Near-linear construction of exact unitary 2-designs
(Extended abstract)

Richard Cleve[1,2,4] Debbie Leung[1,3,4] Li Liu[1,2] Chunhao Wang[1,2]

We present a unitary 2-design on n qubits that can be exactly implemented with $O(n \log n \log \log n)$ elementary gates from the Clifford group (assuming the Extended Riemann Hypothesis is true). This is essentially a quadratic improvement over all previous (exact and approximate) constructions, which all use $\tilde{\Omega}(n^2)$ gates. (There is one exception, where $O(n \log 1/\varepsilon)$ gates suffice for a notion of approximation within ϵ in a limited context.) Furthermore, our constructions require only $O(n)$ randomness and can be implemented in logarithmic depth.

1 Introduction

The Haar measure on the unitary group is the unique measure that is invariant under multiplication by any group element. Haar-random unitaries, by their symmetries, facilitate many analyses in quantum information [11, 12, 10, 13, 9]. However, Haar-random unitaries have very high computational complexity in that most of them cannot be efficiently implemented or reasonably well approximated by circuits of size polynomial in the number of qubits. They are also expensive to sample in terms of the amount of randomness required. Unitary 2-designs are probability distributions on finite subsets of the unitary group that have some specific properties in common with the Haar measure—and they can have the advantage of being computable by polynomial-size circuits and having low sampling complexity. Unitary 2-designs (and approximations of them) have been applied as efficient ways of achieving *bilateral twirling* [6], *channel twirling* [5], and *decoupling* [16].

There are different ways of defining a unitary 2-design (e.g., in [5, 6, 8]) that are equivalent. One equivalent definition that is operational and conceptually simple is the following. A unitary 2-design is a distribution that is *two-query indistinguishable* from the Haar distribution. That is, no circuit that makes two queries, each to U or to $U^\dagger$ (as illustrated in Fig. 1), can distinguish between these two cases: (a) U is sampled according to the Haar measure; (b) U sampled with respect to the unitary 2-design.

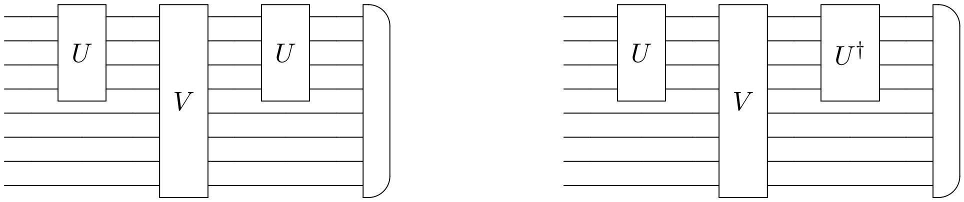

Figure 1: Illustration of the *two-query indistinguishable* property: querying U twice (left); or querying U and $U^\dagger$ (right). The initial state is arbitrary, V is an arbitrary unitary, and the measurement is arbitrary.

[1] Institute for quantum Computing, University of Waterloo
[2] School of Computer Science, University of Waterloo
[3] Department of Combinatorics and Optimization, University of Waterloo
[4] CIFAR

Note that this definition of a unitary 2-design is a clear quantum analogue of a 2-universal hash function [3].

The notion of an *approximate* unitary 2-design has been defined in various ways [5, 6, 8]. One possible definition is to relax the above indistinguishability scenario, where the distinguishing probability is allowed to exceed $\frac{1}{2}$, but must be bounded by $\frac{1}{2} + \epsilon$. However, the analogous natural relaxations of the other definitions of unitary 2-designs are not known to be equivalent (and there is evidence that some are strictly weaker).

2 Previous work

The uniform distribution on the Clifford group is a unitary 2-design (in the exact sense) [5, 6]. This implies that the circuit complexity is $O(n^2/\log n)$ where the gates are one- and two-qubit gates from the Clifford group [1]. Moreover, the sampling cost is $O(n^2)$ random bits of entropy.

A construction in [8] based on a random circuit generation yields ϵ_b-approximate unitary 2-designs of size $O(n(n+\log 1/\epsilon_b))$, where the notion of approximation is related to a bilateral twirling operation. Another construction [5] yields circuits of size $O(n \log 1/\epsilon_c)$ for a notion of approximation related to channel twirling; however, there is evidence (see, e.g., section 1.1 of [2]), that the calibration of the approximation used incurs a blow-up by a factor of 2^n in the bilateral twirl context. In other words, for the more general setting, we need $\epsilon_c \leq \epsilon_b/2^n$—so the circuit size becomes $O(n(n + \log 1/\epsilon_b))$.

All of these constructions incur circuits of size $\tilde{\Omega}(n^2)$ and require $\Omega(n^2)$ random bits of entropy for exact unitary 2-designs as well as their approximations related to bilateral twirling.

Reference [4] proves that there exists a small subgroup of the Clifford group that gives rise to an exact unitary 2-design that uses $5n$ random bits of entropy. Reference [7] and [14] study the necessary and sufficient entropy for exact and approximate unitary 2-designs. Approximately $4n$ random bits of entropy are necessary. The circuit complexities for these constructions are unknown.

2 New result

We give a construction of *exact* unitary 2-designs of circuit size equal to the asymptotic cost of multiplication by arbitrary constants in the finite field $\mathrm{GF}(2^n)$, where $\mathrm{GF}(2^n)$ is represented by a self-dual basis.

We also observe (from existing results [17, 15]) that, under the Extended Riemann Hypothesis (ERH), for infinitely many n, the circuit size for multiplication in $\mathrm{GF}(2^n)$ with respect to a self-dual basis is $O(n \log n \log\log n)$. Therefore, for infinitely many n, under the ERH, we have a unitary 2-design with circuit-size $O(n \log n \log\log n) \subset \tilde{O}(n)$. The elementary gates used by these circuits are one- and two-qubit gates in the Clifford group.

Since our constructions yield exact unitary 2-designs, they are also valid for all notions of approximate unitary 2-designs.

3 New techniques

To explain our techniques, we first describe a primitive called "Pauli mixing," which, when composed with a random Pauli operation, provides one way to construct a unitary 2-design. A probability distribution of unitaries performs *Pauli mixing* if, for *any* non-trivial Pauli matrix P, the process of choosing a unitary U randomly from the distribution and then conjugating P by U results in a uniform distribution on all the $4^n - 1$ non-trivial Pauli operations. Let I, X, Y, Z denote the single-qubit Pauli matrices. Fig. 2 illustates the 15 *non-trivial* 2-qubit Pauli matrices arranged with rows and columns correspinding to their X-structure and Z-structure (respectively).

	IX	XI	XX
IZ	IY	XZ	XY
ZI	ZX	YI	YX
ZZ	ZY	YZ	YY

Figure 2: A natural arrangement of all the non-trivial 2-qubit Paulis into rows and columns. Pauli mixing requires a uniform distribution on the 15 items.

One of our contributions is to show that there exists a decomposition of the unitaries from the subgroup of the Clifford group used in [4] into a constant number of primitive operations. The dominant cost is that of one of these primitive operations: a "multiply-by-r" gate M_r that acts as $M_r|c\rangle = |rc\rangle$, where rc denotes the product when $\{0,1\}^n$ are interpreted as the elements of the finite field $\mathrm{GF}(2^n)$ with respect to a self-dual basis. (We do not know how to make our construction work efficiently with the basis that results from standard constructions of $\mathrm{GF}(2^n)$ in terms of irreducible polynomials.)

We also observe that, based on results in the existing literature, multiplication in $\mathrm{GF}(2^n)$ with respect to a self-dual basis can be performed with $O(n \log n \log\log n)$ gates for infinitely many n using assuming ERH. (It should be noted that the cost of multiplication in $\mathrm{GF}(2^n)$ can be basis-dependent.) In our context, the circuits need to perform multiplication by any non-zero constant from $\mathrm{GF}(2^n)$. Each of our constant-multiplication circuits reduces to CNOT gates—hence is in the Clifford group. These circuits use ancilliary qubits that are each initially in state $|0\rangle$ and returned to this state at the end of the computation of the multiplication.

References

[1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004.

[2] W. Brown and O. Fawzi. Decoupling with random quantum circuits. 2013. arXiv:1307.0632.

[3] J. L. Carter and M. N. Wegman. Universal classes of hash functions (extended abstract). In *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing*, STOC '77, pages 106–112, New York, NY, USA, 1977. ACM.

[4] H. F. Chau. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Trans. Inf. Theory*, 51(4):1451–1468, 2005. arXiv:quant-ph/0405016.

[5] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, Jul 2009.

[6] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48(3):580–598, 2002. arXiv:quant-ph/0103098.

[7] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: on the structure of unitary designs. *Journal of mathematical physics*, 48:052104, 2007.

[8] A. Harrow and R. Low. Random quantum circuits are approximate 2-designs. *Comm. Math. Phys.*, 291(1):257–302, 2009. arXiv:0802.1919.

[9] M. Hastings. Randomizing quantum states: Constructions and applications. *Nature Physics*, 5:255, 2009. arXiv:0809.3972.

[10] P. Hayden, M. Horodecki, J. Yard, and A. Winter. A decoupling approach to the quantum capacity. *Open Systems and Information Dynamics*, 15:7–19, 2008.

[11] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004. quant-ph/0307104.

[12] P. Hayden, D. W. Leung, and A. Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265(1):95–117, 2006. quant-ph/0407049.

[13] P. Hayden and A. Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all p¿ 1. *Communications in Mathematical Physics*, 284(1):263–280, 2008.

[14] A. Roy and A. J. Scott. Unitary designs and codes. *Designs, codes and cryptography*, 53(1):13–31, 2009.

[15] A. Schönhage. Schnelle multiplikation von polynomen über körpern der charakteristik 2. *Acta Informatica*, 7(4):395–398, 1977.

[16] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary approximate two-designs. *New Journal of Physics*, 15(5):053022, 2013.

[17] J. von zur Gathen, A. Shokrollahi, and J. Shokrollahi. Efficient multiplication using type 2 optimal normal bases. In *Arithmetic of Finite Fields*, pages 55–68. Springer, 2007.