

Single-qubit rotation algorithm with logarithmic Toffoli count and gate depth

Christoffer Hindlycke^{✉*} and Jan-Åke Larsson[†]Department of Electrical Engineering, [Linköping University](https://www.linkoping.se), 581 83 Linköping, Sweden

(Received 12 April 2024; accepted 9 October 2024; published 28 October 2024)

Building generic gates from a restricted gate set is a difficult but important problem, especially in the noisy regime where only a limited set of noise-resistant gates are available, e.g., fault-tolerant Clifford gates (generated by Hadamard, phase, and CNOT gates) and fault-tolerant Toffoli gates. The Toffoli is also often used as a building block of many algorithms and will need to be constructed if not directly available. This makes Clifford+Toffoli an attractive gate set for building generic gates. In this Letter we give a simple and efficient algorithm for building an approximate single-qubit rotation using only Clifford+Toffoli, which in turn enables any generic single-qubit unitary. An important difference compared to earlier attempts is that the use of the Toffoli allows us to use simple rounding as opposed to a complicated approximation algorithm. The resulting gate array does not rely on repeatedly applying a fixed rotation, but immediately applies a rotation R_{θ^*} that is ϵ -close to the desired rotation R_{θ} , with a success probability strictly greater than $1/2$. It can be rerun upon failure, giving an expected number of repetitions strictly less than 2, an expected Toffoli count strictly less than $4\lceil\log \frac{1}{\epsilon}\rceil$, an expected gate depth strictly less than $4\lceil\log \frac{1}{\epsilon}\rceil + 6$, and uses $2\lceil\log \frac{1}{\epsilon}\rceil$ ancillas. The small circuit depth of our construction enables low-noise gates on existing quantum computational devices, and allows for arbitrary precision using a very modest number of ancillas.

DOI: [10.1103/PhysRevResearch.6.L042027](https://doi.org/10.1103/PhysRevResearch.6.L042027)

Introduction. The Toffoli gate is a fundamental tool in quantum computing and is crucial in Shor's algorithm [1,2], quantum error correction [3–8], and shallow quantum circuits [9]. Many of these quantum algorithms also need arbitrarily small single-qubit rotations. In general, the approximation of generic gates using a finite gate set is essential. This is especially true in the fault tolerant quantum computing era where direct fault-tolerant constructions are typically available only for a limited number of gates, so that short generation of generic gates is an absolute necessity for high-performance computing [10]. The Solovay-Kitaev theorem [11,12] tells us that with access to a limited but well-chosen set of single-qubit quantum gates, an approximation to any desired single-qubit gate to within distance ϵ can be constructed, with a gate depth close to cubic in the logarithm of $\frac{1}{\epsilon}$; this has recently been improved to the power 1.44 [13].

For specific gate sets, the most common gate set to study is that of Clifford+ T . The algorithm of Kliuchnikov *et al.* [14] achieves complexity logarithmic in $\frac{1}{\epsilon}$, which is optimal up to a multiplicative constant; subsequent efforts have been focused on identifying and reducing this constant [15–20].

The Clifford+Toffoli gate set will be available in future quantum computer hardware, since the Toffoli gate is indispensable for quantum computing, so a large amount of work has been put towards its practical implementation [21–25]. It is therefore natural to ask if generic unitaries can be built using that gate set; some recent results [26,27] give complexity $O(\log \frac{1}{\epsilon})$. An equivalent gate set is Clifford+controlled-phase where the conversion cost from one to the other is a factor 3 [27,28], so that, e.g., the algorithm from Ref. [29] gives an equivalent Toffoli count of $24 \log \frac{1}{\epsilon}$.

Here, we give an explicit construction for approximating any z -axis rotation using the Clifford+Toffoli gate set with an expected Toffoli count $4\lceil\log \frac{1}{\epsilon}\rceil$. Three such rotations allow the approximation of any single-qubit gate. The construction is very simple and efficient, as it requires only a trigonometric expression of the desired rotation angle, rounded to the desired accuracy. The resulting algorithm has an expected gate depth $4\lceil\log \frac{1}{\epsilon}\rceil + 3$ and uses $2\lceil\log \frac{1}{\epsilon}\rceil$ ancillas; the low gate depth and algorithm simplicity will make constructions of this kind ubiquitous in quantum computing.

Our starting point is an algorithm, conceptually simpler than Solovay-Kitaev, but less efficient: Repeatedly applying the fixed rotation generated by a circuit by Nielsen and Chuang (see Ref. [28], p. 198) that contains only gates from Clifford+Toffoli. This fixed φ rotation around the z axis has $\cos \varphi = 3/5$, $\sin \varphi = 4/5$ and is applied with probability $5/8$; see Fig. 1(a). As φ is an irrational multiple of π , repeated application allows for the approximation of any rotation on one qubit around the z axis. This algorithm has a constant gate depth for each repetition but requires $O(\frac{1}{\epsilon})$ repetitions on average.

*Contact author: christoffer.hindlycke@liu.se†Contact author: jan-ake.larsson@liu.se

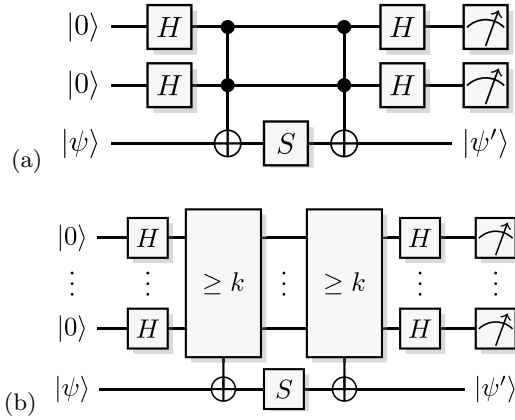


FIG. 1. Circuits for approximate qubit rotation. (a) Circuit that applies R_φ to $|\psi\rangle$ ($\cos \varphi = 3/5$, $\sin \varphi = 4/5$) with probability $5/8$; otherwise a Z gate. (b) Circuit that applies R_{θ^*} to $|\psi\rangle$, close to a desired rotation R_θ with high probability, where the ancilla count n and comparison k should be chosen according to Theorem 1.

In this Letter, we modify this algorithm to be efficient, avoiding a high repetition count. We introduce additional ancillary controls and replace the two Toffoli gates with $\geq k$ tests in the circuit, giving control over the actual rotation angle. This gate array either applies the desired rotation to within distance ϵ with probability strictly greater than $1/2$ or applies a Z gate; the measurement carried out on the controls indicates if a Z gate was applied, and then we correct the input state and try again. The resulting algorithm has a nonconstant gate depth $O(\log \frac{1}{\epsilon})$ for each repetition, but instead requires strictly less than two (a constant number of) repetitions on average. We essentially replace a linear number $O(\frac{1}{\epsilon})$ of repetitions with a logarithmic number $O(\log \frac{1}{\epsilon})$ of ancillas and interconnecting Toffoli gates.

Approximating an arbitrary rotation. The circuit in Fig. 1(a) works by marking a certain number of superposed states, by adding the relative phase factor $i = e^{i\frac{\pi}{2}}$. Increasing the number of controls increases the number of superposed states, giving more fine-grained control over the exact ratio of marked/unmarked states and therefore more control over the resulting rotation angle. Then, the two Toffoli gates can be replaced with an n -qubit $\geq k$ test, as depicted in Fig. 1(b). A $\geq k$ test on n qubits is possible for $0 \leq k \leq 2^n$: If the control binary digit is greater than or equal to a given limit k , the target is inverted. We focus on the quantum state after the second $\geq k$ test; of the computational basis states contained in $|+^n, 0\rangle$, the circuit leaves k states unmarked and marks $2^n - k$ states with an extra phase factor $i = e^{i\frac{\pi}{2}}$. With

$$C = |k + i(2^n - k)|, \quad 0 \leq v = \arg[k + i(2^n - k)] \leq \frac{\pi}{2}, \quad (1)$$

the scalar product with the $|+^n, 0\rangle$ state is

$$\frac{k + i(2^n - k)}{2^n} = \frac{C \cos v + iC \sin v}{C(\cos v + \sin v)} = \frac{e^{iv}}{\cos v + \sin v}. \quad (2)$$

For the $|+^n, 1\rangle$ state, the circuit marks k states of the computational basis and leaves $2^n - k$ states unmarked. The scalar

product with the $|+^n, 1\rangle$ state is

$$\frac{2^n - k + ik}{2^n} = \frac{e^{i(\frac{\pi}{2}-v)}}{\cos v + \sin v} = \frac{e^{iv}}{\cos v + \sin v} e^{i(\frac{\pi}{2}-2v)}. \quad (3)$$

Therefore, if the measurement outcome after the final Hadamards is n zeros, we have performed an R_{θ^*} rotation, where $\theta^* = \frac{\pi}{2} - 2v$, so that $-\frac{\pi}{2} \leq \theta^* \leq \frac{\pi}{2}$ and

$$k = C \cos v = 2^n \frac{\cos v}{\cos v + \sin v} = 2^n \frac{1 + \tan \frac{\theta^*}{2}}{2}. \quad (4)$$

We can now perform a rotation R_{θ^*} arbitrarily close to an ideal rotation R_θ for $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$, by adjusting the number of controlling ancillas n and rounding $2^{n-1} \tan \frac{\theta}{2}$ to the closest integer. Calculating $\tan \frac{\theta}{2}$ can be done in polynomial time on a classical computer. We have the following theorem.

Theorem 1. Given a desired rotation angle $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$ and accuracy $\epsilon > 0$, choose ancilla count

$$n = 1 + \lceil \log \frac{1}{\epsilon} \rceil \quad (5)$$

and comparison

$$k = 2^{n-1} + \lfloor 2^{n-1} \tan \frac{\theta}{2} + \frac{1}{2} \rfloor, \quad (6)$$

which corresponds to choosing θ^* so that

$$2^{n-1} \tan \frac{\theta^*}{2} = \lfloor 2^{n-1} \tan \frac{\theta}{2} + \frac{1}{2} \rfloor. \quad (7)$$

Using $|0\rangle^{\otimes n} |\psi\rangle$ as the input to the circuit in Fig. 1(b), if the ancilla measurement outcomes are all zero, the circuit applied an R_{θ^*} rotation to $|\psi\rangle$, with an extra global phase, such that $\|R_\theta - R_{\theta^*}\| \leq |\theta - \theta^*| \leq \epsilon$. This happens with probability $\frac{1}{2} + \frac{1}{2} \tan^2(\frac{\theta^*}{2}) \geq \frac{1}{2}$.

Proof. By the preceding equations, when the measurement outcomes are all zero, the circuit applied the rotation R_{θ^*} with an extra global phase $v = \frac{\pi}{4} - \frac{\theta^*}{2}$, and this happens for all $|\psi\rangle$ with probability

$$P(0^n) = \frac{1}{(\cos v + \sin v)^2} = \frac{1}{1 + \cos \theta^*} = \frac{1 + \tan^2 \frac{\theta^*}{2}}{2}. \quad (8)$$

It remains to bound the distance between the actual rotation R_{θ^*} being carried out and the desired rotation R_θ . We have

$$\begin{aligned} \|R_\theta - R_{\theta^*}\| &= \sup_{\langle \varphi | \varphi \rangle = 1} \|(R_\theta - R_{\theta^*})|\varphi\rangle\|_2 = |e^{i\theta} - e^{i\theta^*}| \\ &= |e^{i\frac{\theta+\theta^*}{2}} (e^{i\frac{\theta-\theta^*}{2}} - e^{-i\frac{\theta-\theta^*}{2}})| = 2 \left| \sin \frac{\theta-\theta^*}{2} \right| \\ &\leq |\theta - \theta^*| \leq 2 \left| \tan \frac{\theta-\theta^*}{2} \right| = 2 \left| \frac{\tan \frac{\theta}{2} - \tan \frac{\theta^*}{2}}{1 + \tan \frac{\theta}{2} \tan \frac{\theta^*}{2}} \right| \\ &\leq 2 \left| \tan \frac{\theta}{2} - \tan \frac{\theta^*}{2} \right| \leq 2^{-n+1} \leq 2^{-\log \frac{1}{\epsilon}} = \epsilon, \end{aligned} \quad (9)$$

because $\tan \frac{\theta}{2} \tan \frac{\theta^*}{2} \geq 0$. ■

In Theorem 1 we use the smallest possible choice for n such that the error is less than ϵ . We note that for $\theta^* \neq 0$, the probability of success is strictly greater than $1/2$. We should also point out that if $\theta^* = 0$, measurement outcomes all zero will result in an $R_0 = \mathbb{I}$ rotation having been applied by our circuit, which then must be close enough to the desired R_θ rotation. This case is better handled by applying the identity operator to $|\psi\rangle$, so the success probability is then 1. Similarly,

$\theta^* = \pm \frac{\pi}{2}$ corresponds to applying the $S = R_{\pi/2}$ or the $S^\dagger = R_{-\pi/2}$ rotation, but also gives the trivial comparisons $k = 2^n$ or $k = 0$; the S or $S^\dagger$ gate is then applied with probability 1, as stated in the theorem.

Corollary 1. The approximation in Theorem 1 can be made exact if and only if there exists an n such that $2^n \tan \frac{\theta}{2}$ is an integer.

Proof. Theorem 1 gives $\theta^* = \theta$ if and only if using such an n . ■

Corollary 2. The set of θ for which Theorem 1 gives an exact R_θ is dense in $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$.

Proof. Let $\theta_m = 2 \arctan(2^{-m} \lfloor 2^m \tan \frac{\theta}{2} + \frac{1}{2} \rfloor)$. Theorem 1 gives $\theta_m^* = \theta_m$ for $n \geq m + 1$, and $\lim_{m \rightarrow \infty} \theta_m = \theta$. ■

If the measurement outcomes are not all zero, the following holds.

Theorem 2. Let n, k, θ^* be as in Theorem 1. Using $|0\rangle^{\otimes n} |\psi\rangle$ as input to the circuit in Fig. 1(b), if the ancilla measurement outcomes are not all zero, the circuit applied a Z gate to $|\psi\rangle$, with an extra global phase. This happens with probability $\frac{1}{2} - \frac{1}{2} \tan^2(\frac{\theta^*}{2}) \leq \frac{1}{2}$.

Proof. The probability that the measurement outcomes are not all zero follows from Theorem 1. After the second $\geq k$ test, the measurement eigenstate for outcome x is

$$|\Theta_{n,x}\rangle = H^{\otimes n} |x\rangle = 2^{-\frac{n}{2}} \sum_{y=1}^{2^n-1} (-1)^{x \cdot y} |y\rangle. \quad (10)$$

Also, with $|\psi\rangle = |0\rangle$, at that point the quantum state is

$$|\Psi_{n,k}\rangle = 2^{-\frac{n}{2}} \left(\sum_{j=0}^{k-1} |j\rangle + \sum_{j=k}^{2^n-1} i |j\rangle \right), \quad (11)$$

and with $|\psi\rangle = |1\rangle$ the quantum state is

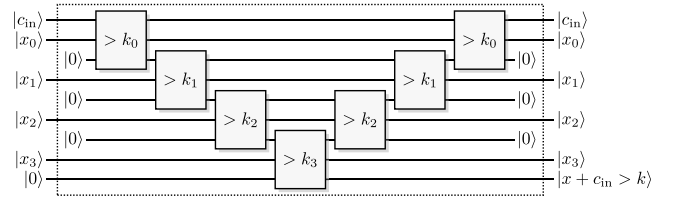
$$|\Phi_{n,k}\rangle = 2^{-\frac{n}{2}} \left(\sum_{j=0}^{k-1} i |j\rangle + \sum_{j=k}^{2^n-1} |j\rangle \right). \quad (12)$$

If $x \neq 0$ we have

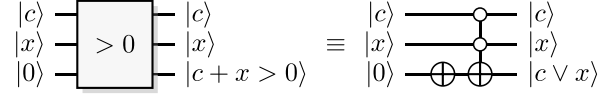
$$\begin{aligned} \langle \Theta_{n,x} | \Psi_{n,k} \rangle &= 2^{-n} \left(\sum_{j=0}^{k-1} (-1)^{x \cdot j} + i \sum_{j=k}^{2^n-1} (-1)^{x \cdot j} \right) \\ &= 2^{-n} \left((1-i) \sum_{j=0}^{k-1} (-1)^{x \cdot j} + i \sum_{j=0}^{2^n-1} (-1)^{x \cdot j} \right) \\ &= 2^{-n} (1-i) \sum_{j=0}^{k-1} (-1)^{x \cdot j} \end{aligned} \quad (13)$$

and

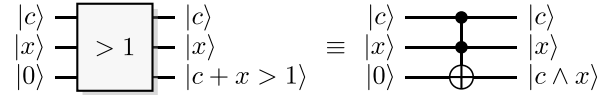
$$\begin{aligned} \langle \Theta_{n,x} | \Phi_{n,k} \rangle &= 2^{-n} \left(i \sum_{j=0}^{k-1} (-1)^{x \cdot j} + \sum_{j=k}^{2^n-1} (-1)^{x \cdot j} \right) \\ &= 2^{-n} (i-1) \sum_{j=0}^{k-1} (-1)^{x \cdot j} = -\langle \Theta_{n,x} | \Psi_{n,k} \rangle, \quad (14) \end{aligned}$$



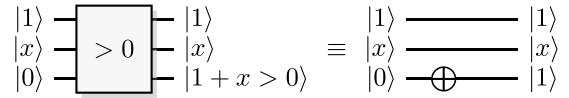
(a) Comparator circuit from bitwise ripple-carry comparisons



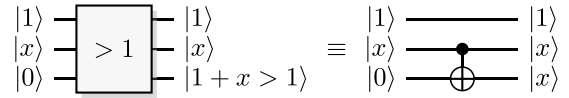
(b) Bit comparison with $k_j = 0$, white controls are inverted



(c) Bit comparison with $k_j = 1$



(d) Bit comparison with $k_j = 0$ and carry-in $|c\rangle = |1\rangle$



(e) Bit comparison with $k_j = 1$ and carry-in $|c\rangle = |1\rangle$

FIG. 2. Bitwise ripple-carry comparator made of a sequence of Toffoli gates. For indices where $k_j = 0$, the modified Toffoli realizes a quantum OR gate. If carry-in is constant 1 the bit comparisons simplify.

so the circuit applied a Z gate on $|\psi\rangle$ with the global phase $\arg(1-i) = -\frac{\pi}{4}$ or $\arg(i-1) = \frac{3\pi}{4}$ depending on the sign of the remaining sum in Eq. (13). ■

Explicit gate array and gate counts. A straightforward construction of the $\geq k$ test is to encode k in an additional ancillary n -qubit register and use a ripple-carry comparator [30]. But since k is a classical constant, we can also use it to build the gate array. A ripple-carry bitwise comparison with a classical constant k is shown in Figs. 2(a)–2(c). Note that the circuit in Fig. 1(a) is a special case of our circuit where $n = 2$ and $k = 3$. Also, the construction is somewhat similar to a textbook n -control Toffoli construction, in fact, using this design for a $\geq k = 2^n - 1$ comparator gives exactly the construction in Ref. [28], Fig. 4.10.

This greater-than ($>k$) comparator can be turned into a greater-or-equal ($\geq k$) comparator by setting carry-in to 1, such a constant input can also be used to simplify the gate array. If $k_j = 0$ and $|c\rangle$ is known to be $|1\rangle$ [see Fig. 2(d)], neither carry-in nor the input $|x\rangle$ are used so they can be omitted from the circuit, and carry-out is $|1\rangle$ so further reductions will occur. If $k_j = 1$ and $|c\rangle$ is known to be $|1\rangle$ [see Fig. 2(e)], the comparison outputs $|x\rangle$ itself so the carry-in can be omitted; if the bit comparison target is an ancillary system also the controlled-NOT (CNOT) and target ancilla can be omitted, and only $|x\rangle$ needs to be retained.

With these simplifications the lowest significant bit comparison uses no gates and no ancilla internal to the comparator. Also, the highest significant comparison uses a single Toffoli and no ancilla internal to the comparator, and the others use two Toffolis and one ancilla internal to the comparator. Thus, the comparator uses $2n - 3$ Toffolis, and $n - 2$ internal ancillas.

We use two comparators in the circuit which would give total Toffoli count $4n - 6$ but this can be reduced further by omitting the uncomputation of the intermediate values in the internal ancillas and reusing the same ancillas in the second comparator, which then only needs to perform the uncomputation step. After this reduction, the Toffoli count is $2n - 2 = 2\lceil \log \frac{1}{\epsilon} \rceil$. Since the comparator-internal ancilla count is $n - 2$, the total ancilla count of the gate array is also $2n - 2 = 2\lceil \log \frac{1}{\epsilon} \rceil$.

If the lowest significant bits of k are 0, the Toffoli count reduces further because of the constant output of the bit comparator of Fig. 2(d), in which case the lowest significant bits of x are also not needed. When this happens one can reduce the ancilla count n but retain the same accuracy ϵ , and we give an example below that may clarify this. In any case, an upper bound to the Toffoli count is $2n - 2 = 2\lceil \log \frac{1}{\epsilon} \rceil$.

Repeat until success. The circuit of Fig. 1(b) performs a probabilistic approximation, so it can fail. The following algorithm, which has random runtime, instead always succeeds and has several other good properties.

Theorem 3. Let X be the random number of times Algorithm 1 repeats until it applies an R_{θ^*} rotation to $|\psi\rangle$. Then X is geometrically distributed, $X \geq 1$, $P(X > m) < 2^{-m}$, and $E(X) < 2$.

ALGORITHM 1. Rotation algorithm.

Input $\theta, \epsilon, |\psi\rangle$
Output $R_{\theta^*} |\psi\rangle$ where $\|R_{\theta} - R_{\theta^*}\| \leq \epsilon$
1: **choose** n, k, θ^* as in Theorem 1
2: **if** $\theta^* \neq 0$ **repeat**
3: **prepare** n ancillary qubits $|\phi\rangle = |0\rangle^{\otimes n}$
4: **apply** $H^{\otimes n}$ to $|\phi\rangle$
5: **apply** a $\geq k$ test on $|\phi\rangle$ with target $|\psi\rangle$
6: **apply** S to $|\psi\rangle$
7: **apply** a $\geq k$ test on $|\phi\rangle$ with target $|\psi\rangle$
8: **apply** $H^{\otimes n}$ to $|\phi\rangle$
9: **measure and discard** ancillas $|\phi\rangle$
10: **if** outcomes are not all zero **then**
11: **apply** Z to $|\psi\rangle$
12: **until** outcomes are all zero

Proof. Each repetition of Algorithm 1 is independent and at least one attempt is needed, so $X \geq 1$. By Theorem 2 the probability of applying R_{θ^*} to $|\psi\rangle$ is strictly greater than $1/2$. Then, X is geometrically distributed, $P(X > m) < 1 - \sum_{j=1}^m 2^{-j} = 2^{-m}$ and $E(X) < \frac{1}{1/2} = 2$. ■

Corollary 3. Algorithm 1 has an expected Toffoli count strictly less than $4\lceil \log \frac{1}{\epsilon} \rceil$.

Proof. The gate array has at most Toffoli count $2\lceil \log \frac{1}{\epsilon} \rceil$, so the corollary follows from Theorem 3. ■

Corollary 4. Algorithm 1 has an expected gate depth strictly less than $4\lceil \log \frac{1}{\epsilon} \rceil + 6$.

Proof. If the gate in Fig. 2(b) is counted as a single modified Toffoli, the gate depth is the Toffoli count plus 3, so the corollary follows from Theorem 3. ■

Example: Approximating the T gate. The T (or $\frac{\pi}{8}$) gate is a frequently used universal gate that applies an $R_{\frac{\pi}{4}}$ rotation to a single qubit. For illustrative purposes we perform a coarse approximation here with $\|T - R_{\theta^*}\| \leq |\frac{\pi}{4} - \theta^*| \leq 10^{-2}$. The number of ancillas should be chosen as

$$n = 1 + \lceil \log 10^2 \rceil = 8, \quad (15)$$

so that

$$k = 2^7 + \lfloor 2^7 \tan \frac{\pi}{8} + \frac{1}{2} \rfloor = 128 + 53 = 10110101_2. \quad (16)$$

The probability of success per repetition is

$$P(0^n) = \frac{1 + (\frac{53}{128})^2}{2} = \frac{19193}{32768} \approx 0.5857. \quad (17)$$

We select n to give at least the desired accuracy, but here

$$2^7 \tan \frac{\pi}{8} = 110101.000001001\dots_2, \quad (18)$$

so the rounding error is much smaller than $\frac{1}{2}$. The actual approximation error is

$$\|T - R_{\theta^*}\| \leq \left| \frac{\pi}{4} - \theta^* \right| = \frac{\pi}{4} - 2 \arctan \frac{53}{128} \approx 2.579 \times 10^{-4}. \quad (19)$$

The small rounding error has the effect that selecting n in the range $8 < n \leq 12$ would give zeros for the lowest significant bits of k . Then the simplification in Fig. 2(d) would apply one or more times, so that the circuit still would simplify to that in Fig. 3. For the T gate, the choice $n = 8$ gives such a good approximation that the next improvement does not occur until $n = 13$.

In actual use the accuracy will need to be better. For example, factoring an m -bit integer using Shor's algorithm requires approximating close to $2m \log m$ single-qubit gates [16], and with $m = 10000$ this number is 2.7×10^5 . If the total error

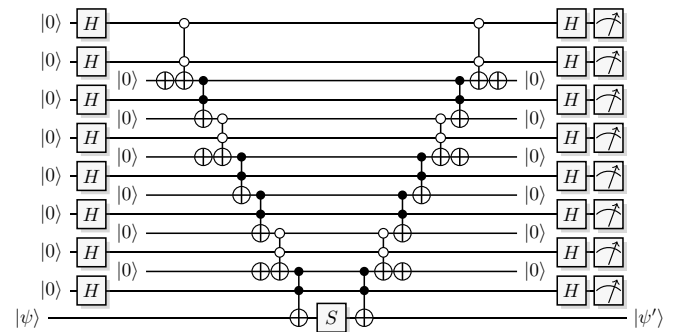


FIG. 3. Gate array that approximates the T gate. If ancilla measurement outcomes are all zero, the circuit applied an R_{θ^*} rotation to $|\psi\rangle$ where $\|T - R_{\theta^*}\| \leq |\frac{\pi}{4} - \theta^*| < 2.6 \times 10^{-4}$. This happens with probability > 0.58 ; for other measurement outcomes the circuit applied a Z gate on $|\psi\rangle$. The circuit contains a comparator with the integer $k = 10110101_2$, starting with the least significant bit comparison at the top.

due to gate approximation is required to be less than 0.01%, assuming the errors add, we need $\epsilon \approx 10^{-4}/(2.7 \times 10^5) \approx 3.8 \times 10^{-9}$ or $n = 33$.

Conclusions. We have proposed an algorithm for generating a phase rotation R_{θ^*} that is ϵ -close to a desired rotation R_{θ} , inspired by an earlier construction in Nielsen and Chuang [28]. The construction uses a $\geq k$ test that allows for simple selection of the rotation angle, and consists only of gates from the Clifford+Toffoli gate set. Our algorithm that uses this circuit has an expected Toffoli count strictly less than $4\lceil \log \frac{1}{\epsilon} \rceil$, an expected gate depth strictly less than $4\lceil \log \frac{1}{\epsilon} \rceil + 6$, and uses $2\lceil \log \frac{1}{\epsilon} \rceil$ ancillas,

This is a cubic improvement over the Solovay-Kitaev algorithm [11,12] and an improvement both over existing generic algorithms and those specifically involving the Clifford+Toffoli gate set [13,26,27]. A lower bound

can be obtained by a simple counting argument [31], but that bound depends on the gate set size which here involves the number of ancillas, so the bound increases slightly slower than logarithmic in $\frac{1}{\epsilon}$, allowing a small margin for improvement. However, the present algorithm uses only gates with bounded fan-in [9], so there may not be such a margin: We conjecture this is the case. Proving this would be an interesting development of our results.

Our construction only relies on being able to calculate $\tan \frac{\theta}{2}$, so it requires only a polynomial classical runtime and space to generate. In addition, the relative simplicity of our algorithm makes it attractive as a standard tool in quantum engineering. It is our hope that this, in combination with its efficient implementation, will make it useful for both theoretical and practical pursuits.

-
- [1] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1994), pp. 124–134.
 - [2] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26**, 1484 (1997).
 - [3] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52**, R2493 (1995).
 - [4] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo, Experimental quantum error correction, *Phys. Rev. Lett.* **81**, 2152 (1998).
 - [5] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, Benchmarking quantum computers: The five-qubit error correcting code, *Phys. Rev. Lett.* **86**, 5811 (2001).
 - [6] J. Chiaverini, D. Leibfried, T. Schaetz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, and D. J. Wineland, Realization of quantum error correction, *Nature (London)* **432**, 602 (2004).
 - [7] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Realization of three-qubit quantum error correction with superconducting circuits, *Nature (London)* **482**, 382 (2012).
 - [8] D. Nigg, M. Müller, E. A. Martinez, P. Schindler, M. Hennrich, T. Monz, M. A. Martin-Delgado, and R. Blatt, Quantum computations on a topologically encoded qubit, *Science* **345**, 302 (2014).
 - [9] S. Bravyi, D. Gosset, and R. König, Quantum advantage with shallow circuits, *Science* **362**, 308 (2018).
 - [10] J. Preskill, Reliable quantum computers, *Proc. R. Soc. London, Ser. A* **454**, 385 (1998).
 - [11] A. Y. Kitaev, Quantum computations: Algorithms and error correction, *Russ. Math. Surv.* **52**, 1191 (1997).
 - [12] C. M. Dawson and M. A. Nielsen, The Solovay-Kitaev algorithm, *arXiv:quant-ph/0505030*.
 - [13] G. Kuperberg, Breaking the cubic barrier in the Solovay-Kitaev algorithm, *arXiv:2306.13158*.
 - [14] V. Kliuchnikov, D. Maslov, and M. Mosca, Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits, *Phys. Rev. Lett.* **110**, 190502 (2013).
 - [15] A. Paetznick and K. M. Svore, Repeat-until-success: non-deterministic decomposition of single-qubit unitaries, *Quantum Inf. Comput.* **14**, 1277 (2014).
 - [16] V. Kliuchnikov, D. Maslov, and M. Mosca, Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits, *IEEE Trans. Comput.* **65**, 161 (2016).
 - [17] N. J. Ross and P. Selinger, Optimal ancilla-free Clifford+ T approximation of z -rotations, *Quantum Inf. Comput.* **16**, 901 (2016).
 - [18] P. Selinger, Efficient Clifford+ T approximation of single-qubit operators, *arXiv:1212.6253*.
 - [19] A. Bocharov, M. Roetteler, and K. M. Svore, Efficient synthesis of universal repeat-until-success quantum circuits, *Phys. Rev. Lett.* **114**, 080502 (2015).
 - [20] V. Gheorghiu, M. Mosca, and P. Mukhopadhyay, T -count and T -depth of any multi-qubit unitary, *npj Quantum Inf.* **8**, 141 (2022).
 - [21] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O’Brien, A. Gilchrist, and A. G. White, Simplifying quantum logic using higher-dimensional Hilbert spaces, *Nat. Phys.* **5**, 134 (2009).
 - [22] T. Monz, K. Kim, W. Hänsel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, Realization of the quantum Toffoli gate with trapped ions, *Phys. Rev. Lett.* **102**, 040501 (2009).
 - [23] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. S. Bishop, B. R. Johnson, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Demonstration of two-qubit algorithms with a superconducting quantum processor, *Nature (London)* **460**, 240 (2009).
 - [24] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva, and A. Wallraff, Implementation of a Toffoli gate with superconducting circuits, *Nature (London)* **481**, 170 (2012).
 - [25] H. Levine, A. Keesling, G. Semeghini, A. Omran, T. T. Wang, S. Ebadi, H. Bernien, M. Greiner, V. Vuletić, H. Pichler, and M. D. Lukin, Parallel implementation of high-fidelity multiqubit gates with neutral atoms, *Phys. Rev. Lett.* **123**, 170503 (2019).
 - [26] M. Amy, A. N. Glaudell, S. M. Li, and N. J. Ross, Improved synthesis of Toffoli-Hadamard circuits, *arXiv:2305.11305*.
 - [27] P. Mukhopadhyay, Synthesizing Toffoli-optimal quantum circuits for arbitrary multi-qubit unitaries, *arXiv:2401.08950*.

- [28] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. (Cambridge University Press, Cambridge, UK 2010).
- [29] A. Glaudell, Quantum compiling methods for fault-tolerant gate sets of dimension greater than two, Ph.D. thesis, University of Maryland, College Park, 2019.
- [30] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, A new quantum ripple-carry addition circuit, [arXiv:quant-ph/0410184](#).
- [31] A. W. Harrow, B. Recht, and I. L. Chuang, Efficient discrete approximations of quantum gates, *J. Math. Phys.* **43**, 4445 (2002).