Efficient Synthesis of Universal Repeat-Until-Success Quantum Circuits

Alex Bocharov, Martin Roetteler, and Krysta M. Svore
Quantum Architectures and Computation Group, Microsoft Research, Redmond, Washington 98052, USA
(Received 17 July 2014; published 27 February 2015)

Recently it was shown that the resources required to implement unitary operations on a quantum computer can be reduced by using probabilistic quantum circuits called repeat-until-success (RUS) circuits. However, the previously best-known algorithm to synthesize a RUS circuit for a given target unitary requires exponential classical runtime. We present a probabilistically polynomial-time algorithm to synthesize a RUS circuit to approximate any given single-qubit unitary to precision ε over the Clifford + T basis. Surprisingly, the T count of the synthesized RUS circuit surpasses the theoretical lower bound of $3\log_2(1/\varepsilon)$ that holds for purely unitary single-qubit circuit decomposition. By taking advantage of measurement and an ancilla qubit, RUS circuits achieve an expected T count of $1.15\log_2(1/\varepsilon)$ for single-qubit z rotations. Our method leverages the fact that the set of unitaries implementable by RUS protocols has a higher density in the space of all unitaries compared to the density of purely unitary implementations.

DOI: 10.1103/PhysRevLett.114.080502 PACS numbers: 03.67.Ac, 03.67.Mn

Introduction.—With rapid maturation of quantum devices, efficient compilation of high-level quantum algorithms into lower-level physical circuits becomes an important step toward a scalable quantum computer architecture. Scalability necessitates the use of fault-tolerant components in order to reliably perform computations of arbitrary length. A universal gate set that arises, e.g., from the concatenated Steane code or the surface code family, is Clifford + T basis, consisting of the two-qubit controlled-NOT gate (CNOT) and the single-qubit Hadamard H and $T = R_z(\pi/4)$ gates. Efficient algorithms to ε-approximate a single-qubit gate with an $\{H, T\}$ circuit exist [1,2]. Any z rotation requires a number of T gates close to the information-theoretic lower bound of $3\log_2(1/\varepsilon)$ ([3], Sec. 9). For general rotations, Euler angle decompositions [4] $e^{i\delta}R_z(\alpha)HR_z(\beta)HR_z(\gamma)$ for $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ can be used to obtain the best-known upper bound of $9\log_2(1/\varepsilon)$.

Recently, Paetznick and Svore [5] showed that by using probabilistic circuits—specifically, a class of circuits called repeat-until-success (RUS) circuits—the number of T gates can be reduced by a factor of at least 2.5. Their synthesis algorithm is an optimized exhaustive search with exponential classical runtime, limiting its practicality for a wide range of precisions ε. In this Letter, we develop an efficient algorithm to synthesize RUS circuits for approximating a given single-qubit unitary that runs in probabilistically polynomial classical runtime for any precision ε. We show that for z rotations the expected number of T gates required upon success scales roughly as $1.15\log_2(1/\varepsilon)$, improving over the $3\log_2(1/\varepsilon)$ lower bound on ancilla-free, unitary methods [1,2]. For general rotations, our method leads to RUS protocols with an expected T count of $3.45\log_2(1/\varepsilon)$, improving over the upper bound of $9\log_2(1/\varepsilon)$ for unitary circuits. A salient feature of our approach is the solution of the approximation step via integer relation problems and the classical PSLQ algorithm (Partial Sums of sQuares with Lower trapezoidal orthogonal decomposition, see [6]).

Intuitively, RUS protocols have a higher density and thus better approximation properties, specifically for z rotations, as illustrated in Fig. 1, with further explanation given below. Much of our technical contribution renders this intuition rigorous by translating the increase in density due to measurement into shorter circuit sizes.

The use of measurement to improve the computational power of unitary circuits is not entirely new. Research on measurement-based computation [7–9] suggests that quantum measurement allows circuits additional computational power at a lower cost in circuit resources. The use of measurement in the context of decomposition appears in methods of [10–13].

RUS circuits.—The general layout of the RUS protocol [5] is shown in Fig. 2. Here U is a unitary operation acting on $n + m$ qubits, of which n are target qubits and m are ancillary qubits. The protocol uses measurement of the ancilla qubits in such a way that one measurement outcome is labeled "success" and all other measurement outcomes are labeled "failure." Let the probability of the success outcome be p and the unitary applied to the target qubits upon measurement be V. Let $C(U)$ be the cost of the circuit that performs U. We assume for simplicity that any operator W_i performed on target qubits upon a failure measurement is unitary and that each W_i^{-1} can be implemented by a circuit with the same fixed cost $C(W)$.

In the RUS protocol, the circuit in the dashed box is repeated on the $(n + m)$-qubit state until the success measurement is observed. Each time a failure measurement is observed, an appropriate operator W^{-1} is applied in order to revert the state of the target qubits to their original input

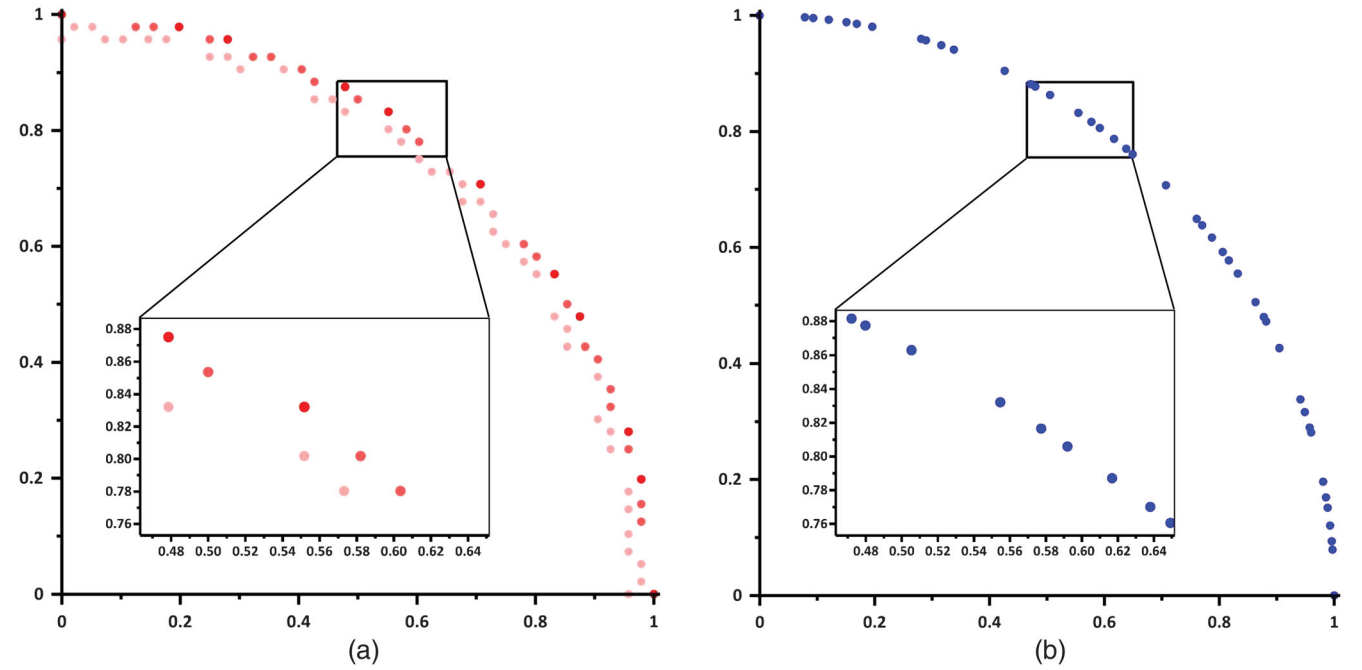

FIG. 1 (color). Approximationsof z rotations by (a) unitary circuits of T depth of at most 8 and (b) RUS protocols with a comparable expected T depth of at most 7.5.

state $|\psi\rangle$. The number of repetitions of the circuit is finite with probability 1. The statistical expectation of the overall cost to observe success is

$$E[C(V)] = [C(U) + C(W)(1-p)]/p. \qquad (1)$$

We refer to the circuit implementing the unitary U as the *RUS design* and its cost $C(U)$ as the *design cost*.

We measure the cost of a circuit in terms of T gates since fault-tolerant implementations of T gates typically require 1 to 2 orders of magnitude more resources than a fault-tolerant Clifford gate [14–16]. In the following we focus on the case where the corrections W_i are Clifford gates, i.e., $C(W_i) = 0$. This has the effect of reducing Eq. (1) to $E[C(V)] = C(U)/p$. We refer to the number of T gates in a circuit as the T *count* and the number of time steps containing T gates as the T *depth*. The optimal T count has been proven to be an invariant of the unitary operation represented by a Clifford + T circuit [17–19].

Background.—At the heart of Clifford + T synthesis is the algebraic number ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4}$, also known as the ring of cyclotomic integers of order eight. It consists of all numbers of the form $a\omega^3 + b\omega^2 + c\omega + d$, where a, b, c, d are arbitrary integers. It was shown in [20] that a unitary V on n qubits is representable exactly by a Clifford + T circuit if and only if it is of the form $V = 1/\sqrt{2}^k M$, where M is a matrix over $\mathbb{Z}[\omega]$ and k is some non-negative integer. Equivalently, we can assume that M is a matrix over $\mathbb{Z}[i, 1/\sqrt{2}]$. To satisfy the unitary condition, we require $MM^\dagger = 2^k \mathbf{1}_{2^n}$. We employ methods of [2,21] in our main algorithm below.

In Fig. 1 we illustrate a key advantage of RUS designs for approximating z rotations. We consider 1(a) unitary protocols and 1(b) RUS protocols with one ancilla qubit to implement a unitary $V = \left[\begin{smallmatrix} x & -y^* \\ y & x^* \end{smallmatrix}\right]$. In 1(a) we require that $x \in \mathbb{Z}[i, 1/\sqrt{2}]$ satisfies the norm equation $|y|^2 = 1 - |x|^2$ (red points). In 1(b) we display the upper left entry z of a two-qubit unitary U that defines a RUS design (blue points). Here z is of the form $x/\sqrt{|x|^2 + |y|^2}$, where $x = x_0/\sqrt{2^\ell}$, $y = y_0/\sqrt{2^\ell}$ with $x_0, y_0 \in \mathbb{Z}[\omega]$, $\ell = 3$ and satisfies the norm equation $|z|^2 = 2^\ell - |x_0|^2 - |y_0|^2$. The axes in 1(a) and 1(b) denote the real and imaginary part and range from 0 to 1. Only the upper left quadrant of the unit circle is shown; the remaining quadrants are given by symmetry. With respect to the metric $d(V, V') = \sqrt{1 - [|\mathrm{tr}(V^\dagger V')|/2]}$, the 144 z rotations shown in blue in 1(b) exhibit distances between nearest neighbors of at most $\varepsilon_{\max} = 0.0676$. In 1(a) only 40 circuits are within distance $\varepsilon_{\max}$ of any z rotation (dark red points). In the asymptotic limit for the T count, this ratio tends to 3, one of our main contributions. Further points are at cutoff distances $\varepsilon_{\max} = 0.1398$ (light red) and 0.2139 (very light red),

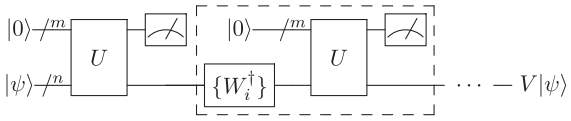

FIG. 2. RUS design to implement unitary V.

corresponding to RUS protocols with expected T depths of 6.7 and 6.2, respectively. Intuitively, the blue points are akin to rational numbers, and the red points to integers. Thus, the blue points provide a much denser covering than the red points. We analyze the density with which cyclotomic rationals are distributed in Sec. A of [27].

Overview of the algorithm.—Our algorithm ε approximates an axial rotation $R_z(\theta)$ by a RUS circuit over the Clifford + T basis in four stages, shown in Fig. 1 in Sec. B of [27]. We measure the distance between a target unitary V and its approximation V' via the invariant metric $d(V, V')$ [22].

The first stage approximates the phase factor $e^{i\theta}$ with a unimodal cyclotomic rational, i.e., an algebraic number of the form z^*/z, where $z \in \mathbb{Z}[\omega]$, by finding an approximate solution of an integer relation problem. We note that z is defined up to an arbitrary real-valued factor. The second stage performs several rounds of random modification $z \mapsto (rz)$, where $r \in \mathbb{Z}[\sqrt{2}]$, in search of an r such that (a) the *norm equation* $|y|^2 = 2^L - |rz|^2$ is solvable for $y \in \mathbb{Z}[\omega]$, $L \in \mathbb{Z}$, and (b) the one-round success probability $|rz|^2/2^L$ is sufficiently close to 1. In the third stage, the two-qubit matrix corresponding to the unitary part of the RUS circuit is assembled. During the fourth stage, a two-qubit RUS circuit that implements the desired $R_z(\theta)$ rotation on success and an easily correctable Clifford gate on failure is synthesized.

Stage 1: Cyclotomic rational approximation.—The phase $e^{i\theta}$ is representable exactly as z^*/z if and only if the expression $a[\cos(\theta/2) - \sin(\theta/2)] + b\sqrt{2}\cos(\theta/2) + c[\cos(\theta/2) + \sin(\theta/2)] + d\sqrt{2}\sin(\theta/2)$ is exactly zero (see Sec. C of [27] for proof). By making this expression arbitrarily small, then $|z^*/z - e^{i\theta}|$ will be arbitrarily small. Let θ be a real number and $z = a\omega^3 + b\omega^2 + c\omega + d, a, b, c, d \in \mathbb{Z}$ be a cyclotomic integer. Then $|z^*/z - e^{i\theta}| < \varepsilon$ if and only if $|a[\cos(\theta/2) - \sin(\theta/2)] + b\sqrt{2}\cos(\theta/2) + c[\cos(\theta/2) + \sin(\theta/2)] + d\sqrt{2}\sin(\theta/2)| < \varepsilon|z|$, which can be shown by direct complex expansion of $ie^{-i\theta/2}(z^* - e^{i\theta}z)$.

To approximate any phase $e^{i\theta}$ with a cyclotomic rational z^*/z, where $z \in \mathbb{Z}[\omega]$, we customize the PSLQ integer relation algorithm [6,23] which attempts to find an integer relation between $[\cos(\theta/2) - \sin(\theta/2)]$, $\sqrt{2}\cos(\theta/2)$, $[\cos(\theta/2) + \sin(\theta/2)]$, $\sqrt{2}\sin(\theta/2)$. It terminates iterative attempts if and only if $|z^*/z - e^{i\theta}| < \varepsilon$ [24]. Upon termination, our customization also outputs the integer relation candidate $\{a, b, c, d\}$ for which the condition has been satisfied. The desired cyclotomic integer is then given by $z = a\omega^3 + b\omega^2 + c\omega + d$. We find empirically (by simulation) that the PSLQ performance is very close to optimal with $|z| < \kappa\varepsilon^{-1/4}$, where $\kappa = 3.05 \pm 0.28$.

Stage 2: Randomized search.—Once the desired z is obtained, the next stage is to include z in a unitary

$$\frac{1}{\sqrt{2^L}}\begin{bmatrix} z & y \\ -y^* & z^* \end{bmatrix}, \tag{2}$$

where $y \in \mathbb{Z}[\omega]$ and $L \in \mathbb{Z}$. We would like $|z|^2/2^L$ to be reasonably large since this value equals the one-round success probability of the RUS circuit. Unfortunately, the majority of z values do not allow for this. To create a unitary of the form, Eq. (2), we seek a y that satisfies the normalization condition $(|y|^2 + |z|^2)/2^L = 1$, or equivalently, $|y|^2 = 2^L - |z|^2$. It is known [3,20] that $|z|^2$ belongs to the real-valued ring $\mathbb{Z}[\sqrt{2}]$ and thus so does $2^L - |z|^2$.

Given an arbitrary $\xi \in \mathbb{Z}[\sqrt{2}]$, the identity $|y|^2 = \xi$, considered as an equation for an unknown $y \in \mathbb{Z}[\omega]$, is called a norm equation in $\mathbb{Z}[\omega]$. A necessary condition for easy solvability of the norm equation is that in Eq. (2), $|z|^2 \leq 2^L$ and $|z^\bullet|^2 \leq 2^L$, where $(\cdot)^\bullet : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]$ extends the $\omega \mapsto (-\omega)$ map.

Our strategy generalizes that of [3]. We consider a fixed initial $z \in \mathbb{Z}[\omega]$ where we can replace z in z^*/z by rz, where $r \in \mathbb{Z}[\sqrt{2}]$ is arbitrary, without changing the fraction. For a randomly picked $r \in \mathbb{Z}[\sqrt{2}]$, we set $L_r = \lceil \log_2(|rz|^2) \rceil$.

We want L_r close to its lower bound $L_1 = \lceil \log_2(|z|^2) \rceil$. For some small $\delta > 0$, we constrain $L_r \leq (1 + \delta)L_1$, which implies $r^2 \leq 2^{\delta L_1}$. Moreover, we also require $(r^\bullet)^2 \leq 2^{\delta L_1}$. Thus r is sampled from $S_\delta = \{a + b\sqrt{2} | a, b \in \mathbb{Z}, |a \pm b\sqrt{2}| \leq 2^{\delta L_1/2}\}$. The cardinality, $\mathrm{card}(S_\delta)$, is approximately equal to $2^{1/2+\delta L_1}$, corresponding to the area of $\{|a \pm b\sqrt{2}| \leq 2^{\delta L_1/2}\}$ in the (a, b) plane.

While $\mathrm{card}(S_\delta)$ is $O(1/\varepsilon^\delta)$ and thus exponential in $\log_2(1/\varepsilon)$, under a certain working conjecture it suffices to use polylogarithmically many random values of r. We conjecture (and have supporting empirical evidence) that for large enough δL_1 there are $\Omega([2^{\delta L_1}/(\delta L_1)])$ values of $r \in S_\delta$ for which the norm equation $|y|^2 = 2^{L_r} - |rz|^2$ is easily solvable, and in particular for large enough k there are $\Omega[2^{\delta L_1}/(k\delta L_1)]$ values for which the equation is solvable and $p(r) > 1 - 1/k$. We discuss this conjecture in more detail in Sec. D.2 of [27].

Setting $k = L_1$, we infer from the conjecture that a sample of a size in $O(\delta L_1^2)$ should contain at least one value of r such that the equation $|y|^2 = 2^{L_r} - |rz|^2$ is easily solvable and $p(r) > 1 - 1/L_1$. For such r the expected average cost of a RUS circuit that implements $(rz)^*/(rz)$ is less than $[2(1 + \delta)L_1 + \mathrm{const}]/(1 - 1/L_1)$. The latter converges in the asymptotic limit to $2(1 + \delta)L_1 + c_0$, where c_0 is a constant.

These observations lead to an algorithm for stage 2 as shown in Fig. 2 in Sec. D. 1 of [27]. It takes the value δ and sample size factor sz as hyperparameters. The T count function computes the minimal T count of a Clifford + T decomposition of a unitary (without necessarily performing such decomposition) and can be efficiently computed using methods in [17,25].

Input: angle θ , target precision ε, size factor sz ▷ hyperparameter δ

procedure SINGLE-QUBIT-DESIGN(θ, ε, sz)
  $ret \leftarrow None, \epsilon \leftarrow 2\varepsilon$
  while $ret = None$ **do**
    $\epsilon \leftarrow \epsilon/2$
    Compute $z \in \mathbb{Z}[\omega]$ s.t. $|z^*/z - e^{i\theta}| < \epsilon$ ▷ Lemma 2
    $Y \leftarrow$ RAND-NORMALIZATION-1(z, sz)
    if $Y \neq None$ **then**
      $r \leftarrow first(Y); y \leftarrow last(Y)$
      $L \leftarrow \log_2(|rz|^2 + |y|^2)$
      $ret \leftarrow \frac{1}{\sqrt{2}^L} \begin{bmatrix} rz & y \\ -y^* & rz^* \end{bmatrix}$
    end if
  end while
end procedure

Output: ret ▷ requisite unitary

FIG. 3. Algorithm to design the unitary V.

Stage 3: RUS unitary design.—When the randomized normalization algorithm succeeds for a given z, we can construct a single-qubit unitary V of the form, Eq. (2), where $y, z \in \mathbb{Z}[\omega], L \in \mathbb{Z}$, and $|z|^2/2^L > 1/2$ which maps to the probability of success of the RUS circuit. The unitary V can be decomposed exactly into an optimal ancilla-free Clifford + T circuit using methods in [20].

The algorithm in Fig. 3 outputs the unitary V. It calls the randomized normalization algorithm and is designed to combat its infrequent failure. A failure can only happen if we never encounter an easily solvable norm equation for any random sample. Every iteration of the precision $\epsilon \leftarrow \epsilon/2$ in the while loop of the algorithm adds sz more candidate norm equations to the search space. For large enough sz, the probability of never encountering a solvable norm equation decreases exponentially with the number of iterations.

Stage 4: RUS circuit synthesis.—From V we construct a two-qubit unitary U such that $U = \left[\begin{smallmatrix} V & 0 \\ 0 & V^\dagger \end{smallmatrix}\right]$. We synthesize U as a two-qubit repeat-until-success circuit on one ancilla qubit and one target qubit, such that the circuit applies a z rotation of z^*/z to the target qubit on success and the Pauli-Z operation on failure.

The unitary U can be realized as a two-qubit Clifford + T circuit such that the T count is the same or up to 9 gates higher than the T count of the optimal single-qubit Clifford + T circuit for unitary V (see Sec. E in [27] for the proof). The intuition is that given two single-qubit Clifford + T circuits with the same T count, one circuit can be manufactured from the other by insertion and deletion of Pauli gates, plus the addition of at most two non-Pauli Clifford gates which can result in a small potential T-count increase. The pseudocode for the two-qubit RUS circuit synthesis algorithm is given in Fig. 3 in Sec. E of [27]. Moreover, we find that half of the Pauli gates in the RUS circuit can be eliminated using a set of rewrite rules, described in Sec. F of [27]. We present an example of applying our RUS synthesis algorithm to the rotation $R_z(\pi/64)$ in Sec. G of [27].

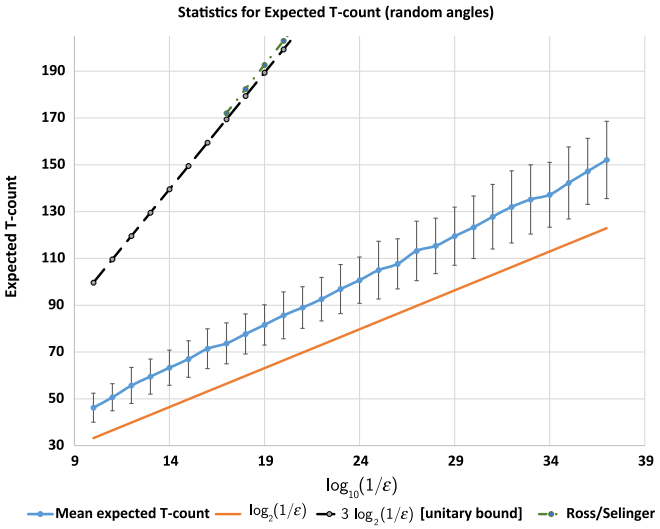

FIG. 4 (color online). Precision ε versus mean expected T count for a set of 1000 random angles.

Numerical results.—We evaluate the performance of our algorithm on a set of 1000 angles randomly drawn from the interval $(0, \pi/2)$ at 25 target precisions $\varepsilon \in \{10^{-11}, \ldots, 10^{-35}\}$. Figure 4 plots the precision ε versus the mean (and standard deviation) expected T count across the RUS circuits generated for the set of 1000 random angles. The regression formula for the mean expected T count is $3.817 \log_{10}(1/\varepsilon) + 9.2 = 1.149 \log_2(1/\varepsilon) + 9.2$ (blue). We also plot the mean T count achievable by Ref. [1] (green). We find similar results for the synthesis of Fourier angles (Sec. H of [27]).

Conclusions.—We have developed an efficient algorithm to synthesize an arbitrary single-qubit gate into a RUS circuit. The leading term for the expected T count is given by $c \log_2(1/\varepsilon)$, where c is approximately 1.15 for axial rotations. On average, our algorithm achieves a factor of 2.5 improvement over the theoretical lower bound for ancilla-free unitary Clifford + T decomposition, significantly reducing the resources required to implement quantum algorithms on a device.

We have also developed generalizations of RUS constructions to a broader set of targets including all unitary operations representable over the field of cyclotomic rationals. Our generalized designs allow tight control over the T depth and are presented in Sec. I of [27]. Future work will extend information-theoretic lower bounds for the expected cost of the RUS circuits to the generalized RUS designs. We plan to develop compilation algorithms to synthesize generalized RUS designs and to characterize the relationship between the number of ancillas, the properties of the RUS design, and their expected T counts.

We thank Gerry Myerson for pointing us to Wolfgang Schmidt's book [26]. We thank the QuArC team for discussing early versions of this work.

[1] N. Ross and P. Selinger, arXiv:1403.2975.
[2] V. Kliuchnikov, arXiv:1306.3200.
[3] P. Selinger, arXiv:1212.6253.
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] A. Paetznick and K. M. Svore, Quantum Inf. Comput. **14**, 1277 (2014).
[6] H. Ferguson and D. Bailey, http://crd.lbl.gov/dhbailey/dhbpapers/pslq.pdf.
[7] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson, Phys. Rev. A **82**, 020301 (2010).
[8] K. Shah and D. Oi, arXiv:1303.2066.
[9] V. Danos, E. Kashefi, and P. Panagaden, J. Assoc. Comput. Mach. **54**, 8 (2007).
[10] N. C. Jones, J. D. Whitfield, P. L. McMahon, M. Yung, R. van Meter, A. Aspuru-Guzik, and Y. Yamamoto, New J. Phys. **14**, 115023 (2012).
[11] C. Jones, Phys. Rev. A **87**, 022328 (2013).
[12] G. Duclos-Cianci and K. M. Svore, Phys. Rev. A **88**, 042325 (2013).
[13] N. Wiebe and V. Kliuchnikov, New J. Phys. **15**, 093041 (2013).
[14] S. Bravyi and A. Y. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[15] A. Meier, B. Eastin, and E. Knill, arXiv:1204.4221.
[16] S. Bravyi and J. Haah, Phys. Rev. A **86**, 052329 (2012).
[17] A. Bocharov and K. M. Svore, Phys. Rev. Lett. **109**, 190501 (2012).
[18] K. Matsumoto and K. Amano, arXiv:0806.3834.
[19] B. Giles and P. Selinger, arXiv:1312.6584.
[20] V. Kliuchnikov, D. Maslov, and M. Mosca, Quantum Inf. Comput. **13**, 607 (2012).
[21] B. Giles and P. Selinger, Phys. Rev. A **87**, 032332 (2013).
[22] A. Fowler, Quantum Inf. Comput. **11**, 867 (2011).
[23] P. Bertok, http://library.wolfram.com/infocenter/MathSource/4263/.
[24] If the trace distance metric is used to approximate unitaries and ϵ is the trace distance requested, it would suffice to set $\epsilon = \sqrt{2}\epsilon$ in this context.
[25] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo, arXiv:1308.4134.
[26] W. Schmidt, *Diophantine Approximation* (Springer-Verlag, Berlin, 1980).
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.114.080502 for the mathematical background for the letter, proofs of several key statements and additional numerical simulation results.