Catalytic z-rotations in constant T-depth

Isaac H. Kim

Department of Computer Science, University of California, Davis, CA, 95616, USA

We show that the T-depth of any single-qubit z-rotation can be reduced to 3 if a certain catalyst state is available. To achieve an ϵ-approximation, it suffices to have a catalyst state of size polynomial in $\log(1/\epsilon)$. This implies that $\mathsf{QNC}^0_f/\mathsf{qpoly}$ admits a finite universal gate set consisting of Clifford+T. In particular, there are catalytic constant T-depth circuits that approximate multi-qubit Toffoli, adder, and quantum Fourier transform arbitrarily well. We also show that the catalyst state can be prepared in time polynomial in $\log(1/\epsilon)$.

arXiv:2506.15147v3 [quant-ph] 5 Aug 2026

1 Introduction

A fundamental result in quantum computing is the Solovay-Kitaev theorem [1], which states that a finite set of universal gates can approximate the continuous gate set arbitrarily well, with an overhead that scales polylogarithmically with the inverse precision. While the Solovay-Kitaev theorem applies to any universal gate set, there are more efficient methods tailored to specific gate sets. A common example in the literature is Clifford+T, or alternatively, Clifford+Toffoli. Both gate sets can be realized in a fault-tolerant manner using a variety of methods, making them the standard gate set for fault-tolerant quantum computation.

For a long time, a common cost metric used for these gate sets has been the number of non-Clifford gates. This is because the cost of these gates turned out to be substantially more expensive than that of the Clifford gates; see Ref. [2] and the references therein. In particular, the T-count or Toffoli-count has been the primary metric to minimize. From this perspective, there are essentially optimal methods for approximating single-qubit z-rotations [3, 4, 5, 6]; they all possess the optimal $\mathcal{O}(\log(1/\epsilon))$ T-count (or equivalently, Toffoli-count), where ϵ is the approximation error.

However, if the goal is to minimize the computation time, one should instead optimize the T-depth. In the surface code-based approach to fault-tolerant quantum computation [7], there is a standard space-time tradeoff one can make [8, 9]. Keeping the overall space-time volume of the computation as a constant, it is possible to reduce time by using more space. Once the time overhead is reduced to the maximum extent possible, the computation time is essentially limited by the T-depth of the underlying circuit. Therefore, the T-depth of a circuit determines the minimal time needed to execute the circuit on a fault-tolerant quantum computer. Recent works also show that the cost of T-gates can be much cheaper than previously anticipated, suggesting that this metric may become practically relevant in the future [10, 11, 12, 13, 14]; see Ref. [15, 16] for the recent experiments.

Thus it is natural to ask what the achievable time overhead of single-qubit rotation is, quantified in terms of the T-depth. To that end, it is worth noting that the number of T-gates necessary to achieve ϵ-approximation is $\Omega(\log(1/\epsilon))$ [17]. While the existing methods [3, 4, 5, 6] match this lower bound, they are all sequential in nature. Is it possible

to parallelize them so that the T-depth can be brought down to a constant? This question was raised recently in Ref. [18].

The main purpose of this paper is to investigate this question and provide a partial but positive answer. Before we proceed further, let us make a few remarks to explain our main result clearly. For any Clifford+T circuit, one can apply all the T-gates in one step by preparing the associated magic states and carrying out the computation by gate teleportation [19]. However, gate teleportation requires an adaptive basis change depending on the measurement outcome, which cannot be parallelized in general. For this reason, we focus on circuits with constant T-depth without any adaptive basis change. We also note that there are several different versions of this problem one can consider, depending on the types of ancilla we use. The cheapest type of ancilla is the dirty ancilla. These are qubits in an unknown state, which must be returned to the original state after the computation. The second is a clean ancilla, which is initialized to a known simple state, such as $|0\dots0\rangle$. The third would be a *catalyst state* [20, 21, 17, 22]. This is a special state prepared offline before the computation, which is then used in the computation. These states are returned to the original state after the computation, and therefore can be reused later.

In this paper, we show that constant T-depth rotation is possible using an appropriate catalyst state, answering the third (and the weakest) version of the problem in the affirmative. Specifically, we show that for every $a \in [2^n - 1]$, there is a unitary U_a with the following properties. First, it applies a single-qubit z-rotation proportional to a:

$$U_a((\alpha|0\rangle + \beta|1\rangle)|\phi_a\rangle) = (\alpha|0\rangle + \beta e^{\frac{2\pi a i}{2^n-1}}|1\rangle)|\phi_a\rangle, \tag{1}$$

where $|\phi_a\rangle$ is a state over $\mathcal{O}(n)$ qubits. Second, U_a has T-depth of 3 and a Clifford depth of $\mathcal{O}(\log n)$. Third, $|\phi_a\rangle$ can be prepared in time polynomial in n. Therefore, the catalyst state $|\phi_a\rangle$ can be prepared with a modest cost, after which the rotation can be realized in constant T-depth. We also discuss a variant of this construction in which the rotation angle is not fixed to a constant. The T-depth remains the same for this variant, though we seem to need n copies of the same catalyst state.

Because single-qubit rotation is a widely used subroutine in quantum computing, our protocol can be used to lower the time overhead of a large class of quantum subroutines. One simple way to understand this consequence is in terms of the complexity class QNC^0_f [23, 24]. The circuits in this class are constant-depth quantum circuits assisted by unbounded fanout (which is a Clifford), using arbitrary one- and two-qubit gates. Because our result lets us simulate any one- and two-qubit gate in constant T-depth using a catalyst state, any circuit in QNC^0_f can be simulated by a constant T-depth circuit using a catalyst state. Interestingly, QNC^0_f includes a rich family of circuits. It includes unbounded fan-in, addition (which may or may not be modular), quantum Fourier transform, and even the quantum part of the factoring algorithm [23, 24]. Our result implies that these can all be done in constant T-depth, insofar as enough catalyst states are available.

The fact that unbounded fan-in and addition can be realized in constant T-depth (albeit with a catalyst) is somewhat counterintuitive. Because T-gates and Toffolis can be converted to each other up to a Clifford and a catalyst state, it follows that there are unbounded fan-in and adders that can be realized in constant Toffoli depth. This is in contrast to the classical case, in which the Toffoli depth of these circuits is known to be $\Omega(\log n)$ [25, 23]. Because Clifford gates cannot generate additional Toffolis, it seems somewhat surprising that they can help us reduce the Toffoli depth of these circuits.

So, what makes this counterintuitive result possible? A broad direction we take in our construction is to use a specialized form of in-place adder. To provide more context, let us recall the well-known method for implementing single-qubit rotation with an

adder [1, 26]. Let ADD_a be a unitary that implements $\mathsf{ADD}_a|x\rangle = |(x+a) \mod 2^n\rangle$. Because $|QFT\rangle := \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{\frac{-2\pi ij}{2^n}} |j\rangle$ is an eigenstate of ADD_a with an eigenvalue of $e^{\frac{2\pi ia}{2^n}}$, applying the phase kickback trick to ADD_a and $|QFT\rangle$, we can implement the single-qubit z-rotation with an angle of $\frac{2\pi a}{2^n}$. Because there is a logarithmic-depth in-place adder [26], the phase kickback unitary can be implemented in logarithmic depth. This observation lets us implement single-qubit z-rotation using $\mathcal{O}(\log(1/\epsilon))$ qubits in depth $\mathcal{O}(\log\log(1/\epsilon))$ [1, Theorem 13.5].

The main difficulty is that there is no known in-place reversible adder that can be implemented in constant depth, even if one deviates from the standard binary representation. For instance, there is a constant-depth adder using signed-digit representation [27], but it is unclear if this method can be made both reversible and in-place. A new idea seems necessary to break the $\mathcal{O}(\log\log(1/\epsilon))$ barrier.

The main idea that lets us overcome this barrier is to use special polynomials over $\mathbb{F}_2$, the *primitive polynomials* of $\mathrm{GF}(2^n)$. It turns out that there is a simple recurrence relation inherited from this polynomial which simultaneously satisfies a number of nice properties: (i) the recurrence relation has a period of 2^n-1, (ii) it has a Clifford implementation, and (iii) it has a constant-depth implementation. In effect, we have an n-qubit Clifford that has a period of 2^n-1 which can be implemented in constant depth. By preparing an eigenstate of this Clifford and applying phase kickback, we obtain the desired operation. The fact that this Clifford is constant-depth guarantees us that the phase kickback operation can be implemented in constant T-depth.

The rest of the paper is structured as follows. In Section 2, we explain our constant T-depth protocol for fixed single-qubit rotation. We provide a discussion and an outlook in Section 3.

2 Primitive Polynomial Method

Recall that $\mathrm{GF}(2^n) = \mathbb{F}_2[x]/\langle f(x)\rangle$, where $f(x)$ is a monic irreducible polynomial of degree n. The elements of $\mathrm{GF}(2^n)$ can be conveniently written in terms of the root of $f(x)$, say α.

$$\mathrm{GF}(2^n) = \left\{ \sum_{j=0}^{n-1} c_j \alpha^j : c_j \in \mathbb{F}_2 \right\}. \tag{2}$$

We say $f(x)$ is *primitive* if α generates the multiplicative subgroup of $\mathrm{GF}(2^n)$, consisting of the nonzero elements. Unless specified otherwise, we assume $f(x)$ is primitive throughout this paper.

Consider a recurrence relation $g_{n+1}(\alpha) = \alpha g_n(\alpha)$, where $g_n(\alpha) \in \mathrm{GF}(2^n)$. Because $f(x)$ is primitive, multiplication by α acts transitively on the set of nonzero elements. In particular, the period of the recurrence relation is 2^n-1.

This recurrence relation induces a linear transformation on the coefficients of $g_n(\alpha) = \sum_{j=0}^{n-1} g_n^j \alpha^j \in \mathrm{GF}(2^n)$. Without loss of generality, let $f(x) = x^n + \sum_{j=0}^{n-1} f_j x^j$. (Here $f_0 = 1$ since otherwise $f(x)$ is not irreducible.) The recurrence relation can be written as follows:

$$\begin{pmatrix} g_{n+1}^0 \\ g_{n+1}^1 \\ \vdots \\ g_{n+1}^{n-2} \\ g_{n+1}^{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & f_0 \\ 1 & 0 & \cdots & 0 & 0 & f_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & f_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & f_{n-1} \end{pmatrix} \begin{pmatrix} g_n^0 \\ g_n^1 \\ \vdots \\ g_n^{n-2} \\ g_n^{n-1} \end{pmatrix}. \tag{3}$$

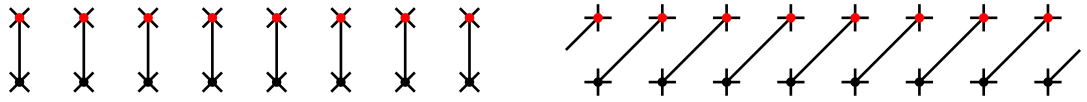

Figure 1: A depth-2 circuit consisting of SWAP gates for implementing S. The red dots are ancillary qubits. In the right figure, a periodic boundary condition in the x-direction is used.

We denote the $n \times n$ matrix as C_f, which is the *companion matrix* of $f(x)$. This matrix is invertible and its order is $2^n - 1$. Furthermore, it can be decomposed into a product of the cyclic permutation and an upper triangular matrix:

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & f_1 \\ 0 & 1 & \cdots & 0 & 0 & f_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & f_{n-1} \\ 0 & 0 & \cdots & 0 & 0 & f_0 \end{pmatrix} \tag{4}$$

To summarize, there are two different ways of representing elements of $\mathrm{GF}(2^n)$: (i) viewing them as a polynomial [Eq. (2)] and (ii) as a binary vector. In Section 2.1 and 2.2, we will take the second point of view. In Section 2.4, the first point of view will prove to be more useful.

2.1 Clifford Interpretation

Because C_f is a binary invertible matrix, we can define a Clifford unitary associated to it. Define U_f as

$$U_f|z\rangle = |C_f z\rangle, \tag{5}$$

where z is an n-dimensional binary vector. Thanks to Eq. (4), U_f can be decomposed into two simple Cliffords: (i) cyclic shift S and (ii) a CNOT gate (denoted as CX) with multiple targets. More specifically, let $Q_f = \{j : f_{j+1} = 1, j \neq 0\}$. The control and the targets of CX are $n-1$ and Q_f, respectively. Thus we denote the CX part of the circuit as $\mathsf{CX}_{n-1\to Q_f}$.

Let us discuss the decomposition of S and $\mathsf{CX}_{n-1\to Q_f}$ into one- and two-qubit Clifford gates. For S, a sequential $n-1$ application of SWAP suffices, which yields the depth of $n-1$. Intuitively, if we have n ancillary qubits prepared in an identical state, e.g., $|0\ldots0\rangle$, it is easy to see that a depth-2 circuit suffices; see Fig. 1. Less obvious is the fact that the same depth can be achieved without using any ancillas. Define $\mathsf{Rev}_{a,b}$ as a map that reverses the order of qubits $a, ..., b$. It is straightforward to verify that

$$\mathsf{S} = \mathsf{Rev}_{0,n-1} \cdot \mathsf{Rev}_{1,n-1}. \tag{6}$$

Since $\mathsf{Rev}_{a,b}$ is a depth-1 SWAP circuit, S can be realized by a depth-2 SWAP circuit. Moreover, the number of SWAPs is still $n-1$.

For $\mathsf{CX}_{n-1\to Q_f}$, the decomposition $\mathsf{CX}_{n-1\to Q_f} = \prod_{j\in Q_f} \mathsf{CX}_{n-1\to j}$ yields a depth-$|Q_f|$ circuit. Because the controls of the CX gates overlap, it is not possible to convert this into a constant-depth circuit. However, a constant-depth implementation is possible if unbounded fanout is available. Using unbounded fanout, we can apply the following transformation:

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\ldots0\rangle + \beta|1\ldots1\rangle \tag{7}$$

using $|Q_f|$ additional ancillary qubits. Then we can apply a depth-1 circuit comprised of CX from one of the qubits in this $|Q_f|$-qubit register to a qubit in Q_f. Applying the inverse of the fanout, we can implement $\mathsf{CX}_{n-1\to Q_f}$.

Because unbounded fanout is essentially a composition of CX gates [Fig. 2], one might wonder if there is anything to be gained from it. The answer turns out to be yes when we later aim to apply a controlled version of U_f. The key point is that the unbounded fanout can remain as Clifford, even when the other parts of the circuit are changed to non-Clifford gates. This is crucial to achieving constant T-depth; see Section 2.2 for more details.

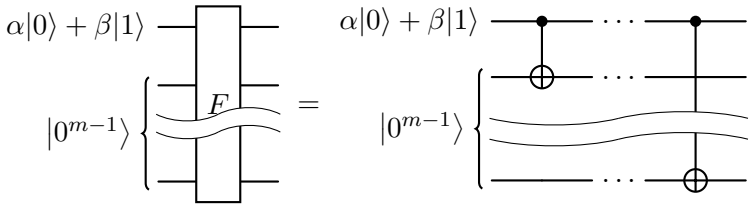

Figure 2: Fanout gate can be realized by a sequence of CX gates.

An important property of U_f is that its eigenvalues nearly uniformly cover the unit circle. Because C_f acts trivially on the zero element, $|0\dots0\rangle$ is an eigenvector of C_f with an eigenvalue of 1. The remaining eigenvectors are

$$|\psi_k\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{j=0}^{2^n-2} \tilde{\omega}^{-jk} |C_f^j v\rangle, \tag{8}$$

for $k \in [2^n-1]$, where $\tilde{\omega} = e^{\frac{2\pi i}{2^n-1}}$ and v is a distinguished nonzero binary vector, say $v = 1\dots0$. The eigenvalue associated to $|\psi_k\rangle$ is $\tilde{\omega}^k$.

2.2 Phase Kickback

Given a state $|\psi_k\rangle$, by applying the phase kickback to U_f, we can implement a z-rotation with an angle of $\frac{2\pi k}{2^n-1}$. If the goal is to apply this specific phase, then it suffices to have only $|\psi_k\rangle$. However, in many cases one would be interested in approximating an *arbitrary* rotation. For that, it suffices to have $|\psi_{2^t}\rangle$ for every $t \in [n]$. Selectively applying phase kickback to these states, one can implement any single-qubit z-rotation with an angle of $2m\pi/(2^n-1)$, where $m \in \mathbb{Z}$.

More generally, it suffices to have $|\psi_{a2^t}\rangle$, $t \in [n]$, for any fixed a that is coprime to 2^n-1. Selectively applying phase kickback to these states, we obtain a single-qubit z-rotation with an angle of $2ma\pi/(2^n-1)$, where $m \in \mathbb{Z}$. Since a is coprime to 2^n-1, for any $b \in [2^n-1]$, there is some m such that $ma = b \mod (2^n-1)$.

In fact, these phase kickbacks can be parallelized using unbounded fanout. After applying the unbounded fanout [Eq. (7)] to $n-1$ ancillary qubits, we can apply the n controlled U_fs in parallel, followed by the inverse of the unbounded fanout. The requisite size of the catalyst state for this method is n^2, and if we were to parallelize the phase kickbacks, we need $n-1$ additional ancillary qubits.

Now the remaining question is whether the controlled $U_f = \mathsf{S} \cdot \mathsf{CX}_{n-1\to Q_f}$ can be parallelized. To that end, we can again use unbounded fanout so that the control qubit is expanded to n qubits. The controlled S operation can be realized by replacing the individual SWAP with controlled SWAP, also known as the Fredkin gate. This yields a depth-2 circuit consisting of Fredkin gates; see Fig. 3 (top) for an example. (The same

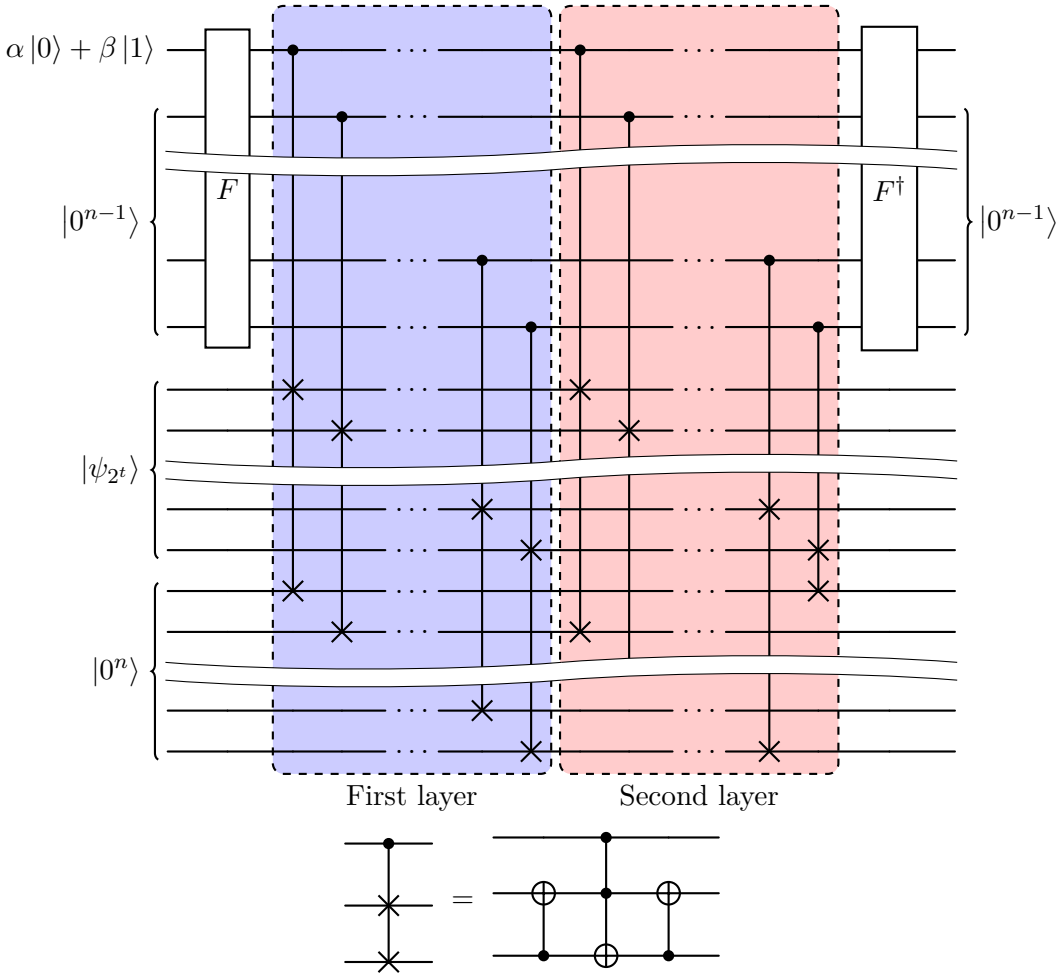

Figure 3: Top: Depth-2 implementation of controlled S. Bottom: Relation between controlled-SWAP and Toffoli.

approach can be applied to Eq. (6).) The Fredkin gate is equivalent to a Toffoli up to Clifford [Fig. 3, bottom], whose T-depth is 1 [28]. Therefore, the controlled S has a T-depth of 2. For $\mathsf{CX}_{n-1\to Q_f}$, the fanout can remain as is. We only need to change the CX gates to CCX, which is Toffoli. The circuit identity is shown in Fig. 4. Thus the T-depth of $\mathsf{CX}_{n-1\to Q_f}$ is 1. Altogether, the T-depth of the controlled U_f is 3.

We remark that the Clifford depth of our method is also modest. Note that the only nonlocal gate we used is unbounded fanout. It is well known that this can be realized in a logarithmic-depth circuit consisting of CX gates [29].

To summarize, insofar as $|\psi_{a2^t}\rangle$ is prepared offline for all $t \in [n]$ for some a coprime to $2^n - 1$, we can apply any rotation of $\frac{2\pi k}{2^n-1}$ for any $k \in [2^n - 1]$ using three layers of Toffoli and logarithmically many layers of CX gates. The number of qubits used is $3n^2$. In order to ensure m-bit precision, it suffices to choose $n = m + 1$.

2.3 Resource Estimate

In Section 2.2, we found that the T-depth (or equivalently, the Toffoli depth) of our method is 3. Here we quantify the number of non-Clifford gates used in our method and discuss a certain spacetime tradeoff we can make, depending on the number of non-Clifford gates one can apply in parallel. For this discussion, it will be convenient to phrase the result in terms

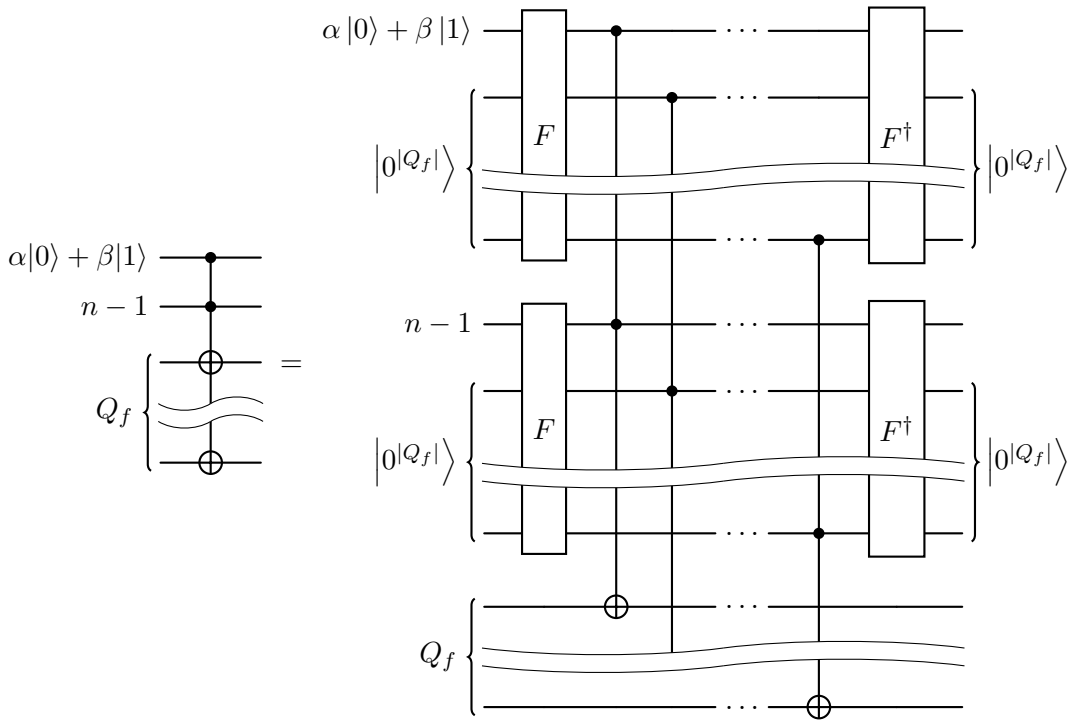

Figure 4: Using unbounded fanout, controlled $\mathsf{CX}_{n-1\to Q_f}$ can be implemented by a circuit with a Toffoli depth of 1.

of Toffoli gates. We also focus on the fixed-angle rotation for convenience. The resource estimate for the variable-angle rotation can be obtained by multiplying the non-Clifford gate count by a factor of n.

We also make what may seem at first like a strange assumption: that n is at most 660. The reason for making this assumption is the following. For any $n \leq 660$, a primitive polynomial that satisfies $|Q_f| = 4$ exists [30]. In fact, for many n, there are primitive polynomials with $|Q_f| = 2$ [31, 32]. Let us discuss a few instructive examples. In Ref. [33, Appendix F], the authors discuss two quantum computing applications that require precision of $\epsilon = 1.1\times10^{-8}$ (for quantum dynamics simulation) and $\epsilon = 1.6\times10^{-11}$ (for quantum chemistry simulation). This translates into using $n = 27$ and $n = 36$, respectively. The following primitive polynomials will be suitable for this purpose [30, 32]:

$$\begin{aligned} x^{27} + x^{20} + x^{13} + x^7 + 1 \quad & \text{for } n = 27, \\ x^{36} + x^{11} + 1 \quad & \text{for } n = 36. \end{aligned} \tag{9}$$

Thus, for every $n \leq 660$, the controlled version of $\mathsf{CX}_{n-1\to Q_f}$ uses at most 4 Toffolis. We note that practically we will almost never need $n > 660$, because that corresponds to an astronomically high precision of $< 4.78 \times 10^{-198}$.

As for the controlled version of S, we note that S can be implemented using $n-1$ SWAP gates in depth 2 [Eq. (6)]. Therefore, the controlled version of S uses at most $n-1$ Toffoli gates with a Toffoli depth of 2. Combining this with the controlled version of $\mathsf{CX}_{n-1\to Q_f}$, we arrive at a Toffoli count of at most $n+3$ (and sometimes $n+1$), Toffoli depth of 3, and $n-1$ additional ancillary qubits needed for fanout.

If we can apply at most $\kappa \geq 2$ Toffoli gates in parallel, it would make sense to only use $\kappa - 1$ additional ancillary qubits for the fanout. The overall Toffoli count would remain the same and the Toffoli depth would be $2\lceil\frac{n-1}{\kappa-1}\rceil + \lceil\frac{4}{\kappa}\rceil$. Therefore, as the number of

available non-Clifford gates increases, our method can be easily adapted to make it more time-efficient.

2.4 Efficient Preparation of the Catalyst State

Here we show that there is a polynomial-time quantum algorithm for preparing any $|\psi_k\rangle$. We actually describe two algorithms. The first algorithm is based on Shor's algorithm for the discrete logarithm problem [34]. The second algorithm is based on the Frobenius endomorphism. The first algorithm is conceptually simpler, but it is less efficient. The complexity of both algorithms is dominated by the number of multiplications in $\mathrm{GF}(2^n)$. The first algorithm uses $\mathcal{O}(n)$ multiplications whereas the second algorithm uses the multiplication just three times; if we consider the cost *per resource state*, the number of multiplications approaches one.

We remark that in both algorithms we use quantum phase estimation of U_f, which would yield an approximate eigenstate. In order to obtain an ϵ'-approximation of $|\psi_k\rangle$ for some randomly chosen k, we would incur a cost polynomial in $\log(1/\epsilon')$ and n; see Section 2.4.1. (Note ϵ' may be chosen to be different from the precision of the rotation angle, which we denoted as ϵ throughout this paper.)

In this section, it will be convenient to represent the elements of $\mathrm{GF}(2^n)$ as $\alpha^j, j \in [2^n - 1]$. Recall that we chose $f(x)$ to be primitive, so this covers all the nonzero elements. So we write down $C_f^j v$ as α^{j+j_0}. We set $j_0 = 0$ for convenience, after which $|\psi_k\rangle$ becomes

$$|\psi_k\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{j=0}^{2^n-2} \tilde{\omega}^{-jk} |\alpha^j\rangle. \tag{10}$$

2.4.1 Algorithm Based on Discrete Logarithm

Consider any nonzero binary vector, say $|10\ldots0\rangle$, and apply quantum phase estimation for U_f. Since this is a Clifford, $U_f^{2^t}$ is a Clifford for all t. Moreover, they can be obtained by squaring. Thus the quantum phase estimation up to a precision ϵ' can be performed in gate cost polynomial in $\log(1/\epsilon')$ and n. Indeed, this entails applying $O(\log 1/\epsilon')$ layers of controlled $U_f^{2^t}$, each of which has $O(n^2)$ complexity. Because the overlap of the initial state with any $|\psi_k\rangle$ is $\frac{1}{2^n-1}$, the post-measurement state will be an ϵ'-approximation of $|\psi_k\rangle$, where k is random.

Without loss of generality, suppose we obtained $|\psi_k\rangle$. We show that there is a polynomial-time algorithm that converts $|\psi_k\rangle$ to any other $|\psi_{k'}\rangle$. Note that

$$|\psi_{k'}\rangle = U_{k'-k}|\psi_k\rangle, \tag{11}$$

where U_m is defined as

$$U_m|\alpha^j\rangle = \tilde{\omega}^{-jm}|\alpha^j\rangle. \tag{12}$$

The unitary U_m can be realized in two steps. The first step is to infer j from α^j, and the second step is to apply the phase proportional to j. The second step can be approximated well by the standard phase gradient method [1]. So we focus on the first step, which is more nontrivial.

Inferring j from α^j is precisely the discrete logarithm problem. Famously, there is a polynomial-time quantum algorithm that can solve this problem [34]. Therefore, there is a polynomial-time algorithm that implements $|\alpha^j\rangle|0\rangle \mapsto |\alpha^j v\rangle|j\rangle$. Knowing j, one can apply the requisite phase of $\tilde{\omega}^{-jm}$. One can then uncompute j, by solving this discrete logarithm

problem again. This completes the implementation of U_m, which is clearly polynomial-time. The main bottleneck of the algorithm is the modular exponentiation, consisting of n modular multiplications.

2.4.2 Algorithm Based on Frobenius Endomorphism

Frobenius endomorphism is an endomorphism of $\mathrm{GF}(2^n)$ defined as $g(\alpha) \mapsto g(\alpha)^2$ for any $g(\alpha) \in GF(2^n)$. Because the field has characteristic 2, this operation is linear. Moreover, it is invertible because $g(\alpha)^{2^n} = 1$ for any $g \in GF(2^n)$. Thus this map is in fact an automorphism. Let U_F be a unitary that implements this automorphism:

$$U_F|\alpha^j\rangle = |\alpha^{2j}\rangle. \tag{13}$$

This is a Clifford because $g(\alpha) \mapsto g(\alpha)^2$ is linear.

Applying U_F to $|\psi_k\rangle$, we get

$$\begin{aligned} U_F|\psi_k\rangle &= \frac{1}{\sqrt{2^n-1}} \sum_{j=0}^{2^n-2} \tilde{\omega}^{-jk}|\alpha^{2j}\rangle \\ &= \frac{1}{\sqrt{2^n-1}} \sum_{j=0}^{2^n-2} \tilde{\omega}^{-jk\cdot 2^{-1}}|\alpha^{j}\rangle \\ &= |\psi_{k\cdot 2^{-1}}\rangle. \end{aligned} \tag{14}$$

where 2^{-1} is the inverse of 2 modulo 2^n-1. Applying the inverse of U_F on both sides, we get $U_F^\dagger|\psi_k\rangle = |\psi_{2k}\rangle$. By repeatedly applying $U_F^\dagger$ $t \in [n]$ times, we obtain a catalyst state $|\psi_{k\cdot 2^t}\rangle$. Because U_F is Clifford, no extra non-Clifford gate is needed for this conversion.

With Eq. (14) in mind, we can now describe the algorithm. Similar to the first step in Section 2.4.1, we begin by applying quantum phase estimation for U_f to some nonzero binary vector. The post-measurement state is $|\psi_k\rangle$, where k is uniformly random. We continue to the next step if k is coprime to 2^n-1. Otherwise, repeat until this condition is met. The probability of success is

$$\frac{\varphi(N)}{N} \geq \frac{1}{e^\gamma \log\log N + \frac{3}{\log\log N}}, \tag{15}$$

where $\varphi(N)$ is Euler's totient function, γ is Euler's constant, and $N = 2^n-1$ [35]. Thus on average we need to repeat this procedure at most $\mathcal{O}(\log n)$ times.

Next, we copy $|\psi_k\rangle$, following the approach of Cleve and Watrous [36]. They observed that with a modular subtraction (or instead, addition) one can efficiently "clone" a quantum Fourier state. An analogous thing to do here is to use modular division (or instead, multiplication). Define U_{mul} as

$$U_{\mathrm{mul}}(|\alpha^j\rangle|\alpha^{j'}\rangle) = |\alpha^j\rangle|\alpha^{j+j'}\rangle. \tag{16}$$

Note that

$$U_{\mathrm{mul}}(|\psi_0\rangle|\psi_k\rangle) = |\psi_{-k}\rangle|\psi_k\rangle. \tag{17}$$

(Note $|\psi_0\rangle$ can be prepared with probability of $1 - 1/(2^n-1)$ by preparing the uniform superposition state and applying phase estimation for U_f.) Applying the same procedure on $|\psi_{-k}\rangle$, we obtain a copy of $|\psi_k\rangle$. Finally, one can uncompute $|\psi_{-k}\rangle$. This takes a total of three multiplications. If we want to make m copies, we can reuse $|\psi_{-k}\rangle$ multiple times and then uncompute. The number of multiplications is then $m+2$.

Now, applying $(U_F^\dagger)^t$ to each copy, we can convert $|\psi_k\rangle$ to $|\psi_{k2^t}\rangle$. Since this conversion is purely Clifford, the dominant cost of the algorithm comes from the multiplication in $\mathrm{GF}(2^n)$. The cost of multiplication for each $|\psi_{k2^t}\rangle$ approaches one. This way, we obtain $|\psi_{k2^t}\rangle$, $t \in [n]$, where k is coprime to $2^n - 1$. This is enough to apply the phase kickback procedure described in Section 2.2.

3 Discussion

In this paper, we show that an arbitrary single-qubit rotation can be approximated arbitrarily well by a circuit whose T-depth is 3, using a catalyst state. We note that this leads to several nontrivial facts about quantum circuits. A good way to understand this implication is in terms of the complexity class QNC_f^0 [23, 24]. This is a class of quantum circuits consisting of constant-depth quantum circuits (with arbitrary one- and two-qubit gates), accompanied by unbounded fanout. Because every rotation can be replaced by a constant T-depth circuit and a catalyst state, we can conclude that any circuit in QNC_f^0 can be simulated by a constant T-depth circuit with the help of the catalyst states. These catalyst states can be viewed as quantum advice, whose size is at most polynomial in the input size [37]. Thus we conclude that $\mathsf{QNC}_f^0/\mathsf{qpoly}$ [38] admits a finite universal gate set, which is Clifford+T. Interestingly, QNC_f^0 includes many interesting circuits, such as OR (or equivalently, Toffoli), addition, quantum Fourier transform, and even the quantum part of the factoring algorithm [23]. Thus all these circuits can be implemented in constant T-depth, with the help of a catalyst state.

We leave the following questions for future work. First, note that for fixed rotation angle the size of the catalyst state and the T-count is $\mathcal{O}(\log(1/\epsilon))$. However, if the rotation angle is variable, these numbers change to $\mathcal{O}(\log^2(1/\epsilon))$. Can there be a constant T-depth catalytic circuit with $\mathcal{O}(\log(1/\epsilon))$ T-count? Secondly, we leave it as an open problem to show/disprove that constant T-depth rotation is possible using only clean/dirty ancillas. Thirdly, our work shows that many subroutines, e.g., multi-qubit Toffoli, addition, quantum Fourier transform can be implemented in constant T-depth with some catalyst state. However, plugging in our result directly to Ref. [23] will likely yield impractically large circuits. We leave it as an open problem to devise compact and efficient catalytic constant T-depth circuits for these subroutines. Lastly, we note that the circuits for multi-qubit Toffoli, addition, and quantum Fourier transform using our approach will be only approximately correct; the rotation angles used in Ref. [23] are not integer multiples of $2\pi/(2^n - 1)$. We leave it as an open problem to devise catalytic constant T-depth circuits that implement these operations exactly.

Note: After this preprint appeared, several improvements were made. Gidney pointed out that there is an alternative construction that uses T-depth of 2 [39]. Notably, this construction uses $\mathcal{O}(n)$-size catalyst state to implement arbitrary rotation. Gidney also pointed out that in the setup in which different Pauli rotations are applied in sequence, the amortized T-depth can approach 1. More recently, it was pointed out that using measurement-based uncomputation the T-depth can be lowered to 1, without amortization [40].

Author contribution statement: ChatGPT model O3 was used for literature search, for finding invertible boolean functions that have large periods.

Acknowledgements

I thank Michael Beverland, Earl Campbell, ChatGPT (OpenAI, model O3), Craig Gidney, Daniel Litinski, Vadym Kliuchnikov, Tuomas Laakkonen, Natalie Parham, and Henry Yuen for helpful discussions. I thank Aram Harrow for pointing out Theorem 13.5 in Ref. [1]. The figures in this paper are drawn using Quantikz [41].

References

[1] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. "Classical and quantum computation". Number 47 in Graduate Studies in Mathematics. American Mathematical Soc. (2002).

[2] Daniel Litinski. "Magic state distillation: Not as costly as you think". Quantum **3**, 205 (2019).

[3] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. "Asymptotically optimal approximation of single qubit unitaries by clifford and t circuits using a constant number of ancillary qubits". Physical review letters **110**, 190502 (2013).

[4] Neil J. Ross and Peter Selinger. "Optimal ancilla-free clifford+t approximation of z-rotations" (2016). arXiv:1403.2975.

[5] Alex Bocharov, Martin Roetteler, and Krysta M Svore. "Efficient synthesis of universal repeat-until-success quantum circuits". Physical review letters **114**, 080502 (2015).

[6] Vadym Kliuchnikov, Kristin Lauter, Romy Minko, Adam Paetznick, and Christophe Petit. "Shorter quantum circuits via single-qubit gate approximation". Quantum **7**, 1208 (2023).

[7] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. "Surface codes: Towards practical large-scale quantum computation". Phys. Rev. A **86**, 032324 (2012).

[8] Austin G. Fowler. "Time-optimal quantum computation" (2013). arXiv:1210.4626.

[9] Daniel Litinski. "A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery". Quantum **3**, 128 (2019).

[10] Hayato Goto. "Minimizing resource overheads for fault-tolerant preparation of encoded states of the steane code". Scientific reports **6**, 19578 (2016).

[11] Christopher Chamberland and Kyungjoo Noh. "Very low overhead fault-tolerant magic state preparation using redundant ancilla encoding and flag qubits". npj Quantum Information **6**, 91 (2020).

[12] Tomohiro Itogawa, Yugo Takada, Yutaka Hirano, and Keisuke Fujii. "Even more efficient magic state distillation by zero-level distillation" (2024). arXiv:2403.03991.

[13] Craig Gidney, Noah Shutty, and Cody Jones. "Magic state cultivation: growing t states as cheap as cnot gates" (2024). arXiv:2409.17595.

[14] Lucas Daguerre and Isaac H. Kim. "Code switching revisited: Low-overhead magic state preparation using color codes". Phys. Rev. Res. **7**, 023080 (2025).

[15] Lucas Daguerre, Robin Blume-Kohout, Natalie C. Brown, David Hayes, and Isaac H. Kim. "Experimental demonstration of high-fidelity logical magic states from code switching". Phys. Rev. X **15**, 041008 (2025).

[16] Shival Dasu, Simon Burton, Karl Mayer, David Amaro, Justin A. Gerber, Kevin Gilmore, Dan Gresh, Davide DelVento, Andrew C. Potter, and David Hayes. "Breaking even with magic: demonstration of a high-fidelity logical non-clifford gate" (2025). arXiv:2506.14688.

[17] Michael Beverland, Earl Campbell, Mark Howard, and Vadym Kliuchnikov. "Lower bounds on the non-clifford resources for quantum computations". Quantum Science and Technology **5**, 035009 (2020).

[18] Natalie Parham. "Quantum circuit lower bounds in the magic hierarchy" (2025). arXiv:2504.19966.

[19] Daniel Gottesman and Isaac L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". Nature **402**, 390–393 (1999).

[20] Earl T. Campbell. "Catalysis and activation of magic states in fault-tolerant architectures". Phys. Rev. A **83**, 032317 (2011).

[21] Craig Gidney and Austin G. Fowler. "Efficient magic state factories with a catalyzed $|CCZ\rangle$ to $2|T\rangle$ transformation". Quantum **3**, 135 (2019).

[22] M. Amy, M. Crawford, A. N. Glaudell, M. L. Macasieb, S. S. Mendelson, and N. J. Ross. "Catalytic embeddings of quantum circuits" (2023). arXiv:2305.07720.

[23] Peter Høyer and Robert Špalek. "Quantum fan-out is powerful". Theory of computing **1**, 81–103 (2005).

[24] Yasuhiro Takahashi and Seiichiro Tani. "Collapse of the hierarchy of constant-depth exact quantum circuits". computational complexity **25**, 849–881 (2016).

[25] Richard Beigel. "The polynomial method in circuit complexity". In [1993] Proceedings of the Eighth Annual Structure in Complexity Theory Conference. Pages 82–95. IEEE (1993).

[26] Craig Gidney. "Halving the cost of quantum addition". Quantum **2**, 74 (2018).

[27] Algirdas Avizienis. "Signed-digit number representations for fast parallel arithmetic". IRE Transactions on electronic computers **EC-10**, 389–400 (1961).

[28] Peter Selinger. "Quantum circuits of t-depth one". Phys. Rev. A **87**, 042302 (2013).

[29] Cristopher Moore and Martin Nilsson. "Parallel quantum computation and quantum codes". SIAM journal on computing **31**, 799–815 (2001).

[30] Janusz Rajski and Jerzy Tyszer. "Primitive polynomials over gf (2) of degree up to 660 with uniformly distributed coefficients". Journal of Electronic testing **19**, 645–657 (2003).

[31] Richard P Brent and Paul Zimmermann. "The great trinomial hunt". Notices of the AMS **58**, 233–239 (2011). url: https://www.ams.org/notices/201102/rtx110200233p.pdf.

[32] Joerg Arndt. "Complete list of primitive trinomials over GF(2) up to degree 400". https://www.jjj.de/mathdata/all-trinomial-primpoly.txt (2003). Text file generated 2003-01-16.

[33] Michael E. Beverland, Prakash Murali, Matthias Troyer, Krysta M. Svore, Torsten Hoefler, Vadym Kliuchnikov, Guang Hao Low, Mathias Soeken, Aarthi Sundaram, and Alexander Vaschillo. "Assessing requirements to scale to practical quantum advantage" (2022). arXiv:2211.07629.

[34] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In Proceedings 35th annual symposium on foundations of computer science. Pages 124–134. Ieee (1994).

[35] J Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". Illinois Journal of Mathematics **6**, 64–94 (1962).

[36] Richard Cleve and John Watrous. "Fast parallel circuits for the quantum fourier transform". In Proceedings 41st Annual Symposium on Foundations of Computer Science. Pages 526–536. IEEE (2000).

[37] Harumichi Nishimura and Tomoyuki Yamakami. "Polynomial time quantum computation with advice". Information Processing Letters **90**, 195–204 (2004).

[38] Adam Bene Watts, Robin Kothari, Luke Schaeffer, and Avishay Tal. "Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits". In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. Pages 515–526. (2019).

[39] Craig Gidney. "Post on x (twitter)". https://x.com/CraigGidney/status/1936285631359197210. Accessed: 2026-02-12.

[40] Isaac H. Kim and Tuomas Laakkonen. "Any clifford+t circuit can be controlled with constant t-depth overhead" (2025). arXiv:2512.24982.

[41] Alastair Kay. "Tutorial on the quantikz package" (2023). arXiv:1809.03842.