Efficient Synthesis of Universal Probabilistic Quantum Circuits†

Alex Bocharov*, Martin Roetteler*, and Krysta M. Svore*

*Quantum Architectures and Computation Group,
Microsoft Research, Redmond, WA (USA)

†Based on http://arxiv.org/abs/1404.5320 and http://arxiv.org/abs/1409.3552

Summary. Techniques to efficiently compile higher-level quantum algorithms into lower-level fault-tolerant circuits are needed for the implementation of a scalable, general purpose quantum computer. Several universal gate sets arise from augmenting the set of Clifford gates by additional gates that arise naturally from the underlying fault-tolerance scheme. Examples are the Clifford+T basis which arises, e.g., from the surface code and the concatenated Steane code, in which the gate $T = \left[\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{smallmatrix}\right]$ is added, and the Clifford+$\pi/12$ basis which arises, e.g., from quantum computing with metaplectic anyons [1], in which the gate $K = \left[\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\pi/6} \end{smallmatrix}\right]$ is added.

While in principle the Solovay-Kitaev algorithm [2, 3] can be used to solve the synthesis problem for *any* universal gate set, and therefore also the above-mentioned special cases, there are certain disadvantages to this approach, in particular the large depth of the resulting circuits. The best-known upper bound on the circuit depth is $O(\log^{3.97}(1/\varepsilon))$, where ε is the precision of the target approximation. In addition, the compilation time of the Solovay-Kitaev method, i.e., the time it takes to execute the classical algorithm that produces the output circuit, is quite high, namely almost cubic in $\log(1/\varepsilon)$. Fortunately, it was shown recently [4–7] that for the Clifford+T basis, elementary number theory can be leveraged to obtain much more efficient algorithms for approximating a single-qubit gate. The number of T gates in the resulting circuits scales close to $3\log_2(1/\varepsilon)$ for single-qubit rotations around the Z-axis and the compilation time for these algorithms has essentially the same scaling.

The point of the present work is two-fold. The first purpose (i) is to show that the constant in the above estimates can be further reduced; this may come as a surprise as there is an information-theoretic lower bound that establishes that there are Z-rotations that require $3\log_2(1/\varepsilon)$ many T gates to reach an approximation precision ε. However, this bound makes two assumptions: that the underlying circuits are unitary and that they act only on a single qubit. By relaxing both assumptions to (1) allow measurements and adaptive decisions on earlier results and (2) allow to operate on more than one qubit through the use of an ancilla, we show that this bound can be surpassed. Indeed, our best schemes lead to an expected T-gate count of $1.149\log_2(1/\varepsilon)$ for arbitrary Z-rotations. The second purpose (ii) is to show that we can overcome the limitation to only synthesize for the Clifford+T basis and develop a general synthesis framework. For several gate sets where the elementary gates have elements from an algebraic number field, we have developed algorithms that can synthesize efficient probabilistic quantum circuits. This includes the field $\mathbb{Q}(e^{\pi i/4})$, related to the Clifford+T basis, and the field $\mathbb{Q}(e^{\pi i/6})$, related to the metaplectic anyons.

We present two methods to synthesize probabilistic quantum circuits. Both can be thought of as Markov chains that implement a walk on a set of unitaries in which the target Z-rotation is an absorbing state of the walk: first, a method called "Repeat-Until-Success" in which all failure branches are just the identity so that no correction is necessary, with the drawback (with small probability) of a potentially unlimited run-time of the circuit, and second, a method called "Probabilistic Quantum Circuits with Fallback" in which the chain is always guaranteed to terminate, and corrections are performed in an adaptive fashion. Our main result is an efficient algorithm for single-qubit decomposition that achieves an expected gate count of $\log_b(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$, where b is related to an expansion property of the underlying basis; b is defined so that for a given

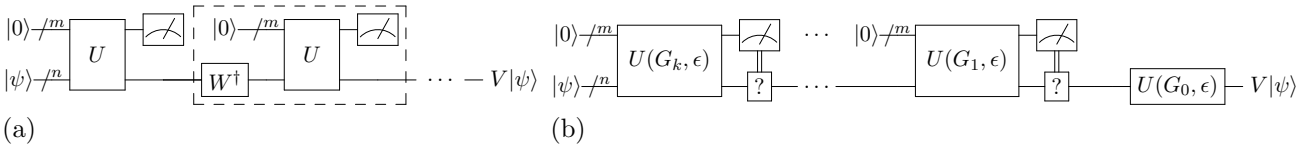


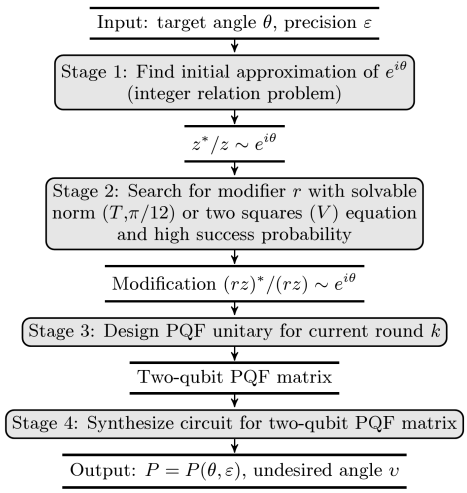
Figure 1: (a) RUS and (b) PQF protocols to implement a unitary V.

depth t the number of unique circuits scales as $\Theta(b^t)$. Specifically, $b = 2$ for Clifford+T, $b = 4$ for Clifford+$\pi/12$, and $b = 5$ for the so-called Clifford+V basis [8].

Probabilistic Quantum Circuits. The general layout of a Repeat-Until-Success (RUS) circuit protocol is shown in Fig. 1(a) [9]. Consider a unitary operation U acting on $n + m$ qubits, of which n are target qubits and m are ancillary qubits, where U is decomposed into a Clifford+T circuit. Consider a measurement of the ancilla qubits, such that one measurement outcome is labeled "success" and all other measurement outcomes are labeled "failure". Let the unitary applied to the target qubits upon measurement be V. 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 Clifford operator $W^\dagger$ is applied in order to revert the state of the target qubits to their original input state $|\psi\rangle$. We mainly focus on the case where $m = n = 1$ and where W is the identity. The *expected cost* of a RUS design is most often below the cost obtained with a purely unitary circuit design.

In contrast, the Probabilistic Quantum Circuit with Fallback (PQF) protocol requires at most a small finite number of rounds, each of which implement (possibly different) unitaries $U(G_i, \varepsilon)$ on several qubits that upon successful measurement lead to the application of G_i, and one final, purely unitary, correction step, called *fallback*, as shown in Fig. 1(b). The "question mark" box denotes the binary classical control switch that implements the remainder of the circuit if and only if the measurement result is 1. Let $F_j|\psi\rangle$ be the undesired result upon measurement of 1 at the j-th round of the protocol. Then $G_{j-1} = G_j F_j^\dagger$ and we note that the synthesis algorithm computes $\Pi_{j=0}^{k-1} G_j$. The final fallback correction step may have considerable cost, however the probability of requiring the fallback step can be very small, allowing for a decrease in overall expected cost.

Synthesis Algorithm. We have developed an algorithm to compile RUS circuits to approximate single-qubit rotations over the Clifford+T basis and an algorithm to compile PQF circuits that works equally well over at least three universal bases: Clifford+T, Clifford+$\pi/12$, and Clifford+V. The two algorithms share the same general flow shown on the right. However, since the PQF protocol implements different intermediate target rotations at each round, the compilation sequence shown must be run for each PQF round. The first stage of the sequence 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 of the form $a_0 \sin(\theta/2) + a_1 \sin(\theta/2 + \pi/m) + \ldots + a_{d-1} \sin(\theta/2 + (d-1)\pi/m) = 0$, $a_j \in \mathbb{Z}$, where d is algebraic degree of $e^{2\pi i/m}$, and $m = 4$ for the V basis, $m = 8$ for Clifford+T, and $m = 12$ for Clifford+$\pi/12$. This is a so-called "integer relation problem" and we solve it using the PSLQ algorithm [11, 12] where the termination condition is replaced by $|z^*/z - e^{i\theta}| < \varepsilon$. PSLQ can be thought of as a multivariate generalization of the continued fraction algorithm. We have proven that PSLQ performance is very close to optimal with



$|z| < \kappa\,\varepsilon^{-1/4}$, for Clifford+$T$ and Clifford+$\pi/12$, and $|z| < \kappa\,\varepsilon^{-1/2}$ for Clifford+V.

The second stage aims at "boosting" the success probability: we perform several modification trials $z \mapsto (r\,z)$, where r is in the real subring R of the cyclotomic integers $\mathbb{Z}[\omega]$. The purpose of the trials is to find an $r \in R$ such that (1) the probability of an undesired measurement outcome is asymptotically small (e.g., in $O(1/\log(1/\varepsilon))$), and (2) $r\,z$ can be expanded into a unitary matrix

$$U = \frac{1}{\sqrt{b}^L} \begin{bmatrix} r\,z & y \\ -y^* & r\,z^* \end{bmatrix}$$

where $y \in \mathbb{Z}[\omega]$, $b = 5$ for the V basis; $b = 2$ for the Clifford+T and Clifford+$\pi/12$ bases.

In the third stage, the two-qubit matrix corresponding to the unitary part of the RUS circuit or to the unitary part of the current round in the PQF protocol is assembled. This stage is core for the circuit synthesis given a suitable matrix U as above has been found (at Stage 2). For a PQF round the desired two-qubit matrix is simply $U_{PQF} = \mathrm{CNOT}\,(I \otimes V)\,\mathrm{CNOT}$ whereas in the RUS case it is $U_{RUS} = \left[\begin{smallmatrix} V & 0 \\ 0 & V^\dagger \end{smallmatrix}\right]$.

During the fourth stage, an exact two-qubit circuit that implements the unitary obtained in Stage 3 is compiled. It is somewhat hard only in the RUS version. We have proved in [10] that a two-qubit circuit for U_{RUS} can be obtained as an expansion of a single-qubit Clifford+T for V using processes described as *T-code representation* and *Pauli decoration*. We have proven that an overhead introduced by these processes never exceeds nine T gates.

Cost Analysis. We prove that, given a desired precision ε, our PQF compilation method generates multi-round PQF circuits with a mean expected execution cost in $\log_b(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$, where $b = 5$ for the V basis, $b = 4$ for Clifford+$\pi/12$ and $b = 2$ for Clifford+T. The RUS circuits generated by the RUS compilation method over Clifford+T display the same asymptotic bound with $b = 2$. We also show that multi-round PQF circuits follow a law of diminishing returns, with a mean expected execution cost of the form $C_{round}/p + O(q^k)$, where k is the number or rounds, C_{round} is a typical cost of executing the two-cubit unitary for a round, p is a typical probability of obtaining the favorable measurement in a round, and $q = 1 - p$ is a typical probability of obtaining the unfavorable measurement. Since our methods suppress q to a value in $O(1/\log(1/\varepsilon))$, then possible distinction between the k-round and $k+1$-round PQF protocols is in $O(1/\log(1/\varepsilon)^k)$.

Numerical Results. We evaluate the performance of our algorithms on a set of 1000 angles randomly drawn from $(0, \pi/2)$ at 30 target precisions $\varepsilon \in \{10^{-11}, \ldots, 10^{-40}\}$. Fig. 2 compares the cost of RUS and one-round PQF circuits over the Clifford+T basis. Maximum likelihood bounds for mean expected T-count are $1.149\,\log_2(1/\varepsilon) + 9.2$ for RUS and $\log_2(1/\varepsilon) + 4\,\log_2(\log_2(1/\varepsilon)) + 1.187$ for one-round PQF. The mean expected V-count for Clifford+V is $\log_5(1/\varepsilon) + 0.95\,\log_5(\log_5(1/\varepsilon)) + 7.26$; the mean expected $\pi/12$-count for Clifford+$\pi/12$ is $\log_4(1/\varepsilon) + 2\,\log_2(\log_2(1/\varepsilon)) + 3.48$.

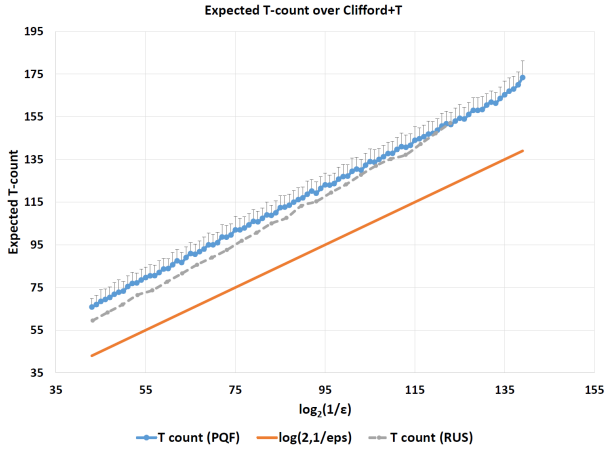


Figure 2: Precision ε versus mean expected T-count.

[1] S. X. Cui and Z. Wang, "Universal quantum computation with metaplectic anyons," (2014), 1405.7778.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[3] C. Dawson and M. Nielsen, Quantum Information and Computation **6**, 81 (2006).
[4] P. Selinger, "Efficient Clifford+T approximation of single-qubit operators," (2012), 1212.6253.
[5] N. Ross and P. Selinger, "Optimal ancilla-free Clifford+T approximation of z-rotations," (2014), 1403.2975.
[6] V. Kliuchnikov, D. Maslov, and M. Mosca, "Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits," (2012), 1212.6964.
[7] V. Kliuchnikov, "Synthesis of unitaries with Clifford+T circuits," (2013), 1306.3200.
[8] A. Bocharov, M. Gurevich, and K. Svore, "Efficient decomposition of single-qubit gates into V basis circuits," (2013), 1303.1411.
[9] A. Paetznick and K. Svore, "Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries," (2013), 1311.1074.
[10] A. Bocharov and M. Roetteler and K. Svore, "Efficient synthesis of universal Repeat-Until-Success circuits," (2014), 1404.5320.
[11] H. Ferguson and D. Bailey, "A polynomial time, numerically stable integer relation algorithm," http://crd.lbl.gov/ dhbailey/dhbpapers/pslq.pdf.
[12] P. Bertok, "PSLQ integer relation algorithm implementation," (2004), http://library.wolfram.com/infocenter/MathSource/4263/.