^i}{\partial p_j} = \frac{1}{2}\pi^i(p,\phi)\left(\frac{\delta_{ij}}{p_i} + \frac{1}{p_0}\right), \qquad \frac{\partial \pi^i}{\partial \phi_j} = \mathrm{i}\delta_{ij}\pi^i(p,\phi). \tag{B7}$$

Therefore, A and C are diagonal and thus commute, meaning that $\det(J) = \det(AD - CB)$. The matrix elements are $(AD - CB)_{ij} = \frac{\mathrm{i}}{p_0}\left(\delta_{ij} + \frac{p_i}{p_0}\right)$.

By the matrix determinant lemma [68], $\det(M + uv^T) = (1 + v^T M^{-1} u)\det(M)$ with $M = \frac{\mathrm{i}}{p_0}\delta_{ij}$ and $u_i = \mathrm{i}/p_0$ and $v_i = p_i/p_0$, we find that

$$\det(J) = \left(\frac{\mathrm{i}}{p_0}\right)^n \left(1 + \sum_{i=1}^n \frac{p_i}{p_0}\right) = \left(\frac{i}{p_0}\right)^n \frac{1}{p_0} = \frac{(-1)^{n/2}}{p_0^{n+1}}. \tag{B8}$$

The proposition follows. □

C Approximate projective toric designs

Throughout this appendix, we will be concerned with uniform finite $P(T^n)$ t-designs; that is, $P(T^n)$ t-designs X that are finite and the measure space $(X, \Sigma = \mathcal{P}(X), \nu)$ is such that $\nu(A) = |A| / |X|$. We will restrict to finite n. We will define approximate projective toric designs and prove a loose bound on the number $M(t, \varepsilon, \delta)$ of uniformly random points needed to form such a design.

For $\mathbf{p} \in \mathbb{N}_0^n$, let $f_{\mathbf{p}}(\phi)$ denote the monomial $\prod_{i=1}^n \mathrm{e}^{i\phi_i p_i}$. Notice that $\bar{f}_{\mathbf{p}}(\phi) = f_{\mathbf{p}}(-\phi) = f_{-\mathbf{p}}(\phi)$.

Definition C.1. *We say that $C \subset P(T^n)$ is a (uniform) ε-approximate projective toric t-design if, for all $\mathbf{p} \in P_t^{(n)}$,*

$$\left| \frac{1}{|C|} \sum_{\phi \in C} f_{\mathbf{p}}(\phi) - \int_{P(T^n)} f_{\mathbf{p}} \, \mathrm{d}\mu_{n-1} \right| = \left| \frac{1}{|C|} \sum_{\phi \in C} f_{\mathbf{p}}(\phi) - \delta_{\mathbf{p},\mathbf{0}} \right| \le \varepsilon. \tag{C1}$$

Here, $P_t^{(n)}$ is the set defined in Eq. (10),

$$P_t^{(n)} \coloneqq \left\{ \mathbf{q} - \mathbf{r} \;\middle|\; \mathbf{q}, \mathbf{r} \in \mathbb{N}_0^n, \; \sum_{i=1}^n q_i = \sum_{i=1}^n r_i = t \right\}. \tag{C2}$$

Note of course that with $\varepsilon = 0$ we recover the definition of an (exact) projective toric design. There is redundancy in $P_t^{(n)}$. Indeed, if Eq. (C1) is satisfied for $\mathbf{p}$, then it is automatically satisfied for $-\mathbf{p}$. Furthermore, Eq. (C1) is trivially satisfied for any C when $\mathbf{p} = \mathbf{0}$. Hence, we are in fact interested in the set $S_t^{(n)}$ defined by $S_t^{(n)} \coloneqq (P_t^{(n)} \setminus \{\mathbf{0}\})/\mathbb{Z}_2$, where $\mathbb{Z}_2$ denotes the group action $\mathbf{p} \mapsto \pm\mathbf{p}$. Therefore, $C \subset P(T^n)$ is an ε-approximate t-design if and only if, for all $\mathbf{p} \in S_t^{(n)}$,

$$\left| \frac{1}{|C|} \sum_{\phi \in C} f_{\mathbf{p}}(\phi) \right| \le \varepsilon. \tag{C3}$$

Define the probability space $\mathcal{C}_M$ to be the ensemble over subsets of $P(T^n)$ of size M. Specifically, to draw a random $C \subset P(T^n)$ from $\mathcal{C}_M$, we simply draw M uniformly random points from $P(T^n)$ with respect to the Haar measure. We often denote a subset $C \subset P(T^n)$ of size M by $C = \{\phi^{(1)}, \ldots, \phi^{(M)}\}$, where each $\phi^{(i)} \in P(T^n)$.

Definition C.2. *Let $M(t, \varepsilon, \delta)$ denote the* ***minimum*** *M such that a random C drawn from $\mathcal{C}_M$ is an ε-approximate $P(T^n)$ t-design with probability $1 - \delta$. In other words,*

$$\begin{aligned} M(t, \varepsilon, \delta) = \min_{M \in \mathbb{N}} &\; M \\ \text{s.t.} &\; \Pr_{C \in \mathcal{C}_M} [C \text{ is an } \varepsilon\text{-approx } t\text{-design on } P(T^n)] \ge 1 - \delta. \end{aligned} \tag{C4}$$

In the following, we will find an upper bound on $M(t, \varepsilon, \delta)$. This will tell us that for any $M \ge M(t, \varepsilon, \delta)$, $C \in \mathcal{C}_M$ will be an ε-approximate t-design with probability $\ge 1 - \delta$.

Theorem C.3. *$M(t,\varepsilon,\delta) \leq \frac{G_{n-1}(t)-1}{2\delta\varepsilon^2}$, where $G_{n-1}(t)$ given in Eq. (11).*

Proof. Recall that $|P_t^{(n)}| = 2|S_t^{(n)}| + 1$, and from Lemma 11 $|P_t^{(n)}| = G_{n-1}(t)$. We will therefore prove that $M(t,\varepsilon,\delta) \leq \frac{|S_t^{(n)}|}{\delta\varepsilon^2}$ Define the following notation:

$$\mathop{\mathbb{E}}_{\phi\in P(T^n)} f(\phi) = \int_{P(T^n)} f \, \mathrm{d}\mu_{n-1} \tag{C5a}$$

$$\mathop{\mathbb{E}}_{\phi\in C} f(\phi) = \frac{1}{|C|}\sum_{\phi\in C} f(\phi) \tag{C5b}$$

$$\mathop{\mathbb{E}}_{C\in\mathcal{C}_M} = \mathop{\mathbb{E}}_{\{\phi^{(1)},\ldots,\phi^{(M)}\}\in P(T^n)^M}. \tag{C5c}$$

For $\mathbf{p} \in S_t^{(n)}$, define

$$\Delta(C,\mathbf{p}) \coloneqq \left|\mathop{\mathbb{E}}_{\phi\in C} f_{\mathbf{p}}(\phi) - \mathop{\mathbb{E}}_{\phi\in P(T^n)} f_{\mathbf{p}}(\phi)\right|^2 = \left|\mathop{\mathbb{E}}_{\phi\in C} f_{\mathbf{p}}(\phi)\right|^2. \tag{C6}$$

We compute the mean,

$$\mathop{\mathbb{E}}_{C\in\mathcal{C}_M} \Delta(C,\mathbf{p}) = \frac{1}{M^2} \mathop{\mathbb{E}}_{\{\phi^{(1)},\ldots,\phi^{(M)}\}\in P(T^n)^M} \sum_{i,j=1}^{M} f_{\mathbf{p}}(\phi^{(i)})\bar{f}_{\mathbf{p}}(\phi^{(j)}) \tag{C7a}$$

$$= \frac{1}{M^2}\left[M \mathop{\mathbb{E}}_{\phi\in P(T^n)} f_{\mathbf{p}}(\phi)\bar{f}_{\mathbf{p}}(\phi) + M(M-1)\left(\mathop{\mathbb{E}}_{\phi\in P(T^n)} f_{\mathbf{p}}(\phi)\right)\left(\mathop{\mathbb{E}}_{\theta\in P(T^n)} \bar{f}_{\mathbf{p}}(\theta)\right)\right] \tag{C7b}$$

$$= \frac{1}{M}. \tag{C7c}$$

Meanwhile, we have that

$$\Pr_{C\in\mathcal{C}_M}\left[C \text{ is an } \varepsilon\text{-approx } t\text{-design on } P(T^n)\right] \tag{C8a}$$

$$= \Pr_{C\in\mathcal{C}_M}\left[\forall \mathbf{p}\in S_t^{(n)} : \Delta(C,\mathbf{p}) \leq \varepsilon^2\right] \tag{C8b}$$

$$= 1 - \Pr_{C\in\mathcal{C}_M}\left[\exists \mathbf{p}\in S_t^{(n)} : \Delta(C,\mathbf{p}) > \varepsilon^2\right] \tag{C8c}$$

$$(\textit{union bound}) \geq 1 - \sum_{\mathbf{p}\in S_t^{(n)}} \Pr_{C\in\mathcal{C}_M}\left[\Delta(C,\mathbf{p}) > \varepsilon^2\right] \tag{C8d}$$

$$(\textit{Markov's inequality}) \geq 1 - \sum_{\mathbf{p}\in S_t^{(n)}} \frac{\mathbb{E}_{C\in\mathcal{C}_M}\Delta(C,\mathbf{p})}{\varepsilon^2} \tag{C8e}$$

$$= 1 - \frac{|S_t^{(n)}|}{M\varepsilon^2}. \tag{C8f}$$

Thus, we require that

$$1 - \frac{1}{M\varepsilon^2}|S_t^{(n)}| \geq 1 - \delta. \tag{C9}$$

It follows that any $M \geq \frac{|S_t^{(n)}|}{\delta\varepsilon^2}$ satisfies, so that $M(t,\varepsilon,\delta) \leq \frac{|S_t^{(n)}|}{\delta\varepsilon^2}$. □

References

[1] Carl Friedrich Gauss. "Methodus nova integralium valores per approximationem inveniendi". In Werke. Pages 165–196. Cambridge University Press (1866).

[2] P. Delsarte, J. M. Goethals, and J. J. Seidel. "Spherical codes and designs". Geometriae Dedicata **6**, 363–388 (1977).

[3] R. H. Hardin and N. J. A. Sloane. "McLaren's improved snub cube and other new spherical designs in three dimensions". Discrete & Computational Geometry **15**, 429–441 (1996).

[4] A. H. Stroud. "Approximate calculation of multiple integrals". Prentice-Hall. (1971).

[5] Marc Beckers and Ronald Cools. "A relation between cubature formulae of trigonometric degree and lattice rules". Pages 13–24. Birkhäuser Basel. Basel (1993).

[6] Ronald Cools and Ian H. Sloan. "Minimal cubature formulae of trigonometric degree". Mathematics of Computation **65**, 1583–1600 (1996).

[7] Ronald Cools. "Constructing cubature formulae: The science behind the art". Acta Numerica **6**, 1–54 (1997).

[8] Preston C Hammer and Arthur H Stroud. "Numerical integration over simplexes". Mathematical tables and other aids to computation **10**, 137–139 (1956).

[9] Mohammad Samy Baladram. "On explicit construction of simplex t-designs". Interdisciplinary Information Sciences **24**, 181–184 (2018).

[10] Greg Kuperberg. "Numerical cubature from Archimedes' hat-box theorem" (2004). arXiv:math/0405366.

[11] Greg Kuperberg. "Numerical cubature using error-correcting codes" (2004). arXiv:math/0402047.

[12] Nicolas Victoir. "Asymmetric cubature formulae with few points in high dimension for symmetric measures". SIAM Journal on Numerical Analysis **42**, 209–227 (2004).

[13] Paul D Seymour and Thomas Zaslavsky. "Averaging sets: a generalization of mean values and spherical designs". Advances in Mathematics **52**, 213–240 (1984).

[14] Joseph T. Iosue, Kunal Sharma, Michael J. Gullans, and Victor V. Albert. "Continuous-variable quantum state designs: Theory and applications" (2022). arXiv:2211.05127.

[15] S. G. Hoggar. "T-Designs in Projective Spaces". European Journal of Combinatorics **3**, 233–254 (1982).

[16] S. G. Hoggar. "Parameters of t-Designs in FPd-1". European Journal of Combinatorics **5**, 29–36 (1984).

[17] Eiichi Bannai and Stuart G. Hoggar. "On tight t-designs in compact symmetric spaces of rank one". Proceedings of the Japan Academy, Series A, Mathematical Sciences **61** (1985).

[18] William K Wootters and Brian D Fields. "Optimal state-determination by mutually unbiased measurements". Annals of Physics **191**, 363–381 (1989).

[19] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. "Symmetric informationally complete quantum measurements". Journal of Mathematical Physics **45**, 2171–2180 (2004).

[20] A. Klappenecker and M. Rotteler. "Mutually unbiased bases are complex projective 2-designs". In Proceedings. International Symposium on Information Theory, 2005. Pages 1740–1744. (2005).

[21] Christoph Dankert. "Efficient simulation of random quantum states and operators" (2005). arXiv:quant-ph/0512217.

[22] A. J. Scott. "Tight informationally complete quantum measurements". Journal of Physics A: Mathematical and General **39**, 13507–13530 (2006).

[23] Andris Ambainis and Joseph Emerson. "Quantum t-designs: t-wise independence in the quantum world". In Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07). Pages 129–140. (2007).

[24] Daniel A Roberts and Beni Yoshida. "Chaos and complexity by design". Journal of High Energy Physics **2017**, 1–64 (2017).

[25] Richard Kueng and David Gross. "Qubit stabilizer states are complex projective 3-designs" (2015). arXiv:1510.02767.

[26] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. "Exact and approximate unitary 2-designs and their application to fidelity estimation". Physical Review A **80**, 012304 (2009).

[27] S. J. van Enk and C. W. J. Beenakker. "Measuring Trρ^n on single copies of ρ using random measurements". Phys. Rev. Lett. **108**, 110503 (2012).

[28] Scott Aaronson. "Shadow tomography of quantum states". SIAM Journal on Computing **49**, STOC18–368–STOC18–394 (2020). arXiv:1711.01053.

[29] Hsin-Yuan Huang, Richard Kueng, and John Preskill. "Predicting many properties of a quantum system from very few measurements". Nature Physics **16**, 1050–1057 (2020).

[30] Hsin-Yuan Huang, Richard Kueng, Giacomo Torlai, Victor V. Albert, and John Preskill. "Provably efficient machine learning for quantum many-body problems". Science (2022). arXiv:2106.12627.

[31] Atithi Acharya, Siddhartha Saha, and Anirvan M. Sengupta. "Informationally complete POVM-based shadow tomography" (2021). arXiv:2105.05992.

[32] Richard Kueng, Huangjun Zhu, and David Gross. "Distinguishing quantum states using clifford orbits" (2016). arXiv:1609.08595.

[33] Joseph Emerson, Robert Alicki, and Karol Życzkowski. "Scalable noise estimation with random unitary operators". Journal of Optics B: Quantum and Semiclassical Optics **7**, S347–S352 (2005).

[34] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. "Randomized benchmarking of quantum gates". Physical Review A **77**, 012307 (2008).

[35] Easwar Magesan, J. M. Gambetta, and Joseph Emerson. "Scalable and robust randomized benchmarking of quantum processes". Physical Review Letters **106**, 180504 (2011).

[36] Andrew W Cross, Easwar Magesan, Lev S Bishop, John A Smolin, and Jay M Gambetta. "Scalable randomised benchmarking of non-clifford gates". npj Quantum Information **2**, 1–5 (2016).

[37] M. A. Nielsen. "The entanglement fidelity and quantum error correction" (1996). arXiv:quant-ph/9606012.

[38] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "General teleportation channel, singlet fraction, and quasidistillation". Physical Review A **60**, 1888–1898 (1999).

[39] Michael A Nielsen. "A simple formula for the average gate fidelity of a quantum dynamical operation". Physics Letters A **303**, 249–252 (2002).

[40] Easwar Magesan, Robin Blume-Kohout, and Joseph Emerson. "Gate fidelity fluctuations and quantum process invariants". Physical Review A **84**, 012309 (2011).

[41] Dawei Lu, Hang Li, Denis-Alexandre Trottier, Jun Li, Aharon Brodutch, Anthony P. Krismanich, Ahmad Ghavami, Gary I. Dmitrienko, Guilu Long, Jonathan Baugh, and Raymond Laflamme. "Experimental Estimation of Average Fidelity of a Clifford Gate on a 7-Qubit Quantum Processor". Physical Review Letters **114**, 140505 (2015).

[42] Sergey Bravyi, Anirban Chowdhury, David Gosset, and Pawel Wocjan. "Quantum hamiltonian complexity in thermal equilibrium". Nature Physics **18**, 1367–1370 (2022).

[43] Andris Ambainis and Adam Smith. "Small pseudo-random families of matrices: Derandomizing approximate quantum encryption". In Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. Pages 249–260. Springer (2004). arXiv:quant-ph/0404075.

[44] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. “Randomizing quantum states: Constructions and applications”. Communications in Mathematical Physics **250**, 371–391 (2004).

[45] Shelby Kimmel and Yi-Kai Liu. “Phase retrieval using unitary 2-designs”. 2017 International Conference on Sampling Theory and Applications (SampTA)Pages 345–349 (2017).

[46] Xiao Mi, Pedram Roushan, Chris Quintana, Salvatore Mandra, Jeffrey Marshall, Charles Neill, Frank Arute, Kunal Arya, Juan Atalaya, Ryan Babbush, Joseph C. Bardin, Rami Barends, Andreas Bengtsson, Sergio Boixo, Alexandre Bourassa, Michael Broughton, Bob B. Buckley, David A. Buell, Brian Burkett, Nicholas Bushnell, Zijun Chen, Benjamin Chiaro, Roberto Collins, William Courtney, Sean Demura, Alan R. Derk, Andrew Dunsworth, Daniel Eppens, Catherine Erickson, Edward Farhi, Austin G. Fowler, Brooks Foxen, Craig Gidney, Marissa Giustina, Jonathan A. Gross, Matthew P. Harrigan, Sean D. Harrington, Jeremy Hilton, Alan Ho, Sabrina Hong, Trent Huang, William J. Huggins, L. B. Ioffe, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Cody Jones, Dvir Kafri, Julian Kelly, Seon Kim, Alexei Kitaev, Paul V. Klimov, Alexander N. Korotkov, Fedor Kostritsa, David Landhuis, Pavel Laptev, Erik Lucero, Orion Martin, Jarrod R. McClean, Trevor McCourt, Matt McEwen, Anthony Megrant, Kevin C. Miao, Masoud Mohseni, Wojciech Mruczkiewicz, Josh Mutus, Ofer Naaman, Matthew Neeley, Michael Newman, Murphy Yuezhen Niu, Thomas E. O’Brien, Alex Opremcak, Eric Ostby, Balint Pato, Andre Petukhov, Nicholas Redd, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vladimir Shvarts, Doug Strain, Marco Szalay, Matthew D. Trevithick, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, Igor Aleiner, Kostyantyn Kechedzhi, Vadim Smelyanskiy, and Yu Chen. “Information Scrambling in Computationally Complex Quantum Circuits”. Science **374**, 1479–1483 (2021). arXiv:2101.08870.

[47] Yasuhiro Sekino and Leonard Susskind. “Fast scramblers”. Journal of High Energy Physics **2008**, 065 (2008).

[48] Patrick Hayden and John Preskill. “Black holes as mirrors: quantum information in random subsystems”. Journal of high energy physics **2007**, 120 (2007).

[49] Ingemar Bengtsson and Karol Życzkowski. “Geometry of quantum states: an introduction to quantum entanglement”. Cambridge University Press. Cambridge (2008).

[50] Terence Tao and Van Vu. “Additive combinatorics”. Cambridge University Press. Cambridge (2006).

[51] Kevin O’Bryant. “A Complete Annotated Bibliography of Work Related to Sidon Sequences”. The Electronic Journal of Combinatorics (2004).

[52] R. C. Bose and S. Chowla. “Theorems in the additive theory of numbers”. Commentarii Mathematici Helvetici **37**, 141–147 (1962).

[53] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. “On mutually unbiased bases”. International Journal of Quantum Information **08**, 535–640 (2010).

[54] J. H. Conway and N. J. A. Sloane. “Low–dimensional lattices. VII. Coordination sequences”. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **453**, 2369–2389 (1997).

[55] OEIS Foundation Inc. “The On-Line Encyclopedia of Integer Sequences”. `https://oeis.org/A108625`.

[56] Bernhard G. Bodmann and John Haas. “Achieving the orthoplex bound and constructing weighted complex projective 2-designs with Singer sets” (2015). arXiv:1509.05333.

[57] Donald L. Cohn. “Measure theory”. Birkhäuser Advanced Texts. Birkhäuser. Boston (2013). Second edition.

[58] Sadahiro Saeki. “A Proof of the Existence of Infinite Product Probability Measures”. The American Mathematical Monthly **103**, 682–683 (1996).

[59] W.N. Bailey. "Generalized Hypergeometric Series, By W.N. Bailey". Cambridge Tracts in Mathematics and Mathematical Physics, No. 32. Camrbridge University Press. (1964). url: https://books.google.com/books?id=TVyswgEACAAJ.

[60] Lucy Joan Slater. "Generalized hypergeometric functions". Cambridge Univ. Press. Cambridge (1966).

[61] Marko Petkovšek, Herbert S. Wilf, and Doron Zeilberger. "A=B". A K Peters. (1996).

[62] Wadim Zudilin. "Hypergeometric heritage of W. N. Bailey". Notices of the International Congress of Chinese Mathematicians **7**, 32–46 (2019).

[63] James Singer. "A theorem in finite projective geometry and some applications to number theory". Transactions of the American Mathematical Society **43**, 377–85 (1938).

[64] Robin Blume-Kohout and Peter S Turner. "The curious nonexistence of gaussian 2-designs". Communications in Mathematical Physics **326**, 755–771 (2014).

[65] Sean Eberhard and Freddie Manners. "The apparent structure of dense sidon sets". The Electronic Journal of Combinatorics **30** (2023).

[66] William K. Wootters. "Quantum measurements and finite geometry" (2004). arXiv:quant-ph/0406032.

[67] Metod Saniga, Michel Planat, and Haret Rosu. "Mutually unbiased bases and finite projective planes". Journal of Optics B: Quantum and Semiclassical Optics **6**, L19–L20 (2004).

[68] David A. Harville. "Matrix Algebra From a Statistician's Perspective". Springer. New York, NY (1997).