Electronic Colloquium on Computational Complexity, Report No. 13 (2007)

Quantum t-designs: t-wise independence in the quantum world

Andris Ambainis*and Joseph Emerson†

Abstract

A t-design for quantum states is a finite set of quantum states with the property of simulating the Haar-measure on quantum states w.r.t. any test that uses at most t copies of a state. We give efficient constructions for approximate quantum t-designs for arbitrary t. We then show that an approximate 4-design provides a derandomization of the state-distinction problem considered by Sen (quant-ph/0512085), which is relevant to solving certain instances of the hidden subgroup problem.

1 Introduction

t-wise independent and approximately t-wise independent probability distributions have been extremely useful in combinatorics and the theory of computing. In this paper, we study their quantum counterparts, *quantum t-designs.*

Intuitively, a quantum t-design is a probability distribution over quantum states which cannot be distinguished from the uniform probability distribution over all quantum states (the Haar measure) if we are given t copies of a state from this probability distribution. More formally, we define

Definition 1 *[Generalization of the definition in Ref. [16]] A probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is a complex projective (t,t)-design if*

$$\sum_i p_i(|\phi_i\rangle\langle\phi_i|)^{\otimes t} = \int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi,$$

where the integral over $|\psi\rangle$ on the left hand side is taken over the Haar measure on the unit sphere in $\mathbf{C}^N$.

This definition of complex-projective (t,t)-designs, or *quantum t-designs* has been previously studied in two contexts.

In the context of quantum information theory, [3, 16, 11, 12, 5] have studied quantum 2-designs, giving constructions of 2-designs with $O(N^2)$ states and applying them to various problems in quantum information. Hayashi et al. [9] gave a construction of a t-design for arbitrary t with $O(t)^N$ of states. This is efficient for a fixed dimension N but inefficient when N is much larger than t. The $N=2$ (one-qubit) case was independently solved by Iblisdir and Roland [10].

*Department of Combinatorics and Optimization and the Institute for Quantum Computing, University of Waterloo, ambainis@uwaterloo.ca. Supported by NSERC, CIAR, ARO, MITACS and IQC University Professorship.

†Department of Applied Mathematics and the Institute for Quantum Computing, University of Waterloo, jemerson@uwaterloo.ca. Supported by NSERC and MITACS.

ISSN 1433-8092

Second, quantum t-designs are related to t-designs of vectors on the unit sphere in $\mathbf{R}^N$, called *spherical t-designs*, which have been studied in the mathematics literature since a seminal paper by Delsarte, Goethals and Seidel [6]. An inefficient construction of an exact spherical t-design with $t^{O(N^2)}$ vectors has been given by Bajnok [2] and Korevaar and Meyers [13]. A spherical t-design in $\mathbf{R}^N$ can be transformed into a $(t/2, t/2)$-design in $\mathbf{C}^{N/2}$. Thus, those results also imply the existence of quantum t-designs with a similar number of states.

To summarize the previous work (for the case when t is fixed and the dimension N is large), inefficient constructions of quantum t-designs with an exponential number of states are known for any t and efficient constructions are known for $t = 2$. The contributions of this paper are as follows:

1. We introduce the notion of an approximate t-design;
2. We give an efficient construction of approximate t-designs, with $O(N^{3t})$ states, for any t;
3. We show how to apply an approximate 4-design to derandomize the state-distinction result by Sen [17].

2 Summary of results

Our definition of an approximate (t, t)-design is as follows:

Definition 2 *A probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is an ϵ-approximate (t, t)-design if*

$$(1-\epsilon)\int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi \le \sum_i p_i (|\phi_i\rangle\langle\phi_i|)^{\otimes t} \le (1+\epsilon)\int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi,$$

where the integral over $|\psi\rangle$ on the left hand side is taken over the Haar measure on the unit sphere in $\mathbf{C}^N$ and

$$\sum_i p_i |\phi_i\rangle\langle\phi_i| = \int_\psi |\psi\rangle\langle\psi| d\psi. \tag{1}$$

Instead of requiring closeness to a t-design in the l_∞ norm, as in Definition 2, one could use a different norm (e.g., l_1 or l_2-norm). This might make design easier to construct but closeness in l_1 or l_2 is not sufficient for Theorem 4 and, possibly, other applications.

Theorem 1 *Fix a constant t. Then, for every $N \ge 2t$, there exists an $O(\frac{1}{N^{1/3}})$-approximate (t, t)-design consisting of $O(N^{3t})$ quantum states*[1].

The t-design of Theorem 1 can be efficiently implemented, for several meanings of "efficiently implemented":

1. It is possible to generate a quantum state $|\phi\rangle$ distributed according to the probability distribution $(p_i, |\phi_i\rangle)$ in time $O(\log^c N)$.
2. Because of equation (1), the operators $Np_i|\phi_i\rangle\langle\phi_i|$ form a POVM measurement. This POVM measurement can be implemented in time $O(\log^c N)$.

[1]The big-O constants can depend on t.

The first property is just the normal definition of being able to sample from the probability distribution. (Since we are dealing with states in N dimensions, which can be described by $\log N$ qubits, "efficient" means polynomial in $\log N$.) The second property may seem unusual at first but it is exactly what we need for our application (Theorem 4).

In section 4.2, we show that the number of states in the ϵ-approximate (t,t)-design can be decreased to $O(N^t \log^c N)$. There is a simple way to generate the states in the resulting (t,t)-design but we are not sure if the corresponding POVM measurement can be efficiently implemented.

We now give the application of Theorem 1. Radhakrishnan et al. [15] have shown

Theorem 2 *Let $|\psi_1\rangle, |\psi_2\rangle$ be two orthogonal quantum states in $\mathbf{C}^N$. Then,*

$$E_{\hat{M}} \|\hat{M}(\psi_1) - \hat{M}(\psi_2)\|_1 = \Omega(1),$$

where $\hat{M}$ is an orthonormal basis picked uniformly at random from the Haar measure.

This result was improved by Sen[17].

Theorem 3 *Let ρ_1, ρ_2 be two mixed states in $\mathbf{C}^N$ with $rank \rho_1 + rank \rho_2 \leq \frac{\sqrt{N}}{K}$ for a sufficiently large K. Then,*

$$E_{\hat{M}} \|\hat{M}(\rho_1) - \hat{M}(\rho_2)\|_1 = \Omega(f),$$

where $\hat{M}$ is an orthonormal basis picked uniformly at random from the Haar measure and $f = \|\rho_1 - \rho_2\|_F$ is the Frobenius norm of $\rho_1 - \rho_2$ ($\|A\|_F = \sqrt{\sum_{k,l=1}^N |a_{kl}|^2}$).

Theorem 2 is a particular case of Theorem 3, since $\||\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|\|_F = 2$. As next theorem shows, we can replace the measurement in a random orthonormal basis by a POVM w.r.t. a complex projective 4-design (where "POVM with respect to $(p_i, |\phi_i\rangle)$" is just the POVM consisting of one-dimensional projectors $Np_i|\phi_i\rangle\langle\phi_i|$).

Theorem 4 *Let $f = \|\rho_1 - \rho_2\|_F$ and $\epsilon < cf^4$, where c is a sufficiently small constant. Then, for any mixed states ρ_1, ρ_2 in $\mathbf{C}^{N \times N}$,*

$$\|\hat{M}(\rho_1) - \hat{M}(\rho_2)\|_1 = \Omega(f),$$

where $\hat{M}$ is a POVM with respect to an ϵ-approximate $(4,4)$-design.

Theorems 4 and 1 together derandomize Theorem 3, as long as $f = \Omega(n^{-1/12})$.

The rest of this paper is structured as follows. In section 3, we compare different definitions of t-designs. Then, in section 4, we give our construction of approximate t-designs (Theorem 1). In section 5, we show how to use (4, 4)-designs for state-distinction (Theorem 4). These are the main results of our paper.

Some more technical claims are postponed to appendices. In appendix A, we derive expressions for expected values of monomials involving amplitudes of a quantum state drawn from Haar measure. In appendix B, we prove two theorems relating definitions of (t,t)-designs and in appendix C, we show how to implement POVM w.r.t. our (t,t)-design efficiently.

3 Definitions of (t,t)-designs

The earlier papers on (t,t)-designs used a different definition of (t,t)-designs, in terms of polynomials of the amplitudes of a state $|\phi_i\rangle$. In this section, we show that the two definitions are equivalent. We also present a condition on the polynomials of amplitudes which implies Definition 2.

Let $p(x_1, \ldots, x_N, y_1, \ldots, y_N)$ be a polynomial of degree at most t in variables $x_1, \ldots, x_N$ and degree at most t in variables $y_1, \ldots, Y_N$. For a state $|\psi\rangle = \sum_{j=1}^N \alpha_j |j\rangle$, we define

$$p(\psi) = p(\alpha_1, \ldots, \alpha_N, \alpha_1^*, \ldots, \alpha_N^*).$$

Definition 3 *A probability distribution over quantum states $(p_i, |\phi_i\rangle)$ is a complex projective (t,t)-design if, for arbitrary polynomial $p(x_1, \ldots, x_N, y_1, \ldots, y_N)$ of degree t in variables $x_1, \ldots, x_N$ and degree t in variables $y_1, \ldots, y_N$, we have*

$$\int_\psi p(\psi) d\psi = \sum_i p_i p(\phi_i), \tag{2}$$

where the integral over $|\psi\rangle$ on the left hand side is taken over the Haar measure on the unit sphere in $\mathbf{C}^N$.

Theorem 5 *$(p_i, |\phi_i\rangle)$ is a complex projective (t,t)-design according to Definition 1 if and only if it is a complex projective (t,t)-design according to Definition 3.*

Proof: In appendix B. $\blacksquare$

As shown in the Appendix A, the Haar-expectation of any unbalanced monomial p (i.e. monomial with $d_i \neq c_i$ for some $i \in \{1, \ldots, N\}$) is

$$\int_\psi p(\psi) d\psi = 0 \tag{3}$$

and the Haar-expectation of any monomial of the form

$$p = \prod_{j=1}^k x_{i_j}^{c_j} (x_{i_j}^*)^{c_j}$$

for distinct $x_{i_1}, \ldots, x_{i_k}$ is

$$\int_\psi p(\psi) d\psi = \frac{c_1! \ldots c_k!}{N(N+1)\ldots(N+d-1)} \tag{4}$$

We show that having an approximate version of these requirements is sufficient for an approximate (t,t)-design:

Theorem 6 *Assume that a probability distribution over quantum states $(p_i, |\phi_i\rangle)$ satisfies the following constraints:*

1. *$\sum_i p_i p(\phi_i) = 0$ for any unbalanced monomial p,*
2. $$\left| \sum_i p_i p(\phi_i) - \frac{c_1! \ldots c_k!}{N(N+1)\ldots(N+d-1)} \right| \leq \epsilon \frac{c_1! \ldots c_k!}{N(N+1)\ldots(N+d-1)}.$$

   for monomials $p = \prod_{j=1}^k x_{i_j}^{c_j} (x_{i_j}^*)^{c_j}$ with $c_1 + \ldots + c_k = d$ and $d \leq t$ and

3. $\sum_i p_i p(\phi_i) = \frac{1}{N}$ *for monomials* $p = x_j x_j^*$*, where* $j \in \{1, 2, \ldots, N\}$*.*

Then, $(p_i, |\phi_i\rangle)$ *is an* $t!\epsilon$*-approximate* (t,t)*-design.*

Proof: In appendix B. ∎

4 Constructing approximate (t,t)-designs

4.1 Main construction

In this section, we prove Theorem 1. It suffices to construct a set of states that satisfies the requirements of Theorem 6. For simplicity, assume that N is a power of 2. We use

Theorem 7 *[19] For any* $N = 2^k$*, there is a set* S *of* N^d *functions* $f : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ *such that, for any distinct* $k_1, \ldots, k_d \in \{0, \ldots, N-1\}$*, the probability distribution of* $f(k_1), \ldots, f(k_d)$ *(where* f *is chosen uniformly at random from* S*) is exactly the uniform distribution over tuples of* d *elements of* $\{0, \ldots, N-1\}$*.*

Such S are called *d-wise* independent sets. The second technical tool that we use is the Gaussian quadrature.

Lemma 1 *[7, Chapter 10.6] Let* X *be a real-valued random variable and* $c_i = E[X^i]$*, for* $i \in \{1, \ldots, 2t\}$*. Then, there exist real* $q_1, \ldots, q_{2t}$ *and* $x_1, \ldots, x_{2t}$ *such that* $q_i \geq 0$*,* $q_1 + \ldots + q_{2t} = 1$ *and*

$$\sum_{i=1}^{2t} q_i x_i^j = c_j,$$

for all $j \in \{1, \ldots, 2t\}$*.*

In other words, for any continuous probability distribution, we can always construct a discrete probability distribution with the first $2t$ moments having the same values.

Let $|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$ be a state drawn from the Haar measure. Let P_N be the probability distribution of α_1 and let $P = \lim_{N\to\infty} \sqrt{N} P_N$. Let α be drawn from P. We let $X = |\alpha|$ with probability 1/2 and $X = -|\alpha|$ with probability 1/2. Then, $E[X^j] = 0$ for odd j and

$$E[X^j] = \lim_{N\to\infty} N^{j/2} \cdot \frac{(j/2)!}{N(N+1)\ldots(N+j/2-1)} = (j/2)!$$

for even j. We apply Lemma 1 to get $q_1, \ldots, q_{2t}$ and $x_1, \ldots, x_{2t}$.

We then replace each q_i with one of the two closest multiples of $1/N$ (i.e., $\frac{\lfloor Nq_i \rfloor}{N}$ or $\frac{\lfloor Nq_i \rfloor + 1}{N}$) so that $q_1 + \ldots + q_{2t}$ remains 1. We simultaneously adjust x_i so that $q_i x_i^2$ stays the same. This changes the probabilities q_j by at most $1/N$ and x_j by at most a factor of $1 + O(1/N)$. The moments $\sum_i q_i x_i^j$ change by at most

$$\frac{2t}{N}(\max_i x_i^j - \min_i x_i^j) = O\left(\frac{1}{N}\right)$$

due to change in probabilities x_i and at most a multiplicative factor of $(1 + O(1/N))^t = 1 + O(1/N)$ due to change in x_j. Thus, we have

Claim 1

$$\left|E[X^{2c_j}] - c_j!\right| = O\left(\frac{1}{N}\right).$$

Let S_1 be a set of t-wise independent functions $f : \{1, \dots, N\} \to \{1, \dots, N\}$ and S_2 be a set of $2t$-wise independent functions $g : \{1, \dots, N\} \to \{1, \dots, N\}$.

We now consider the set of quantum states $|\psi_{f,g}\rangle = \sum_{j=1}^{N} \alpha_{f,g,j}|j\rangle$, (where $f \in S_1$, $g \in S_2$) generated in a following way:

1. Let $\beta_{f,g,j}$ be a complex number with absolute value $a_{f,j} = \frac{x_l}{\sqrt{N}}$ where l is such that $q_1 + \ldots + q_{l-1} < \frac{f(j)}{N} \le q_1 + \ldots + q_l$ and amplitude $e^{i\pi g(j)/N}$.
2. Let
$$\alpha_{f,g,j} = \frac{\beta_{f,g,j}}{\sqrt{\sum_{i=1}^{N} a_{f,i}^2}},$$
for $j \in \{1, \dots, N\}$.
3. Let
$$p_{f,g} = \frac{\sum_{i=1}^{N} a_{f,i}^2}{|S_1| \cdot |S_2|}.$$

We claim that $(p_{f,g}, |\psi_{f,g}\rangle)$ is an approximate (t, t)-design. We first show

Claim 2 *Fix $f \in S_1$. If we pick $|\psi\rangle = \sum_{j=1}^{N} \alpha_{f,g,j}|j\rangle$ uniformly at random from $|\psi_{f,g}\rangle$, $g \in S_2$, then*

1. *$E[h] = 0$ for any unbalanced monomial h of degree at most $2t$;*
2. $$E[h] = \prod_{j=1}^{k} \left(\frac{a_{f,i_j}}{\sqrt{\sum_{i=1}^{N} a_{f,i}^2}} \right)^{2c_j} \tag{5}$$
for a balanced monomial
$$h = (\alpha_{i_1}\alpha_{i_1}^*)^{c_1} \dots (\alpha_{i_k}\alpha_{i_k}^*)^{c_k}$$
of degree at most $2t$.

Proof: Let
$$h = \alpha_{i_1}^{c_1}(\alpha_{i_1}^*)^{d_1} \dots \alpha_{i_k}^{c_k}(\alpha_{i_k}^*)^{d_k}$$
be a monomial of degree $d = \sum_j (c_j + d_j)$ which is at most $2t$. Then, it contains at most $2t$ different variables $\alpha_{i_1}, \dots, \alpha_{i_k}$. Since g is picked from a $2t$-wise independent family of functions, phase of every of those variables is an independent random variable y_j taking values $1, e^{i\pi/N}, \dots, e^{i(2N-1)\pi/N}$ and
$$E[h] = \prod_{j=1}^{k} \left(\frac{a_{f,i_j}}{\sqrt{\sum_{i=1}^{N} a_{f,i}^2}} \right)^{c_j+d_j} \prod_{j=1}^{k} E[e^{i\pi y_j(c_j-d_j)/N}].$$

If, for some j, $c_j \neq d_j$, then the corresponding expectation $E[e^{i\pi y_j(c_j-d_j)/N}]$ is 0. This proves the first part of the claim. Otherwise, all expectations are 1 and the second part follows. ∎

The first part of the claim immediately implies that the first requirement of Theorem 6 is satisfied. To prove the second requirement, we first observe two facts about the normalization factor $\sqrt{\sum_{i=1}^N a_{f,i}^2}$:

1. We have
$$N \min_j x_j^2 \leq \sum_{i=1}^N a_{f,i}^2 \leq N \max_j x_j^2,$$
because each of $a_{f,i}$ is equal to one of x_j.

2. We have
$$Pr_f\left[\left|\sum_{i=1}^N a_{f,i}^2 - 1\right| \geq \frac{C}{\sqrt{N}}\right] \leq \frac{1}{C^2}. \tag{6}$$
To prove this bound, we first observe that $D[a_{f,i}^2] = E[a_{f,i}^4] - E^2[a_{f,i}^2] = 2! - (1!)^2 = 1$. Since the variables $a_{f,i}^2$ are t-wise independent (and, hence, 2-wise independent), we have $D[\sum_{i=1}^N a_{f,i}^2] = N$. The bound now follows from Chebyshev inequality.

We have to bound the expectation of the random variable
$$X' = \prod_{j=1}^k \left(\frac{a_{f,i_j}}{\sqrt{\sum_{i=1}^N a_{f,i}^2}}\right)^{2c_j}, \tag{7}$$
with $a_{f,i} = f(i)$, where $f \in S_1$ and the probability of f is equal to $|S_2|p_{f,g} = \frac{\sum_{i=1}^N a_{f,i}^2}{|S_1|}$. Equivalently, we can bound the expectation of
$$X = \frac{\prod_{j=1}^k a_{f,i_j}^{2c_j}}{(\sum_{i=1}^N a_{f,i}^2)^{d-1}}, \tag{8}$$
when each f is picked with probability $\frac{1}{|S_1|}$. We observe that
$$\frac{1}{N^d}\frac{\min_j^{2d} x_j}{\max_j^{2d-2} x_j} < X < \frac{1}{N^d}\frac{\max_j^{2d} x_j}{\min_j^{2d-2} x_j}.$$
Thus, the maximum and the minimum value of X differ by at most $\frac{D}{N^d}$ where $D = \frac{\min_j^{2d} x_j}{\max_j^{2d-2} x_j} - \frac{\max_j^{2d} x_j}{\min_j^{2d-2} x_j}$ is independent of N. We take $C = N^{1/6}$. If $|\sum_{i=1}^N a_{f,i}^2 - 1| \leq \frac{C}{\sqrt{N}}$, then
$$\left(1 - \frac{1}{N^{1/3}}\right)^{d-1} \prod_{j=1}^k a_{f,i_j}^{2c_j} \leq X \leq \left(1 + \frac{1}{N^{1/3}}\right)^{d-1} \prod_{j=1}^k a_{f,i_j}^{2c_j}.$$
Therefore,
$$\left(1 - \frac{1}{N^{1/3}}\right)^{d-1} E\left[\prod_{j=1}^k a_{f,i_j}^{2c_j}\right] - \frac{D}{N^d} Pr\left[\left|\sum_{i=1}^N a_{f,i}^2 - 1\right| \leq \frac{C}{\sqrt{N}}\right] \leq E[X]$$

$$\leq \left(1+\frac{1}{N^{1/3}}\right)^{d-1} E\left[\prod_{j=1}^{k} a_{f,i_j}^{2c_j}\right] + \frac{D}{N^d} Pr\left[\left|\sum_{i=1}^{N} a_{f,i}^2 - 1\right| \leq \frac{C}{\sqrt{N}}\right].$$

By equation (6),

$$Pr\left[\left|\sum_{i=1}^{N} a_{f,i}^2 - 1\right| \leq \frac{C}{\sqrt{N}}\right] \leq \frac{1}{C^2}.$$

Together with the independence of random variables $a_{f,i_j}^{2c_j}$ (which is implied by t-wise independence of a_{f,i_j} and $k \leq t$), this implies

$$\left(1-\frac{1}{N^{1/3}}\right)^{d-1} \prod_{j=1}^{k} E[a_{f,i_j}^{2c_j}] - \frac{D}{N^{d+1/3}} \leq E[X] \leq \left(1+\frac{1}{N^{1/3}}\right)^{d-1} \prod_{j=1}^{k} E[a_{f,i_j}^{2c_j}] + \frac{D}{N^{d+1/3}}.$$

The theorem now follows from claim 1.

To prove third requirement of Theorem 6, let $|\psi_{f,g}\rangle = \sum_{i=1}^{N} \alpha_{f,g,i}|i\rangle$. Then, the expectation of $x_j x_j^*$ is

$$\sum_{f,g} p_{f,g}\alpha_{f,g,i}\alpha_{f,g,i}^* = \sum_{f,g} \frac{\sum_{i=1}^{N}|\beta_{f,g,i}|^2}{|S_1|\cdot|S_2|} \frac{|\beta_{f,g,i}|^2}{\sum_{i=1}^{N}|\beta_{f,g,i}|^2} = \sum_{f,g} \frac{|\beta_{f,g,i}|^2}{|S_1|\cdot|S_2|}$$

which is just the expectation of $|\beta_{f,g,i}|^2$ when f, g are chosen uniformly at random. This expectation is $\sum_{l=1}^{2t} q_l \frac{x_l^2}{N} = \frac{1}{N}$, by the definition of the random variables x_j. This completes the proof of Theorem 1.

4.2 Improved construction

To decrease the number of states in the (t,t)-design, we use a result about approximately t-wise families of functions.

Definition 4 *A family of functions $f : \{0, \ldots, N-1\} \to \{0, \ldots, m-1\}$ is t-wise δ-dependent if, for any pairwise distinct $i_1, \ldots, i_t \in \{0, \ldots, N-1\}$, the variational distance between the probability distribution of $f(i_1), \ldots, f(i_t)$ and the uniform distribution on $\{0, \ldots, m-1\}^t$ is at most δ.*

Theorem 8 *[14] There is a family of t-wise δ-dependent functions $f : \{0, \ldots, N-1\} \to \{0,1\}$ of cardinality $2^{O(t+\log\log N+\log\frac{1}{\delta})}$.*

Instead of 0-1 valued functions, we will need m-valued functions. If $m = 2^k$, we can use the construction of [14] to construct a $t\log m$-wise δ-dependent family of functions $f' : \{0, \ldots, N\log m - 1\} \to \{0,1\}$ of cardinality $2^{O(t\log m+\log\log N+\log\frac{1}{\delta})}$. We then define $f(i)$ to be equal to the number formed by $f'(i\log N)$, $f'(i\log N+1)$, …, $f'(i\log N+\log N-1)$. This gives us a t-wise δ-dependent family of functions $f : \{0, \ldots, N-1\} \to \{0, \ldots, m-1\}$.

We also use

Theorem 9 *[1] There is a family of t-wise independent functions $f : \{0, \ldots, N-1\} \to \{0,1\}$ of cardinality $O(N^{t/2})$.*

We modify the previous construction in a following way:

- f is picked from a t-wise δ-dependent family of functions $f : \{0, \ldots, N-1\} \to \{0, \ldots, m-1\}$ (where m will be specified later). By the discussion after Theorem 8, such a family has cardinality $O(m^{ct}(\delta \log N)^c)$ for some constant c.
- g is replaced by two functions: $g_1 : \{0, \ldots, N-1\} \to \{0, 1\}$ and $g_2 : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$. g_1 is picked from a $2t$-wise independent family of functions of Theorem 9. g_2 is picked from a t-wise δ-dependent family of functions $\{0, \ldots, N-1\} \to \{0, \ldots, m-1\}$. Instead of $e^{2i\pi g(j)/N}$, our phase is $(-1)^{g_1(j)} e^{2i\pi g_2(j)/m}$.

The number of states in our sample size is then $O(N^t m^{ct}(\log N/\delta)^c)$ for some constant c. We will take $\delta = O(\epsilon)$ and $m = \Omega(1/\epsilon)$. This gives a design with $O(N^t(\log N/\epsilon)^c)$ states. We claim that this gives us an ϵ-approximate (t, t)-design.

The argument is the same as in section 4.1, with the following changes:

1. In Claim 1, we have $O(\frac{1}{mN^{c_j}})$ instead of $O(\frac{1}{N^{c_j+1}})$.
2. In Claim 2, for monomials that contain $\alpha_i^c(\alpha_i^*)^d$ with $c+d$ odd, the expectation is still exactly 0, because of the $(-1)^{g_1(j)}$ multiplier which is 1 with probability 1/2 and -1 with probability 1/2. For monomials
$$h = \alpha_{i_1}^{c_1}(\alpha_{i_1}^*)^{d_1} \ldots \alpha_{i_k}^{c_k}(\alpha_{i_k}^*)^{d_k} \tag{9}$$
with c_1+d_1, ..., c_k+d_k all even, the $(-1)^{g_1(j)}$ term is always 1. Since g_2 is t-wise δ-dependent, the expectation of h for a fixed f deviates from the expectation for t-wise independent g_2 by at most $c\delta$ times
$$\prod_{j=1}^{k} \left(\frac{a_{f,i_j}}{\sqrt{\sum_{i=1}^{N} a_{f,i}^2}} \right)^{c_j+d_j} \tag{10}$$
for some constant c.
3. We then have to bound the expectation of X' (equation (7)) which can be replaced by the expectation of X (equation (8)) in the same way as before. The only change is that f is now chosen from a t-wise δ-dependent distribution. This means that the expectation of
$$\prod_{j=1}^{k} \left(\frac{a_{f,i_j}}{\sqrt{\sum_{i=1}^{N} a_{f,i}^2}} \right)^{c_j+d_j}$$
differs from the expectation under a t-wise independent distribution by at most $\frac{D\delta}{N^d}$.

Overall, this introduces an additional error of order $c(\max \frac{1}{m}, \delta)$ times the expectation of (10). Thus, choosing $\delta = O(\epsilon)$ and $m = \Omega(1/\epsilon)$ with appropriate constants is sufficient for an ϵ-approximate design.

To complete the proof, we have to verify that Theorem 6 works, when, instead of an assumption about balanced terms, we just have an assumption about terms of the form (9). This part is mostly technical and is omitted in this version.

5 Derandomizing the measurement in a random basis

In this section, we prove theorem 4. First, we consider the case when we have an exact $(4, 4)$-design instead of an approximate one. By the definition of POVM,

$$\|\hat{M}(\rho_1) - \hat{M}(\rho_2)\|_1 = \sum_{j=1}^{L} N p_j \, |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle|$$

where L is the number of states in the $(4, 4)$-design. Theorem 4 now follows from

Lemma 2

$$\sum_{j=1}^{L} p_j \, |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle| = \Omega\left(\frac{f}{N}\right).$$

To prove Lemma 2, we use the fourth moment method of Berger [4]:

Lemma 3 *[4] For any random variable S,*

$$E[|S|] \geq \frac{E[S^2]^{3/2}}{E[S^4]^{1/2}}.$$

This means that

$$\sum_{j=1}^{L} p_j \, |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle| \, \frac{(\sum_{j=1}^{L} p_j \, |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle|^2)^{3/2}}{(\sum_{j=1}^{L} p_j \, |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle|^4)^{1/2}}.$$

We now bound the numerator and the denominator of this expression. We first observe that

$$\sum_{j=1}^{L} p_j |\langle \phi_j | \rho_1 - \rho_2 | \phi_j \rangle|^2 = E_{|\phi\rangle} |\langle \phi | \rho_1 - \rho_2 | \phi \rangle|^2 \tag{11}$$

with $|\phi\rangle$ on the right hand side chosen according to the Haar measure. (Let $|\phi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$. Then, equation (11) is true because $|\langle \phi | \rho_1 - \rho_2 | \phi \rangle|^2$ is a polynomial of degree 2 in variables α_i and degree 2 in variables α_i^* and, therefore, its expectation is the same for Haar measure and for a $(4, 4)$-design.) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $\rho_1 - \rho_2$. Then,

$$\lambda_1 + \ldots + \lambda_N = Tr(\rho_1) - Tr(\rho_2) = 0, \tag{12}$$

$$\lambda_1^2 + \ldots + \lambda_N^2 = \|\rho_1 - \rho_2\|_F = f^2.$$

For the moment, assume that $\rho_1 - \rho_2$ is diagonal in the basis $|1\rangle$, ..., $|N\rangle$ and $|i\rangle$ is the eigenvector with the eigenvalue λ_i. By writing out $g(\phi) = (\langle \phi | \rho_1 - \rho_2 | \phi \rangle)^2$ for $|\phi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$, we get that $g(\phi)$ is equal to

$$\sum_{i=1}^{N} \lambda_i^2 (\alpha_i \alpha_i^*)^2 + 2 \sum_{\substack{i,j=1 \\ i<j}}^{N} \lambda_i \lambda_{i-1} \alpha_i \alpha_i^* \alpha_j \alpha_j^*$$

plus some unbalanced terms. When $|\phi\rangle$ is picked from the Haar measure, the expectation of each unbalanced term is 0. The expectation of balanced terms is given by equation (4). This gives us

$$E_{|\phi\rangle}[g] = \frac{2}{N(N+1)} \sum_{i=1}^{N} \lambda_i^2 + \frac{1}{N(N+1)} 2 \sum_{\substack{i,j=1 \\ i<j}}^{N} \lambda_i \lambda_{i-1} =$$

$$\frac{1}{N(N+1)} \left(\sum_{i=1}^{N} \lambda_i \right)^2 + \frac{1}{N(N+1)} \sum_{i=1}^{N} \lambda_i^2 = \frac{f^2}{N(N+1)}. \tag{13}$$

If $\rho_1 - \rho_2$ is not diagonal in the basis $|1\rangle, \ldots, |N\rangle$, let U be a unitary transformation that maps $|1\rangle, \ldots, |N\rangle$ to the eigenbasis of $\rho_1 - \rho_2$. Then,

$$E(\langle\phi|\rho_1 - \rho_2|\phi\rangle)^2 = E(\langle\phi|U^\dagger(\rho_1 - \rho_2)U|\phi\rangle)^2,$$

by the invariance of Haar measure under unitary transformations and $U^\dagger(\rho_1 - \rho_2)U$ is diagonal in the basis $|1\rangle, \ldots, |N\rangle$. Thus, the expression (13) for the expectation remains the same even if $\rho_1 - \rho_2$ is not diagonal in the basis $|1\rangle, \ldots, |N\rangle$.

The expectation of g must be the same if $|\phi\rangle$ is picked from a (4, 4)-design. Therefore,

$$\sum_{j=1}^{L} p_j (\langle\phi_j|\rho_1 - \rho_2|\phi_j\rangle)^2 = \frac{f^2}{N(N+1)}. \tag{14}$$

Similarly,

$$\sum_{j=1}^{L} p_j (\langle\phi_j|\rho_1 - \rho_2|\phi_j\rangle)^4 = E(\langle\phi|\rho_1 - \rho_2|\phi\rangle)^4 = E \left(\sum_{i=1}^{n} \lambda_i \alpha_i \alpha_i^* \right)^4. \tag{15}$$

For the second equality, we again assumed that $\rho_1 - \rho_2$ is diagonal in the basis $|1\rangle, \ldots, |N\rangle$. This assumption can be removed in the same way as before.

Denote $v_i = \lambda_i \alpha_i \alpha_i^*$. Let $N^{\overline{4}}$ be a shortcut for $N(N+1)(N+2)(N+3)$. Then, (15) is equal to

$$E \left[\sum_{i=1}^{N} v_i^4 + \sum_{\substack{i,j=1 \\ i \neq j}}^{N} 4 v_i^3 v_j + \sum_{\substack{i,j=1 \\ i<j}}^{N} 6 v_i^2 v_j^2 + \sum_{\substack{i,j,k=1 \\ j<k, i\neq j, i\neq k}}^{N} 12 v_i^2 v_j v_k + \sum_{\substack{i,j,k,l=1 \\ i<j<k<l}}^{N} 24 v_i v_j v_k v_l \right] =$$

$$\frac{24}{N^{\overline{4}}} \left(\sum_{i=1}^{n} \lambda_i^4 + \sum_{\substack{i,j=1 \\ i \neq j}}^{N} \lambda_i^3 \lambda_j + \sum_{\substack{i,j=1 \\ i<j}}^{N} \lambda_i^2 \lambda_j^2 + \sum_{\substack{i,j,k=1 \\ j<k, i\neq j, i\neq k}}^{N} \lambda_i^2 \lambda_j \lambda_k + \sum_{\substack{i,j,k,l=1 \\ i<j<k<l}}^{N} \lambda_i \lambda_j \lambda_k \lambda_l \right) =$$

$$\frac{1}{N^{\overline{4}}} \left(\sum_{i=1}^{N} \lambda_i \right)^4 + \frac{6}{N^{\overline{4}}} \left(\sum_{i=1}^{N} \lambda_i \right)^2 \left(\sum_{i=1}^{N} \lambda_i^2 \right) +$$

$$\frac{8}{N^{\overline{4}}} \left(\sum_{i=1}^{N} \lambda_i \right) \left(\sum_{i=1}^{N} \lambda_i^3 \right) + \frac{9}{N^{\overline{4}}} \sum_{i=1}^{N} \lambda_i^4 + \frac{6}{N^{\overline{4}}} \sum_{\substack{i,j=1 \\ i<j}}^{N} \lambda_i^2 \lambda_j^2 =$$

$$\frac{9}{N^4}\sum_{i=1}^N \lambda_i^4 + \frac{6}{N^4}\sum_{\substack{i,j=1\\ i<j}}^N \lambda_i^2\lambda_j^2 \leq \frac{9}{N^4}\left(\sum_{i=1}^N \lambda_i^2\right)^2 = \frac{9}{N^4}f^4, \tag{16}$$

with the first equality following from equation (4), the second equality following by a rearrangement of terms, the third equality following from (12) and the inequality following by expanding $\left(\sum_{i=1}^N \lambda_i^2\right)^2$ and using $\lambda_i^2\lambda_j^2 \geq 0$ for all i, j.

By combining Lemma 3 and equations (14), (15) and (16), we get

$$\sum_{j=1}^L p_j\, |\langle\phi_j|\rho_1 - \rho_2|\phi_j\rangle| \geq \frac{(\frac{f^2}{N(N+1)})^{3/2}}{(\frac{9f^4}{N(N+1)(N+2)(N+3)})^{1/2}} \geq \frac{f}{3N}.$$

This implies Lemma 2 in the case when we have an exact $(4,4)$-design.

For the case of ϵ-approximate $(4,4)$-design, we bound the difference between the expectations of $(\langle\phi|\rho_1-\rho_2|\phi\rangle)^2$ and $(\langle\phi|\rho_1-\rho_2|\phi\rangle)^4$ when $|\phi\rangle$ is drawn from the Haar measure and when it is drawn from an approximate $(4,4)$-design. We can rewrite

$$(\langle\phi|\rho_1-\rho_2|\phi\rangle)^2 = \sum_j \lambda_j(\langle\phi|\varphi_j\rangle\langle\varphi_j|\phi\rangle)^2 \tag{17}$$

where λ_j are eigenvalues of $\rho_1-\rho_2$ and $|\varphi_j\rangle$ are the corresponding eigenvectors. By the definition of (t,t)-design, the expectation of

$$(\langle\phi|\varphi_j\rangle\langle\varphi_j|\phi\rangle)^2 = \langle\varphi_j^{\otimes 2}|(|\phi\rangle\langle\phi|)^{\otimes 2}|\varphi_j^{\otimes 2}\rangle$$

changes by at most $\frac{\epsilon}{M}$ (where M is the dimension of symmetric subspace $\mathcal{H}_{sym}$ for 2 copies of a state $|\phi\rangle$) when $|\phi\rangle$ is picked from an ϵ-approximate $(4,4)$ design. The entire sum (17) changes by at most

$$\sum_j |\lambda_j|\frac{\epsilon}{M} \leq \frac{2\epsilon}{M},$$

where the inequality follows from the sum of all positive eigenvalues of $\rho_1-\rho_2$ being at most $Tr\rho_1 = 1$ and the sum of absolute values of negative eigenvalues being at most $Tr\rho_2 = 1$. Since $M \geq \frac{N^2}{2}$, this is at most $\frac{4\epsilon}{N^2}$.

Similarly, we can show that the expectation of $(\langle\phi|\rho_1-\rho_2|\phi\rangle)^4$ changes by at most $\frac{2\cdot 4!\epsilon}{N^4}$ when $|\phi\rangle$ is picked from an ϵ-approximate $(4,4)$ design. For our proof to work, those changes have to be small compared to the expectations of $(\langle\phi|\rho_1-\rho_2|\phi\rangle)^2$ and $(\langle\phi|\rho_1-\rho_2|\phi\rangle)^4$ when $|\phi\rangle$ is picked from the Haar measure. This happens if $\epsilon < cf^4$ for a sufficiently small constant c.

5.1 $(2,2)$-designs are not sufficient

We note that using a $(4,4)$-design is essential for our construction. First, as shown by Berger [4], a bound on the fourth moment is necessary to obtain a bound on $E[|S|]$. Second, some well-known $(2,2)$-designs are insufficient for distinguishing between some orthogonal quantum states.

For example, this is true for $(2,2)$-designs constructed from mutually unbiased bases [11]. Let $|\phi_1\rangle$, ..., $|\phi_N\rangle$ be an orthonormal basis for an N-dimensional Hilbert space and $|\varphi_1\rangle$, ..., $|\varphi_N\rangle$ be another orthonormal basis for the same space. The two bases are *mutually unbiased* if $|\langle\phi_i|\varphi_j\rangle| =$

$\frac{1}{\sqrt{N}}$ for all i, j. If N is prime, there exist $N+1$ orthonormal bases $|\phi_{i,1}\rangle$, …, $|\phi_{i,N}\rangle$ (for $i \in \{1, \ldots, N+1\}$) such that any two of them are mutually unbiased. The collection of states $|\phi_{i,j}\rangle$ (with probabilities $1/N(N+1)$ each) is then a $(2,2)$-design [11].

We now consider the POVM corresponding to this $(2,2)$-design. This POVM is equivalent to randomly choosing $i \in \{1, \ldots, N+1\}$ (with probabilities $1/(N+1)$ each) and then performing an orthogonal measurement in the basis $|\phi_{i,1}\rangle$, …, $|\phi_{i,N}\rangle$.

Let $|\psi_1\rangle = |\phi_{1,1}\rangle$, $|\psi_2\rangle = |\phi_{1,2}\rangle$. Then, measuring in the first basis perfectly distinguishes the states $|\psi_1\rangle$ and $|\psi_2\rangle$ but measuring either of those states in any other basis $|\phi_{i,1}\rangle, \ldots, |\phi_{i,N}\rangle$ produces the uniform probability distribution. Therefore, performing the POVM on $|\psi_1\rangle$ and $|\psi_2\rangle$ produces two probability distributions with the variational distance $2/(N+1)$ between them.

However, since $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, we have $\| |\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2| \|_F = 2$.

6 Open problems

It appears plausible that the methods developed above can be applied to construct approximate t-designs for unitary transformations (defined in [5]). An important set of open questions is whether the efficient approximate t-designs developed above can be applied to derandomize other protocols that make use of random states and/or random unitary operators, for example, the protocol for locking classical correlations [8].

Acknowledgments. We thank Oded Regev for suggesting to use Gaussian quadrature and Robin Blume-Kohout, Aram Harrow, Debbie Leung, Pranab Sen and Andreas Winter for discussions and comments on this paper.

References

[1] N. Alon, L. Babai, A. Itai. A fast and simple algorithm for the maximal independent set problem. *Journal of Algorithms*, 7:567-583, 1986.

[2] B. Bajnok. Construction of spherical t-designs. *Geom. Dedicata*, 43:167-179, 1992.

[3] H. Barnum. Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases. ArXiv.org Preprint quant-ph/0205155, 2002.

[4] B. Berger. The fourth moment method. *SIAM Journal on Computing*, 26:1188-1207, 1997.

[5] C. Danker, R. Cleve, J. Emerson, E. Livine. Exact and Approximate Unitary 2-designs: Constructions and Applications. quant-ph/0606161.

[6] P. Delsarte, J. Goethals, J. Seidel. Spherical codes and designs. *Geom. Dedicata*, 6:363-388, 1977.

[7] R. Hamming. *Numerical methods for scientists and engineers.* McGraw-Hill, 1966.

[8] P. Hayden, D. Leung, P. Shor, A. Winter. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.*, 250(2):371-391, 2004. quant-ph/0307104.

[9] A. Hayashi, T. Hashimoto, M. Horibe. Reexamination of optimal quantum state estimation of pure states. *Phys. Rev. A*, 72: 032325, 2006. Also quant-ph/0410207.

[10] S. Iblisdir, J. Roland. Optimal finite measurements and Gauss quadratures. *Phys. Lett. A*, 358(5-6):368-372, 2006. Also quant-ph/0410237.

[11] Andreas Klappenecker and Martin Roetteler. Mutually unbiased bases are complex projective 2-designs. ArXiv.org Preprint quant-ph/0502031, 2005.

[12] Andreas Klappenecker, Martin Roetteler, Igor E. Shparlinski, and Arne Winterhof, On Approximately Symmetric Informationally Complete Positive Operator-Valued Measures and Related Systems of Quantum States, quant-ph/0503239.

[13] J. Korevaar, J. Meyers. Chebyshev-type quadrature on multidimensional domains. *Journal of Approximation Theory*, 79:144-164, 1994.

[14] J. Naor, M. Naor, Small-bias probability spaces: Efficient constructions and applications, *SIAM J. Computing*, 22: 838-856, 1993.

[15] J. Radhakrishnan, M. Rotteler, P. Sen, On the power of random bases in Fourier sampling, *ICALP'05* and quant-ph/0503114.

[16] J. Renes, R. Blume-Kohout, A. Scott, C. Caves, J. Math. Phys. 45(6):2171-2180 (2004).

[17] P. Sen, Random measurement bases, quantum state distinction and applications to the hidden subgroup problem, *Complexity'06* and quant-ph/0512085.

[18] N. Ullah, Nucl. Phys. 58:65, 1964.

[19] D. Zuckerman. Lecture notes for CS 395T - Pseudorandomness and Combinatorial Constructions (Spring 2001), `http://www.cs.utexas.edu/users/diz/395T/01/`, Lecture 5.

Appendix

A Haar Average of State-Component Monomials

Consider the N-dimensional Hilbert space, $\mathcal{H} = \mathbf{C^N}$ consisting of the set of normalized pure quantum states. These states correspond to the points of a unit sphere S^{2N-1} which is the "surface" of a ball in $2N$ real dimensions. If we remove the arbitrary and unphysical phase associated with each state then we are left with the complex projective space CP^{N-1}. In either case there exists a unique natural measure that is induced by the invariant (Haar) measure on the unitary group $U(N)$: a uniformly random pure state can be defined by the action of a uniformly random unitary matrix on an arbitrary reference state, $|\phi\rangle = U|\phi_0\rangle$. The measure on pure states is distinguished by the rotational invariance of the Haar measure. This measure, which I will denote $\mu(\psi)$, is equivalent to the uniform measure on the unit sphere S^{2N-1}. Choosing a fixed representation, $|\psi\rangle = \sum_i c_i|i\rangle$, the uniform measure for normalized vectors (pure states) in $\mathcal{H}$ can be expressed using the Euclidean parametrization,

$$d\mu(\psi \in S^{2N-1}) = \left(\Pi_{i=1}^N d^2c_i\right) \delta\left(\sum_{l=1}^N |c_l|^2 - 1\right) \tag{18}$$

where δ is the Dirac delta function.

The average value of any function $f : \mathcal{H} \to \mathbf{C}$ takes the explicit form,

$$\langle f(\psi)\rangle_\psi \;= \tfrac{1}{V_{S^{2N-1}}} \textstyle\int_{S^{2N-1}} f(\psi)\, d\mu(\psi \in S^{2N-1}). \tag{19}$$

Often the function can be represented or approximated as a polynomial in the components of the pure state. The terms of such a polynomial may be calculated directly using the Euclidean measure (18) by using an integration trick [18]. Consider first calculating the volume of pure states. We have,

$$\begin{aligned} V_{S^{2N-1}} &= \int_{\psi\in S^{2N-1}} d\mu(\psi) \\ &= \int_{\psi\in S^{2N-1}} \left(\Pi_{i=1}^N d^2u_i\right) r^{-2N+1}\delta\left(\sqrt{\sum |u_l|^2} - r\right) \end{aligned} \tag{20}$$

where we have made the change of variables $c_i = u_i/r$, and used the identity $\delta(a/b-1) = b\delta(a-b)$. (Notice that for calculating the volume of the $2N-1$ sphere one has to be careful about distinguishing the constraint $\delta\left(\sum_{l=1}^N |u_l|^2 - r\right)$ from $\delta(\sqrt{\sum_{l=1}^N |u_l|^2} - r)$ for the variable radius $r^2 = \sum_{l=1}^N |c_l|^2$.) Collecting factors of r on the left hand side, the main trick for evaluating this integral is to introduce the integrating factor $\exp(-r^2)dr$ and then integrate both sides with respect to r,

$$\begin{aligned} V_{S^{2N-1}} \int_0^\infty dr\; r^{2N-1} \exp(-r^2) &= \int \Pi_{i=1}^N d^2u_i\; e^{-\sum_{j=1}^N |u_j|^2} \\ V_{S^{2N-1}} \frac{\Gamma(N)}{2} &= \left[\Gamma\left(\frac{1}{2}\right)\right]^{2N} = \pi^N \\ V_{S^{2N-1}} &= \frac{2\pi^N}{(N-1)!} \end{aligned} \tag{21}$$

where we've used the integral identity $\int_0^\infty r^q e^{-r^2} = (1/2)\Gamma(q+1/2)$, and recovered the well-known result for the volume of the unit R sphere in $R+1$ real dimensions: $V_{S^R} = 2\pi^{R/2}/(R/2-1)!$ with $R = 2N$.

Now we can calculate the correlation function for a k-body product of distinct state components,

$$I(k,t) \equiv \langle |c_1|^{2t_1}|c_2|^{2t_2}\cdots|c_k|^{2t_k}\rangle = \frac{1}{V_{S^{2N-1}}}\int_{\psi\in S^{2N-1}} d\mu(\psi)\; |c_1|^{2t_1}|c_2|^{2t_2}\cdots|c_k|^{2t_k}, \tag{22}$$

which corresponds to the expectation of a homogeneous polynomial of degree (t,t), where $t = \sum_{j=1}^k t_j$. By the same method as above we obtain,

$$\begin{aligned}
I(k,t)\; V_{S^{2N-1}} \int_0^\infty dr\; r^{2N-1+2\sum t_j}\exp(-r^2) &= \int \Pi_{i=1}^N d^2u_i\; e^{-\sum_{l=1}^N |u_l|^2}\Pi_{j=1}^k |u_j|^{2t_j} \\
I(k,t)\frac{2\pi^N}{(N-1)!}\frac{\Gamma(N+\sum t_j)}{2} &= \left[\int d^2u\; e^{-|u|^2}\right]^{N-k} \Pi_{j=1}^k \int d^2u_j\; e^{-|u_j|^2}|u_j|^{2t_j} \\
I(k,t) &= \frac{(N-1)!}{\pi^k(N+t-1)!}\,\Pi_{j=1}^k\int d^2u_j\; e^{-|u_j|^2}|u_j|^{2t_j}. \qquad (23)
\end{aligned}$$

where in the last line we've used

$$\left[\int d^2u\; e^{-|u|^2}\right]^{N-k} = (\pi)^{N-k}. \tag{24}$$

In order to evaluate the remaining factor we change to polar coordinates, with $u_j = x+iy$, and $dxdy = rdrd\theta$, giving for each u_j the factor,

$$\int d^2u_j\; e^{-|u_j|^2}|u_j|^{2t_j} = 2\pi\int_0^\infty dr\; e^{-|u_j|^2}r^{2t_j} = 2\pi\Gamma(t_j+1)/2 = \pi t_j!. \tag{25}$$

Hence,

$$\langle |c_1|^{2t_1}|c_2|^{2t_2}\cdots|c_k|^{2t_k}\rangle = \frac{t_1!t_2!\cdots t_k!}{(N+t-1)(N+t-2)\cdots(N)}. \tag{26}$$

B Proofs of Theorems from section 3

Proof: [of Theorem 5]

In Definition 3, instead of a general polynomial p, it suffices to consider the case when p is a monomial

$$x_1^{c_1}x_2^{c_2}\ldots x_N^{c_N}y_1^{d_1}y_2^{d_2}\ldots y_N^{d_N}.$$

If the equation (2) is true for all monomials p, it will also be true for all polynomials p.

To see the equivalence with Definition 1, observe that each entry of the density matrix $\sum_i p_i(|\phi_i\rangle\langle\phi_i|)^{\otimes t}$ is an expectation of a monomial in the amplitudes of $|\phi_i\rangle$ and the corresponding entry of $\int_\psi(|\psi\rangle\langle\psi|)^{\otimes t}d\psi$ is the expectation of the same monomial when $|\psi\rangle$ is picked from the Haar measure. Thus, if the expectations are the same for any monomial, the density matrices $\sum_i p_i(|\phi_i\rangle\langle\phi_i|)^{\otimes t}$ and $\int_\psi(|\psi\rangle\langle\psi|)^{\otimes t}d\psi$ are the same and Definition 1 holds.

In the other direction, for every monomial of degree t in variables α_i and degree t in variables α_i^*, there is an entry in $\int_\psi(|\psi\rangle\langle\psi|)^{\otimes t}d\psi$ which is equal to its expectation. Therefore, Definition 1 also implies Definition 3. $\blacksquare$

Proof: [of Theorem 6] Let $\mathcal{H}_{sym}$ be the subspace spanned by all states of the form $|\psi\rangle^{\otimes t}$.

Then, $\int_\psi (|\psi\rangle\langle\psi|)^{\otimes t} d\psi$ is just $\frac{I}{M}$, the completely mixed state over the subspace $\mathcal{H}_{sym}$ (where $M = \dim \mathcal{H}_{sym}$). We need to prove that, for any $|\psi_{sym}\rangle \in \mathcal{H}_{sym}$,

$$\frac{1-\epsilon}{M} \leq E\left[\langle\psi_{sym}| \left(p_i |\phi_i\rangle\langle\phi_i|^{\otimes t}\right) |\psi_{sym}\rangle\right] \leq \frac{1+\epsilon}{M}. \tag{27}$$

We can write any state $|\psi_{sym}\rangle \in \mathcal{H}_{sym}$ as

$$|\psi_{sym}\rangle = \sum_{i_1 \leq i_2 \leq \ldots \leq i_t} \alpha_{i_1,\ldots,i_t} |\psi_{i_1,\ldots,i_t}\rangle,$$

where $|\psi_{i_1,\ldots,i_t}\rangle$ is the uniform superposition over all basis states $|j_1,\ldots,j_t\rangle$ such that the multisets $\{i_1,\ldots,i_t\}$ and $\{j_1,\ldots,j_t\}$ are equal.

Let $d_{i_1,\ldots,i_t}$ be the number of different basis states $|j_1,\ldots,j_t\rangle$ such that the multiset $\{j_1,\ldots,j_t\}$ is equal to $\{i_1,\ldots,i_t\}$. (If there are k different elements in $\{i_1,\ldots,i_t\}$, occurring $c_1,\ldots,c_k$ times, then $d_{i_1,\ldots,i_t} = \frac{t!}{c_1!\ldots c_k!}$.) Then, each of $|j_1,\ldots,j_t\rangle$ has the amplitude of $\frac{1}{\sqrt{d_{i_1,\ldots,i_t}}}$ in the state $|\psi_{i_1,\ldots,i_t}\rangle$. Let $\alpha_1,\ldots,\alpha_N$ be the amplitudes of a state $|\psi\rangle = \sum_j \alpha_j |j\rangle$ which is picked from the distribution $(p_i, |\phi_i\rangle)$. Then,

$$\langle\psi_{i_1,\ldots,i_t}|\psi_i\rangle = d_{i_1,\ldots,i_t} \cdot \frac{1}{\sqrt{d_{i_1,\ldots,i_t}}} \langle i_1,\ldots,i_t|\phi_i\rangle = \sqrt{d_{i_1,\ldots,i_t}}\alpha_{i_1}\ldots\alpha_{i_t}.$$

By summing over all components $|\psi_{i_1,\ldots,i_t}\rangle$ of $|\psi_{sym}\rangle$, we get that

$$\langle\psi_{sym}||\phi_i\rangle\langle\phi_i|^{\otimes t}|\psi_{sym}\rangle =$$

$$\left(\sum_{i_1\leq\ldots\leq i_t} \alpha^*_{i_1,\ldots,i_t} \sqrt{d_{i_1,\ldots,i_t}} \alpha_{i_1}\ldots\alpha_{i_t}\right) \left(\sum_{j_1\leq\ldots\leq j_t} \alpha_{j_1,\ldots,j_t} \sqrt{d_{j_1,\ldots,j_t}} \alpha^*_{j_1}\ldots\alpha^*_{j_t}\right). \tag{28}$$

If $|\psi\rangle$ was picked from the Haar measure, the expectation of (28) would be $\frac{1}{M}$. Thus, it suffices to bound the difference of the expected value of (28) between the two cases: $|\psi\rangle$ picked from Haar measure and $|\psi\rangle$ picked from $(p_i, |\phi_i\rangle)$.

We expand both sums in the equation (28). If $j_l \neq i_l$ for some $l \in \{1,\ldots,t\}$, then the expectation of a term

$$\alpha_{i_1}\ldots\alpha_{i_t}\alpha^*_{j_1}\ldots\alpha^*_{j_t} \tag{29}$$

is 0 in both cases. When $j_l = i_l$ for all $l \in \{1,\ldots,k\}$, the expectations of (29) under both distributions differ by at most

$$\epsilon \frac{c_1!\ldots c_k!}{N(N+1)\ldots(N+d-1)} d_{i_1,\ldots,i_t} |\alpha_{i_1,\ldots,i_t}|^2.$$

Since the squared amplitudes $|\alpha_{i_1,\ldots,i_t}|^2$ sum up to 1, this means that the difference between expectation of (28) in the two cases is at most

$$\epsilon \frac{c_1!\ldots c_k!}{N(N+1)\ldots(N+d-1)} d_{i_1,\ldots,i_t} = \epsilon \frac{t!}{N(N+1)\ldots(N+d-1)}.$$

∎

C Efficient implementation

In this section, we show how to implement (an approximation) of the POVM w.r.t. one-dimensional projectors $E_{f,g} = p_{f,g}N|\psi_{f,g}\rangle\langle\psi_{f,g}|$ efficiently.

For this construction, we will need to use the particular family of t-wise independent functions from [19]. Let G be a finite field with N elements (which exists because we constrained N to be power of 2). We associate $\{0, \ldots, N-1\}$ with the elements of G. Using the construction of [19] results in $f(x)$ ranging over all polynomials (in x) over G of degree at most $t-1$ and $g(x)$ ranging over all polynomials over G of degree at most $2t-1$.

We have $E_{f,g} = E_g E_f$ where

1. E_f is a diagonal matrix, with the entries $(E_f)_{j,j} = \frac{1}{N^{t-1}} a_{f,j}^2$ on the diagonal;
2. $E_g = \frac{1}{N^{2t-1}}|\psi_g\rangle\langle\psi_g|$ where $|\psi_g\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{2\pi i\frac{g(j)}{N}}|j\rangle$.

Both E_f and E_g constitute a POVM. Thus, we can perform the measurement in two steps, first measuring E_f and then measuring E_g.

The POVM E_f can be implemented as follows. Let $c_1, \ldots, c_{t-1}$ be arbitrary and let $f_j(x) = c_{t-1}x^{t-1} + \ldots + c_1 x + j$. Then, for each i and each $l \in \{0, \ldots, N-1\}$, there is exactly one j such that $f_j(i) = l$. This means that, for each i,

$$\sum_j a_{f_j,i}^2 = N \sum_{l=1}^{2t} q_l \frac{x_l^2}{N} = 1$$

and $\sum_j E_{f_j} = \frac{I}{N^{t-1}}$.

Thus, $(c_1, \ldots, c_{t-1})$ is a uniformly random $(t-1)$-tuple of elements of $\{0, 1, \ldots, N-1\}$. Let $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$ be the state that is being measured w.r.t. E_f. To measure c_0 (after "measuring" $c_1, \ldots, c_{t-1}$), we first create an ancilla state

$$\sum_{l=1}^{2t} \frac{x_l}{\sqrt{N}} \sum_{i=N(q_1+q_2+\ldots+q_{l-1})+1}^{N(q_1+q_2+\ldots+q_l)} |i\rangle.$$

We then compute $m = c_{t-1}j^{t-1} + \ldots + c_1 j$, perform the transformation $|i\rangle \to |i-m\rangle$, uncompute m and measure $c = i - m$.

Conditional on obtaining outcome c, this results in the transformation $U_c|j\rangle = \frac{x_l}{\sqrt{N}}|j\rangle$ where l is such that

$$q_1 + \ldots + q_{l-1} < \frac{f_c(j)}{N} \leq q_1 + \ldots + q_l.$$

By definition of $a_{f,j}$, we have $a_{f_c,j} = \frac{x_l}{\sqrt{N}}$. Thus, $U_c|j\rangle = a_{f_c,j}|j\rangle$. The corresponding measurement operator is $E_c = U_c U_c^\dagger$. We have $E_{f_c} = \frac{1}{N^{t-1}} E_c$. Thus, taking $c_0 = c$ results in a correct implementation of the POVM E_f.

Next, we show how to measure E_g. Let $d_0, d_2, \ldots, d_{t-1}$ be arbitrary but fixed and $g_j(x) = d_0 + jx + d_2x^2 + \ldots + d_{2t-1}x^{2t-1}$.

Let $U_{g_0}|j\rangle = e^{2\pi i\frac{g_0(j)}{N}}|j\rangle$. Then, $U_{g_0}|\psi'_l\rangle = |\psi_{g_l}\rangle$ where

$$|\psi'_l\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i\frac{jl}{N}}|j\rangle$$

are just the vectors of Fourier basis. This has two consequences. First,

$$\sum_{l=0}^{N-1} |\psi_{g_l}\rangle\langle\psi_{g_l}| = U_{g_0}\left(\sum_{l=0}^{N-1} |\psi'_l\rangle\langle\psi'_l|\right) U_{g_0}^{\dagger} = U_{g_0} I U_{g_0}^{\dagger} = I.$$

Therefore, $(d_0, d_2, \ldots, d_{2t-1})$ is just a uniformly random vector of $2t-1$ values from $\{0, \ldots, N-1\}$ which can be generated by producing the uniform superposition of all $|d_0, d_2, d_3, \ldots, d_{2t-1}\rangle$ and measuring it.

Second, once $(d_0, d_2, \ldots, d_{2t-1})$ has been produced, d_1 can be obtained by performing $U_{g_0}^{\dagger}$ and then an orthogonal measurement in the basis $|\psi'_1\rangle, \ldots, |\psi'_N\rangle$.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/