# Derandomizing Quantum Circuits with Measurement-Based Unitary Designs

Peter S. Turner and Damian Markham

Phys. Rev. Lett. **116**, 200501 — Published 19 May 2016

DOI: 10.1103/PhysRevLett.116.200501

# Derandomizing quantum circuits with measurement based unitary designs

Peter S. Turner[1,*] and Damian Markham[2,†]

[1]School of Physics and Department of Electrical and Electronic Engineering, University of Bristol, HH Wills Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, UK
[2]CNRS LTCI, Departement Informatique et Reseaux, Telecom ParisTech, 23 avenue d'Italie, CS 51327, 75214 Paris CEDEX 13, France

(Dated: April 22, 2016)

Entangled multipartite states are resources for universal quantum computation, but they can also give rise to ensembles of unitary transformations, a topic usually studied in the context of random quantum circuits. Using several graph state techniques, we show that these resources can 'derandomize' circuit results by sampling the same kinds of ensembles quantum mechanically, analogously to a quantum random number generator. Furthermore, we find simple examples that give rise to new ensembles whose statistical moments exactly match those of the uniformly random distribution over all unitaries up to order $t$, while foregoing adaptive feed-forward entirely. Such ensembles – known as $t$-designs – often cannot be distinguished from the 'truly' random ensemble, and so they find use in many applications that require this implied notion of pseudorandomness.

***Introduction*** – Randomness is an important resource in both classical and quantum information theory, underpinning cryptography, characterisation, and simulation. Random unitary transformations are often considered in the form of random quantum circuits, with wide-ranging applications in, for example, estimating noise[1], private channels[2], modelling thermalisation[3], photonics[4], and even black hole physics[5]. Uniform randomness – sampling from the 'flat' measure on a continuous set – is however very resource intensive. A natural definition of a less costly *pseudo*random ensemble is one whose statistical moments are equal to those of the uniform ensemble up to some finite order $t$ – this is the defining property of a $t$-design. Analogous to combinatorial designs that arise in many areas[6], in the quantum community the concept was first applied to states[7], and later to processes[8], the latter being the topic of much recent work (*e.g.* [9]) and are our concern here.

Efficient random circuit constructions for generating approximate $t$-designs have been shown[10]. There, classical randomness is used to assign sequences of gates from a universal gate set, yielding the desired ensemble characteristics (see below). Such a scheme obviously requires a source of classical randomness, something that can be costly, especially if it needs to be trusted. It has been pointed out in the study of typical entanglement[11] that a measurement based (MB) model[12], where unitary transformations are instead realized by sequences of measurements on highly entangled resource states, can avoid this requirement. Furthermore, in practice random circuits would necessitate reconfiguring physical quantum gates, something that is expected to introduce noise. Here we avoid both of these potential problems by showing that fixed resource states with deterministic measurement patterns can yield ensembles of unitary transformations that satisfy the $t$-design condition both approximately and exactly.

Connections between graph states in the MB model and specific random ensembles have been studied in several other contexts[13], as well as in optimizing random circuit constructions[14]. We find that the MB approach produces general pseudorandomness – $t$-designs – in a natural way; we report new exact MB 3-designs using only five and six qubits, within reach of current experiments, and give evidence of their novel mathematical structure. Our approach applies to any MB realization, from condensed matter to photonics, and benefits from the application of graph state techniques such as gFlow[15], blindness[16, 17], verification [18, 19] and error correction [20, 21], providing new possibilities for creating useful unitary ensembles. The role of $t$-designs in quantum estimation[22], in particular randomized benchmarking[1], along with cluster states being an important model for universal quantum computation in realistic hardware, leads one to anticipate MB designs being implemented in the near future. Our results also show that the MB model lends itself to the straightforward integration of pseudorandomness generation as a 'subroutine' into more involved protocols and applications, without the need for feed-forward.

***Approximate MB unitary designs*** – Our strategy is to adapt the random circuit construction of Brandao, Harrow and Horodecki[10] (BHH), which implements approximate $t$-designs, as a MB scheme. A brief review of BHH is as follows. For any matrix $\rho$ on the $t$-fold tensor product of $\mathbb{C}^d$, define its expectation with respect to the uniform Haar measure $\mathrm{d}U$ as $\mathbb{E}^t_{\mathrm{H}}(\rho) := \int \mathrm{d}U\, U^{\otimes t}\rho(U^{\otimes t})^\dagger$, where the integral is performed over the entire unitary group $\mathrm{U}(d)$. An ensemble of unitaries $\{p_i, U_i\}$ is an approximate $t$-design if, for all $\rho$, the expectation is 'close' to that of the uniform Haar ensemble:

$$(1-\epsilon)\mathbb{E}^t_{\mathrm{H}}(\rho) \leq \sum_i p_i\, U_i^{\otimes t}\rho(U_i^{\otimes t})^\dagger \leq (1+\epsilon)\mathbb{E}^t_{\mathrm{H}}(\rho), \quad (1)$$

where for matrices $A \leq B$ if $B-A$ is positive semidefinite, and $\epsilon = 0$ for exact designs.

Consider a universal set of two-qubit gates $\mathcal{U} \subset \mathrm{U}(4)$; for technical reasons $\mathcal{U} \ni U$ must contain its inverses $U^\dagger$ and the matrix elements of each $U$ must be algebraic. One constructs a "parallel" random circuit on $n$ qubits in steps, at each step performing with probability 1/2 either the 'even' unitary $U_{12} \otimes U_{34} \otimes ... \otimes U_{n-1\,n}$, or the 'odd' $U_{23} \otimes U_{45} \otimes ... \otimes U_{n-2\,n-1}$, where each $U_{ij}$ is uniformly randomly sampled from $\mathcal{U}$. BHH show that for sufficiently many (polynomial in $t$, $n$ and $1/\epsilon$) steps, the ensemble of such circuits is an $\epsilon$-approximate $t$-design.

Starting in an 'even' configuration, applying instead an 'odd' can be accomplished by a shift operation, defined over the $n$ inputs and two ancilla qubits $n+1$ and $n+2$,

$$U_S := S_{n\,n+2} S_{n-1\,n+1} \prod_{i=1}^{n-2} S_{i\,i+1}, \tag{2}$$

where $S_{ij} \in \mathrm{U}(4)$ is the swap operation between qubits $i$ and $j$. Iterating the circuit described in Fig. 1 therefore implements a random parallel circuit.

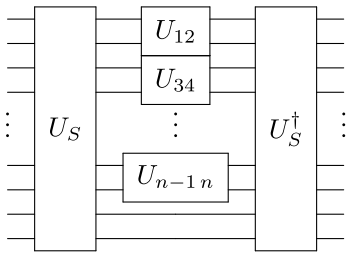


FIG. 1: One step in the random circuit construction of an approximate $t$-design over $n$ qubits. The shift gate $U_S$ and its inverse are together either randomly applied or not applied, with the the two-qubit unitaries in between randomly sampled from the universal set $\mathcal{U}$. Polynomially many iterations of this random circuit will implement an approximate $t$-design[10].

We now show how to implement this random parallel circuit with a MB scheme. The resource state in Fig. 2 (written as a graph, see caption) implements the random qubit unitary

$$U_m(\phi) := H Z^m Z(\phi), \tag{3}$$

where $m \in \{0, 1\}$ is the random measurement outcome, $H$ is the Hadamard matrix, and $Z(\phi) := e^{-iZ\phi/2}$ (similar notation is used for Pauli $X$ and $Y$). This can be understood as a MB quantum computation without the feed-forward corrections – indeed, this is our method for generating ensembles of unitaries[23]. Graphs can be connected (outputs of one identified with the inputs of the next) to perform products of unitaries. By connecting several copies of the graph in Fig. 2 and choosing measurement angles, Figs. 3 and 4 implement certain random one- and two-qubit unitaries, respectively.

These 'gadgets' can be combined to sample from a

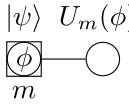


FIG. 2: The fundamental random unitary transformation induced by measurement on a graph state. Nodes are qubits initially prepared in the +1 eigenstate $|+\rangle$ of the Pauli $X$ operator, and edges indicate entanglement via the controlled-$Z$ ($CZ$) operation. Angles $\phi$ indicate projective measurement direction in the Pauli $XY$-plane, with the random outcome bit $m$; output nodes are unmeasured and therefore blank. Here we explicitly include an arbitrary input (square node) state $|\psi\rangle$ and the output; $U_m(\phi)$ is given by Eq. (3).

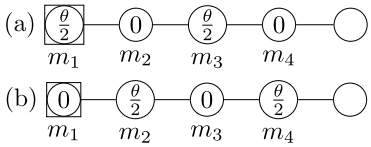


FIG. 3: By measuring the qubits as indicated, (a) implements randomly $Z^{m_1 \oplus m_3} X^{m_2 \oplus m_4} Z(\theta)^{m_2 \oplus 1}$ while (b) implements randomly $Z^{m_3} X^{m_2 \oplus m_4} X(\theta)^{m_3 \oplus 1} Z^{m_1}$, where $\oplus$ denotes bitwise sum (ignoring unimportant global phases).

larger universal set of unitaries; Fig. 5 implements

$$\begin{aligned} U_{ij}^{\mathbf{M}} = {} & (Z_i Z_j)^{M_1} (Z(\pi/2)_i Z(\pi/2)_j CZ_{ij})^{M_2} \\ & X_i^{M_3} X_j^{M_4} Z_i^{M_5} Z_j^{M_6} Z(\pi/4)_i^{M_7} Z(\pi/4)_j^{M_8} \\ & X_i^{M_9} X_j^{M_{10}} Z_i^{M_{11}} Z_j^{M_{12}} X(\pi/4)_i^{M_{13}} X(\pi/4)_j^{M_{14}} Z_i^{M_{15}} Z_j^{M_{16}}, \end{aligned} \tag{4}$$

where, here and in the following, $\mathbf{M}$ is a new bit string whose independently random entries are functions of the measurement results $m_k$. This set is universal because it contains the universal set $\{X(\pi/4), Z(\pi/4), CZ\}$; note also that their matrix elements are algebraic. Furthermore, since $ZX(\pi/4) = X(-\pi/4)Z$, for every $\mathbf{M}$ there exists an $\mathbf{M}'$ such that $U^{\mathbf{M}'} = (U^{\mathbf{M}})^{-1}$, thus satisfying the conditions of the BHH construction.

By decomposing swaps into graph gadgets we can find a MB version of the shift operator of Eq.(2). The key observation is that in order to implement a random unitary composed of several gadget unitaries, certain random outcomes must be correlated. Projecting a set of vertices onto the same outcome can be accomplished by a new graph where that set is replaced with a single vertex in a particular way. In the case of common $Z$ measurements on two qubits this is exactly the "fusion" operation of optical MBQC[24]. Here we require $X$ ($\phi = 0$) measurements to be correlated as these give rise to the crucial dependencies, and we call this graph transformation an $X$-fusion operation; see the supplemental material[25] for details and examples.

The random unitary resulting from Fig. 4 has unwanted $Z(\pi/2)$ rotations correlated to the $CZ$. We can now use $X$-fusion to undo this: simply append $Z(\pi/2)$ gadgets (Fig. 3(a)) and impose correlations using appro-

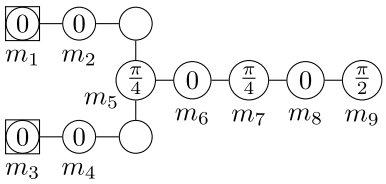


FIG. 4: Graph and measurement pattern implementing the two-qubit gate $U_{ij} = (Z_iZ_j)^M(Z(\pi/2)_iZ(\pi/2)_jCZ_{ij})^{m_6\oplus 1}\times X_i^{m_4}X_j^{m_2}Z_i^{m_3}Z_j^{m_1}$, where $M$ is a random bit which is a function of measurement results $m_{5,7,8,9}$.

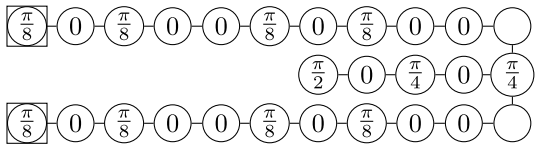


FIG. 5: Measurement gadgets combined in this way sample from a universal set of two-qubit unitaries, given in Eq.(4).

priate X-fusions, resulting in a new (messier) graph.

To find the graph for $U_S$ we first decompose its circuit description into $Z(\pi/2)$, $X(\pi/2)$ and $CZ$. Where $Z(\pi/2)$ and $X(\pi/2)$ appear we use the gadgets of Fig. 3(a) and (b) respectively, and where $CZ$ appears we use (the $X$-fused version of) Fig. 4. The same procedure can be used for $U_S^\dagger$. Between each pair of appropriate outputs of $U_S$ and inputs of $U_S^\dagger$ we insert the two-qubit gadget of Fig. 5. Looking at the corresponding unitaries (see figure captions), we see that, because the non-Pauli gates are Clifford, all the random Paulis can be moved to the left; this allows them to be absorbed into the randomly sampled two-qubit unitaries of Eq.(4), which remain universal. It remains to force all of the appropriate random $U_S$ and $U_S^\dagger$ outcomes to be the same; to do so we apply $X$-fusions on the corresponding qubits. In this way we end up with a large graph, with fixed measurement angles prescribed by the gadgets, that implements the random parallel circuit of Fig. 1.

We can show[25] that the size of this graph state and its preparation time are linear in the number of input qubits $n$. Since only polynomially many iterations of the BHH circuit are required, our construction is also efficient with the same scaling, namely $\lceil log_2(4t)\rceil^2 t^5 t^{3.1}(nt + log(1/\epsilon))$. Thus we have that fixed resource states with fixed measurement settings can give rise to pseudorandom ensembles in the form of approximate $t$-designs for all $t$, $n$ and $\epsilon$. The scheme is efficient but requires a large overhead, which we expect can be greatly improved; this is supported by the following direct construction.

***Exact linear cluster designs*** – We will now show that the MB approach can also produce exact designs with surprisingly few resources. From Eq. (3) it follows that a linear cluster of $L$ qubits yields a unitary

$$U_{\mathbf{m}}(\boldsymbol{\phi}) := U_{m_L}(\phi_L)\cdots U_{m_2}(\phi_2)U_{m_1}(\phi_1), \qquad (5)$$

where $\boldsymbol{\phi} \in [0,\pi]^L$ and $\mathbf{m} \in \{0,1\}^L$ are ordered lists of angles and outcomes, respectively. Here node 1 is the input, and node $L+1$ is the output. We are interested in the ensemble of unitaries $\{p_{\mathbf{m}}, U_{\mathbf{m}}(\boldsymbol{\phi})\}$ for all outcome strings $\mathbf{m}$. The linearity of the cluster ensures that $p_{\mathbf{m}} = 1/2^L$ will be the same for all $\mathbf{m}$, and since an ensemble has $2^L$ elements the distribution is uniform.

A test for $t$-designess can be made using the *frame potential*[7, 27], which is a sum of powers of the ensemble elements' Hilbert-Schmidt overlaps. In our case of a uniform ensemble on qubits it is given by

$$F_L^t(\boldsymbol{\phi}) := \frac{1}{4^L}\sum_{\mathbf{m},\mathbf{m}'}\left|\mathrm{Tr}\left[U_{\mathbf{m}}(\boldsymbol{\phi})^\dagger U_{\mathbf{m}'}(\boldsymbol{\phi})\right]\right|^{2t} \geq \frac{(2t)!}{t!(t+1)!}, \qquad (6)$$

and the bound is known to be achieved if and only if the ensemble is a $t$-design. Equations (3,5) along with the cyclicity of the trace imply that the first and last measurement angles, $\phi_1$ and $\phi_L$, do not affect the frame potential – note this does not mean the nodes themselves are redundant, since their measurement outcomes help to grow the ensemble. The frame potential is also symmetric under the transposition $\phi_{l+1} \leftrightarrow \phi_{L-l}$.

A $t$-design is by definition a $(t-1)$-design, and it is not hard to see that a 1-design must span the operator space, thus any design for the unitary group $\mathrm{U}(d)$ must contain at least $d^2$ elements. Since here $d = 2$ and the $L = 1$ ensemble has but 2 elements, it cannot be a design. For $L = 2$ the frame potential is $F_2^1(\boldsymbol{\phi}) = 1$, which coincides with the minimum in Eq. (6) for all $\boldsymbol{\phi}$ and is therefore always a 1-design, (choosing $\boldsymbol{\phi} = \{0,0\}$ gives the Pauli ensemble up to phase). Any basis is a 1-design, and so we will subsequently concern ourselves with $t \geq 2$.

For $L = 3$ the frame potential is $F_3^2(\boldsymbol{\phi}) = 2(1 + \cos^4\phi_2 + \sin^4\phi_2)$ , which has a global minimum of 3 at $\phi_2 = \pi/4$; this exceeds the 2-design minimum of 2 from Eq. (6). This is not surprising, since there are 8 elements in the ensemble and a lower bound of 10 has been proved[28]. For $L = 4$, one finds the product $F_4^2(\boldsymbol{\phi}) = F_3^2(\phi_2)F_3^2(\phi_3)/4$; each factor can be independently minimised at angle $\pi/4$, yielding $9/4 > 2$. Thus even though there are more than the minimal number of elements, we have proved that for $L = 4$ no choice of angles can give a 2-design, and hence any $(t \geq 2)$-design.

For $L = 5$ the frame potential can be written

$$F_5^2(\boldsymbol{\phi}) = 4X_2X_4\left(x_3^2 + \left(3(1-X_2^{-1})(1-X_4^{-1}) - 1\right)x_3 + 1\right), \qquad (7)$$

where $X_2 := 1 - \cos^2\phi_2 + \cos^4\phi_2$, similarly for $X_4$, and $x_3 = \cos^2\phi_3$. This has a unique minimum of 2 at $X_2 = X_4 = 3/4$ and $x_3 = 1/3$. Since this achieves the bound we do indeed have a 2-design, or more precisely a set of (intimately related) 2-designs as there are several choices of equivalent angles, the simplest being $\phi_2 = \phi_4 = \pi/4$ and $\phi_3 = \arccos\sqrt{1/3}$.

One finds that this ensemble is also a 3-design; $F_5^3(\phi_1, \pi/4, \arccos\sqrt{1/3}, \pi/4, \phi_5) = 5$, again achieving the bound in Eq. (6). However, the $t = 4$ value is $14\frac{14}{27} > 14$, and so it does not define a 4-design (see Fig. 6). We pause here to note that previous design constructions are predominantly related to group actions[27, 28], and in particular it is well known that 3-designs are generated by the Clifford group[8, 29]. One is led to ask whether or not the 32 unitary matrices (see [25] ) in this $L = 5$ qubit 3-design also admit a finite group structure. Due to the irrationality of $\phi_3$ however, any group containing the ensemble must have infinite order. Additionally, the number of ensemble elements for any such MB design must be a power of 2, which is not the case for Clifford designs. Thus it would seem that along with being practically motivated, MB designs are mathematically novel.

The following two facts are not hard to prove: if $\{p_i, U_i\}$ is a $t$-design, then so is $\{p_i, VU_iW\}$ for any $V, W \in \mathrm{U}(d)$; and the ensemble formed by the (uniform) union of a $t$-design and a $t'$-design is a $\min(t, t')$-design. Together they imply that once a MB $t$-design has been achieved, any choice of subsequent measurement pattern will output at least a $t$-design. Thus any measurement pattern including the subsequence $\{1/2, 1/3, 1/2\}$ will remain a 3-design, where we have switched to a more natural parameterization $\phi \to x = \cos^2\phi$. For $L = 6$ calculations can still be carried out analytically, and interestingly a continuous family of 3-designs arises for angles given in the new parameterization by

$$\mathbf{x} = \left\{x_1, \frac{1}{2}, x_3, \frac{3x_3 - 2}{3x_3 - 3}, \frac{1}{2}, x_6\right\}, \quad x_3 \in \left[0, \frac{2}{3}\right]. \qquad (8)$$

We can carry on the search for higher order designs in longer linear clusters, however the computational demands grow quickly and exact results are elusive. Figure 6 shows the difference $\Delta F$ of the first seven frame potentials from the bound for linear clusters up to $L = 10$. Since the frame potential is the square of a 2-norm[27], one finds[30] that $\sqrt{\Delta F}$ is an upper bound on the diamond norm definition of approximate $t$-designs used in Eq. (1). Thus a lower frame potential indicates a better approximate $t$-design, and there are several strategies for trying to minimize it. Figure 6 shows three such, discussed in the caption.

These results beg the question of the existence of exact MB designs for arbitrary graph states with multi-qubit inputs and outputs, in particular square lattice cluster states of $N$ qubits in $L$ layers. Unfortunately the limited amount of nonlocality introduced between linear clusters in this way makes it impossible to find small examples of exact multi-qubit designs. A numerical exploration of the problem shows that the same general behaviour, (exponential convergence to the Haar value, as in Fig. 6), is exhibited by square clusters, but the complexity of the computation prohibits an extensive search. Clearly the way forward is to identify a (likely group) structure in the ensembles that can be exploited in the multi-qubit case; the exact results above are a major step in this direction, but further investigation is required.

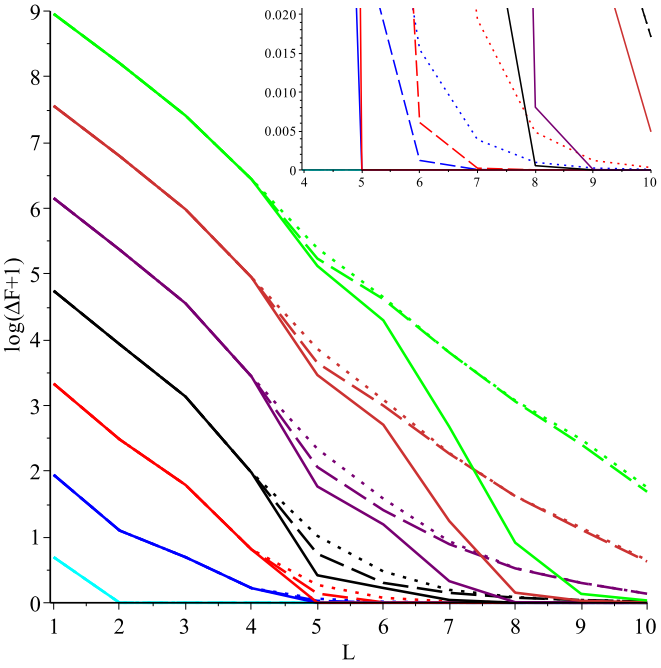


FIG. 6: From bottom to top the $t = 1, 2, \cdots, 7$ frame potentials, given by the difference $\Delta F$ from the exact bound (logarithmic scale) versus linear cluster length $L$ (interpolated). For each we consider three measurement patterns: dotted lines for those consisting entirely of the angle $\pi/4$; dashed lines for those consisting of a single measurement angle $\phi_{\min}$ that minimizes the frame potential; and solid lines for a full multi-angle minimization (performed in Matlab). One sees that the former approach the bound exponentially, albeit with a decreasing rate, as predicted by random quantum circuit results[31]. The latter can be seen to drop much more quickly beyond $L = 4$. Other than the trivial $t = 1$ case, only the $t = 2, 3$ curves reach $\Delta F = 0$ (inset), *e.g.* the exact design for $L = 5$. Despite the $t = 4, 5$ curves coming very close to zero, an analytic solution at $L = 9$ has not been found[32].

***Conclusion*** – We have shown that quantum resource states can produce arguably the most pseudorandomness possible in the form of approximate and exact $t$-designs, despite consuming no classical randomness and requiring neither reconfiguration nor feed-forward. The question raised is: what resources provide the most randomness most efficiently? In this direction it is intriguing to note that the MB approach can give rise to probability distributions that are impossible to efficiently sample classically[33], leading one to imagine resources that outperform classical randomization in principle as well as in practice. Several generalizations come to mind, including arbitrary graphs, qu*d*it nodes, non-standard resource preparations (*e.g.* >2-body entangling gates), and weighted designs. We hope this work motivates further research into these and other possibilities.

The authors would like to thank D. Gross, D. Mahler, T. Rudolph, A. Doherty, A. B. Sainz, A. Scott, A. Roy and S. Bartlett for helpful discussions. PST acknowledges support from EPSRC First Grant EP/N014812/1, US ARO Grant No. W911NF-14-1-0133, and a School of Physics travel grant. DM acknowledges support from ANR grant COMB and ville de Paris grant CiQWii.

* Electronic address: peter.turner@bristol.ac.uk
† Electronic address: markham@enst.fr

[1] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd and D. G. Cory. Science, 302(5653):2098, (2003); J. M. Epstein, A. W. Cross, E. Magesan, and J. M. Gambetta, Phys. Rev. A 89, 062321 (2014).
[2] P. Hayden, D. Leung, P. W. Shor and A. Winter, Comm. Math. Phys. 250, 371, (2004).
[3] M. P. Muller, E. Adlam, L. Masanes and N. Wiebe, Comm. Math. Phys. 340, 499 (2015).
[4] J. C. F. Matthews, R. Whittaker, J. L. O'Brien and P. S. Turner, Phys. Rev. A 91, 020301(R) (2015).
[5] P. Hayden and J. Preskill, J. High E. Phys. 2007(09), 120 (2007).
[6] D. R. Stinson, Combinatorial designs: constructions and analysis, Springer, New York, 2004.
[7] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, J. Math. Phys. 45, 2171 (2004).
[8] C. Dankert, R. Cleve, J. Emerson and E. Livine, Phys. Rev. A 80, 012304 (2012).
[9] R. Cleve, D. Leung, L. Liu and C. Wang, arXiv:1501.04592.
[10] F. G. S. L. Brandao, A. W. Harrow and M. Horodecki, arXiv:1208.0692.
[11] A. D. Plato, O. C. Dahlsten and M. B. Plenio, Phys. Rev. A 78, 042332 (2008).
[12] R. Raussendorff and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001).
[13] B. Collins, I. Nechita and K. Zyczkowski, J. Phys. A: Math. Theor. 43, 275303 (2010); P. Kondratiuk and K. Zyczkowski, Acta Physica Polonica A 124, 1098 (2013).
[14] W. G. Brown, Y. S. Weinstein and L. Viola, Phys. Rev. A 77, 040303(R) (2008).
[15] D. E. Browne, E. Kashefi, M. Mhalla and S. Perdrix, New J. Phys. 9, 250 (2007).
[16] A. Broadbent, J. F. Fitzsimons and E. Kashefi. Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on. IEEE, 2009.
[17] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science, 335(6066), 303-308 (2012).
[18] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[19] S. Barz, J. F. Fitzsimons, E. Kashefi and P. Walther, Nature Physics, 9(11), 727-731 (2013).
[20] D. Schlingemann and R. F. Werner. Physical Review A 65, 012308 (2001).
[21] B. A. Bell, D. A. Herrera-Martí, M. S. Tame, D. Markham, W. J. Wadsworth and J. G. Rarity., Nature Communications 5, 3658 (2014).
[22] A. J. Scott, J. Phys. A: Math. Theor. 41, 055308 (2008).
[23] M. Mhalla, M. Murao, S. Perdrix, M. Someya and P. S. Turner, Theory of Quantum Computation, Communication, and Cryptography, Springer Berlin, 2014, pp. 174-187; arXiv:1006.2616.
[24] D. Browne and T. Rudolph, Phys. Rev. Lett. 95, 010501 (2005).
[25] See Supplemental Material [URL will be inserted by publisher], which includes Refs. [34], [35].
[26] M. Hein, J. Eisert and H. J. Briegel, Phys. Rev. A 69, 062311 (2004).
[27] D. Gross, C. Audenaert and J. Eisert, J. Math. Phys. 48, 052104 (2007).
[28] A. Roy and A. J. Scott, Des. Codes Cryptogr. 53, 13-31 (2009).
[29] P. S. Turner, Proceedings, Nankai Series in Pure, App. Math. and Theo. Phys. 11, World Scientific, 2013; R. Kueng and D. Gross, arXiv:1510.02767; Z. Webb, arXiv:1510.02769; H. Zhu, arXiv:1510.02619.
[30] R. A. Low, PhD thesis, University of Bristol, (2010) arXiv:1006.5227.
[31] J. Emerson, E. Livine and S. Lloyd, Phys. Rev. A 72, 060302(R) (2005)
[32] Conversely, proving the *non*existence of exact designs should be possible using sum-of-squares techniques for bounding the global minima of polynomials, because these have semi-definite programming certificates; however, the problem seems to be numerically unstable and we were unable to coax convincing bounds on the frame potential from SOStools (www.cds.caltech.edu/sostools/).
[33] M. Hoban, J. Wallman, H. Anwar, N. Usher, R. Raussendorf and D. Browne, Phys. Rev. Lett. 112, 140505 (2014).
[34] D. Gottesman, Phys. Rev. A 54, 1862 (1997).
[35] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A 69, 022316 (2004); Phys. Rev. A 70, 034302 (2004).