Quantum circuits of T-depth one

Peter Selinger

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, Canada B3H 4R2

(Received 3 October 2012; published 1 April 2013)

We give a Clifford + T representation of the Toffoli gate of T-depth one, using four ancillas. More generally, we describe a class of circuits whose T-depth can be reduced to one by using sufficiently many ancillas. We show that the cost of adding an additional control to any controlled gate is at most eight additional T gates and T-depth two. We also show that the circuit THT does not possess a T-depth one representation with an arbitrary number of ancillas initialized to $|0\rangle$.

DOI: 10.1103/PhysRevA.87.042302 PACS number(s): 03.67.Lx

I. INTRODUCTION

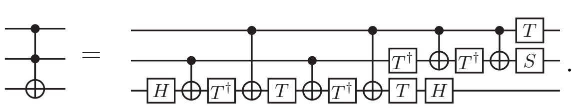
It is known that the gates of the Clifford group, together with the single-qubit non-Clifford gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix},$$

form a good universal gate set for fault-tolerant quantum computation [1]. The decomposition of arbitrary gates into this Clifford + T set, either exactly or to within some given accuracy ϵ, is an important problem [2]. It is often desirable to find decompositions that are optimal with respect to a given cost function. The exact cost function used is application dependent; some possibilities are the total number of gates, the total number of T gates, the circuit depth, and/or the number of ancillas used.

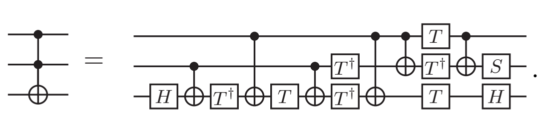
Amy *et al.* [3] recently proposed T-*depth* as a cost function. The idea is to count the number of T *stages* in a circuit, rather than the number of T gates. A T stage is a group of one or more T and/or $T^\dagger$ gates on distinct qubits that can be performed simultaneously. Note that, for the purpose of computing T-count or T-depth, the gates T and $T^\dagger$ can be treated interchangeably, due to the identity $T^\dagger = TS^\dagger$.

To illustrate the concept of T-depth, consider the standard decomposition of the Toffoli gate into the Clifford + T set, as given in Ref. [4]:



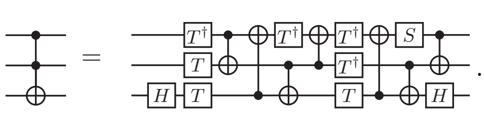
(1)

This decomposition has T-count seven, and in the exact form written, it has T-depth six, because the fourth and fifth T gates form a single T stage. Using trivial commutations, the circuit (1) can easily be reduced to T-depth four:



(2)

Amy *et al.* [3] further improved the T-depth of the Toffoli gate to three, using the following circuit. They conjecture that for circuits without ancillas, this T-depth is optimal:



(3)

The purpose of this paper is to show that, with the use of ancillas, the T-depth of the Toffoli gate, and of many (but not all) other circuits, can be reduced to one. This may be useful in quantum computing architectures where T gates are expensive and ancillas are cheap.

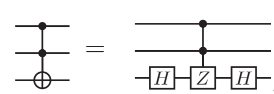
II. A T-DEPTH ONE REPRESENTATION OF THE TOFFOLI GATE

Recall that the Clifford group for any number of qubits is generated by the Hadamard gate H, the phase gate $S = T^2$, the controlled-NOT gate, and unit scalars. As usual, we write X, Y, and Z for the Pauli operators:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Toffoli gate is a doubly controlled NOT gate. It is equivalent to a doubly controlled Z gate via a basis change:



(4)

Now consider a computational basis state $|xyz\rangle$, where $x,y,z \in \{0,1\}$. The effect of the doubly controlled Z gate is to map $|xyz\rangle$ to $(-1)^{xyz}|xyz\rangle$. Let us write "$\oplus$" for modulo-2 addition in $\{0,1\}$, and "$+$" and "$-$" for the usual addition and subtraction of integers. We then have the following inclusion-exclusion style formula for $x,y,z \in \{0,1\}$:

$$\begin{aligned} 4xyz = x + y + z - (x \oplus y) - (y \oplus z) \\ - (x \oplus z) + (x \oplus y \oplus z). \end{aligned} \tag{5}$$

This is easy to prove by case distinction, or algebraically using $x \oplus y = x + y - 2xy$. Now let $\omega = (-1)^{1/4} = e^{i\pi/4}$. From (5), we have

$$(-1)^{xyz} = \omega^{4xyz} = \omega^x \omega^y \omega^z (\omega^\dagger)^{x\oplus y} (\omega^\dagger)^{y\oplus z} (\omega^\dagger)^{x\oplus z} \omega^{x\oplus y\oplus z}. \tag{6}$$

Note that $T|x\rangle = \omega^x|x\rangle$, and therefore, the doubly controlled Z gate can be implemented by applying T gates to qubits in states $|x\rangle$, $|y\rangle$, $|z\rangle$, and $|x \oplus y \oplus z\rangle$, and $T^\dagger$ gates to qubits in states $|x \oplus y\rangle$, $|y \oplus z\rangle$, and $|x \oplus z\rangle$. This can be done in any order, or even in parallel, using four ancillas, as shown in

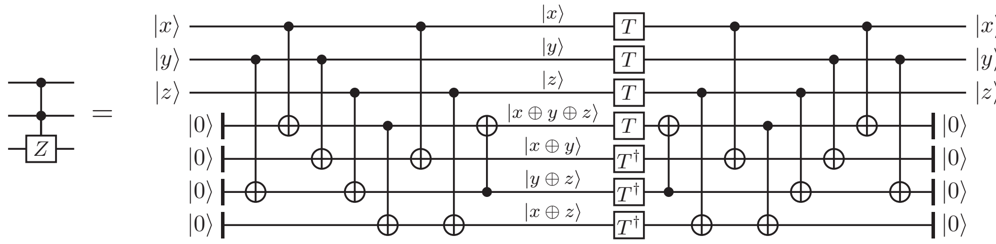


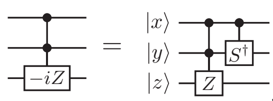
FIG. 1. T-depth one representation of the Toffoli gate.

Fig. 1. Combining this with Eq. (4), we obtain a representation of the Toffoli gate of T-depth one and overall depth seven.

Remark 2.1. It is interesting to note that the decompositions of Nielsen and Chuang (1) and Amy *et al.* (3) follow precisely the same pattern; i.e., they can both be seen to be direct implementations of Eq. (6). The only difference is that in each of the circuits, one of the T gates has been needlessly decomposed into $T^\dagger$ and S.

III. AN APPLICATION TO MULTIPLY CONTROLLED GATES

Consider a doubly controlled $(-iZ)$ gate:

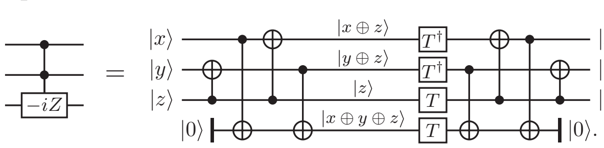


(7)

The doubly controlled Z gate is a diagonal gate whose effect is given by Eq. (6). The controlled-$S^\dagger$ gate is a diagonal gate whose effect is given by $(-i)^{xy} = (\omega^\dagger)^x(\omega^\dagger)^y\omega^{x\oplus y}$. It follows that the combined effect of the two gates is

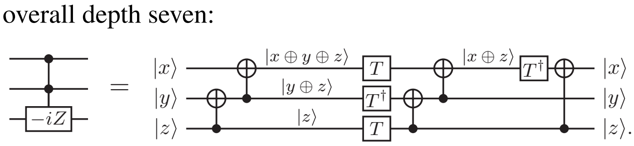
$$(-1)^{xyz}(-i)^{xy} = \omega^z(\omega^\dagger)^{y\oplus z}(\omega^\dagger)^{x\oplus z}\omega^{x\oplus y\oplus z}, \tag{8}$$

which therefore requires a T-count of only four. Using one ancilla, this can be achieved with T-depth one and overall depth five:



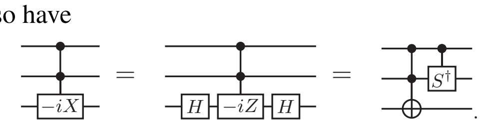
(9)

Alternatively, one can find an implementation that uses no ancilla. It uses fewer overall gates, but has T-depth two and overall depth seven:



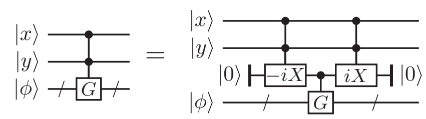
(10)

We also have



(11)

Suppose we have a Clifford + T representation of some controlled quantum gate G, and we wish to obtain an efficient Clifford + T representation of a doubly controlled G gate. Using (9), (11), and (12), the cost of doing so is at most eight additional T gates, increasing the T-depth by at most 2, and the overall depth by at most 14, using two ancillas:

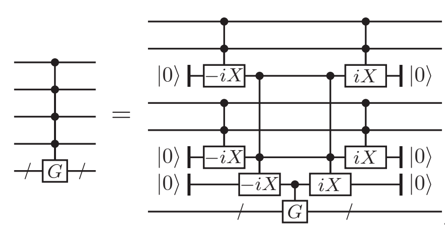


(12)

Note that the cost of the additional control, in terms of the overall gate count, is 28 [2 times 12 gates from Eq. (9) and 2 times 2 Hadamard gates from Eq. (11)]. This can be reduced to 26 by leaving the ancilla in Eq. (9) in state $|x\rangle$ instead of $|0\rangle$; however, doing so requires carrying this ancilla during the computation of G, which may involve a tradeoff.

If (10) is used instead of Eq. (9), the overall gate count cost of Eq. (12) decreases to 22, and the ancilla use to one. However, the depth and T-depth cost increase to 18 and 4, respectively.

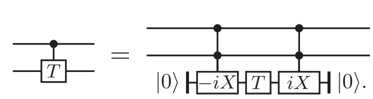
Remark 3.1. The above construction can be iterated to add n additional controls to a controlled gate at the cost of T-count $8n$ and T-depth $2\lfloor\log_2 n + 1\rfloor$. The logarithm in the expression for T-depth arises because a pair of T stages is sufficient to *double* the number of controls, as shown here for $n = 3$:



(13)

For example, this yields an implementation of a triply controlled NOT gate with T-count 15 and T-depth three (7 T gates for the Toffoli gate, and 8 T gates for the additional control); or a quintuply controlled NOT gate with T-count 31 and T-depth five. It is not currently known whether any of these T-counts or depths are optimal.

Remark 3.2. Because the T gate is diagonal with $T|0\rangle = |0\rangle$, it can be regarded as a controlled gate, namely, a controlled global phase change. Therefore, we can use the above procedure to implement a controlled-T gate with T-count nine as follows:



(14)

Using (9), we obtain T-depth 3, depth 15, and gate count 29 with two ancillas. As before, by leaving the ancilla of Eq. (9) in state $|x\rangle$ instead of state $|0\rangle$, the gate count can be reduced to 27. Alternatively, using (10), we obtain T-depth 5, depth 19, and gate count 27 with one ancilla. Except for slightly improved overall gate counts, these results are the same as those in Ref. [3].

IV. T-DEPTH ONE REPRESENTATION OF ALMOST CLASSICAL CIRCUITS

It is straightforward to generalize the construction of Sec. II to circuits built up from T and *almost classical* gates.

Definition 4.1. A unitary operator is *classical* if it is given by a permutation of computational basis states and *diagonal* if its matrix representation is diagonal in the computational basis. Let us call an operator *almost classical* if it can be written as a product of a classical operator and a diagonal operator.

The almost classical operators obviously form a group. Of the 24 single-qubit Clifford operators (taken modulo global phase), exactly 8 are almost classical; they form the subgroup generated by S and X.

Definition 4.2. Let $\mathcal{C}$ be a set of gates. We say that a circuit is *$\mathcal{C}+T$-representable* if it can be built with gates from $\mathcal{C}\cup\{T\}$ and their inverses. We say that such a circuit has *T-depth n* (*relative to $\mathcal{C}$*) if it can be written using only gates from $\mathcal{C}$ and n T stages.

Theorem 4.1. Let $\mathcal{C}$ be any set of almost classical gates, containing the controlled-NOT gate. Using ancillas, any $\mathcal{C}+T$-representable n-qubit circuit can be written of T-depth one (relative to $\mathcal{C}$).

Proof. The proof idea is simple. Each T gate in the circuit is a $\pi/4$ phase change conditioned on some Boolean combination of the inputs. Intuitively, one may copy each such Boolean condition to an ancilla, execute all T gates in parallel, uncompute the ancillas, and finally recompute the output.

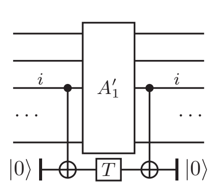
The formal proof proceeds by induction on circuits. For each $\mathcal{C}+T$-representable n-qubit circuit A, we use induction to construct $\mathcal{C}+T$-representable circuits A_1 and A_2 such that A_1 is diagonal and has T-depth at most one, A_2 has T-depth 0, and $A = A_2 \circ A_1$.

The base case occurs when $A = I$ is the identity circuit. In this case, we can let $A_1 = A_2 = I$, and there is nothing to show.

For the induction step, suppose A is of the form $A' \circ G$, where G is a single gate. By induction hypothesis, there is a decomposition $A' = A_2' \circ A_1'$ satisfying the above conditions.

(i) Case 1: G is not equal to T or $T^\dagger$. In this case, we let $A_1 = G^\dagger \circ A_1' \circ G$ and $A_2 = A_2' \circ G$. Then trivially, $A = A_2 \circ A_1$, and A_1 and A_2 have the required T-depths. Moreover, since G is almost classical, A_1 is diagonal.

(ii) Case 2: G is T, applied to the ith qubit. In this case, we let

$A_1 =$  (15)

and $A_2 = A_2'$. Since A_1' is diagonal, so is A_1, and it follows that the ancilla is uncomputed correctly. Moreover, A_1 is equivalent to $A_1' \circ G$, and therefore, $A = A_2 \circ A_1$. Finally, since A_1' has T-depth of at most one, so does A_1.

(iii) Case 3: G is $T^\dagger$, applied to the ith qubit. This is entirely analogous to case 2. ■

A similar result appears in Sec. 6.4 of version 2 of Ref. [3], but with a proof that is quite different.

Note that the gate set $\mathcal{C}$ in Theorem 4.1 is not necessarily assumed to consist of Clifford gates. For example, if on some hypothetical architecture, T gates are expensive but Toffoli gates are cheap, one can include the Toffoli gate in the set $\mathcal{C}$.

In general, the proof of Theorem 4.1 increases the size of the circuit, but only by a constant factor. In practice, it is often possible to find a much smaller circuit than the one constructed in the proof.

If we take $\mathcal{C} = \{S, X, \text{CNOT}\}$ and apply Theorem 4.1 to circuit (1) (excluding the initial and final Hadamard gate), we obtain another T-depth one representation of the Toffoli gate.

We also note that there is a trade-off between T-depth and the number of ancillas. The procedure of the proof of Theorem 4.1 adds one ancilla for each T gate. However, by splitting a circuit with T-count n into two circuits with T-count $\lceil n/2 \rceil$ each, it is clear that one can approximately half the number of ancillas by doubling the T-depth and so forth.

V. SOME CIRCUITS CANNOT BE WRITTEN WITH T-DEPTH ONE

The result of the previous section shows that any two T stages can be combined into a single T stage, provided that they are only separated by almost classical gates. One may wonder whether perhaps *all* Clifford + T circuits can be written of T-depth one, using a sufficient number of ancillas initialized to $|0\rangle$. We show that this cannot be done.

Theorem 5.1. The single-qubit operator THT cannot be implemented as a Clifford + T circuit of T-depth one, using an arbitrary number of ancillas initialized to $|0\rangle$. This is true even if the ancillas are not required to be returned to their initial state at the end of the computation.

Before proving the theorem, we start with a general observation about Clifford + T circuits of T-depth one.

Proposition 5.1. Let U be an n-qubit Clifford + T circuit of T-depth one. Let $|\phi\rangle$ be any single-qubit state, and consider

$$|\psi\rangle = U(|\phi\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle).$$

Consider the $\{+1,-1\}$-valued Pauli observable X applied to the first qubit of ψ; denote its expected value by $E_{|\phi\rangle}$. Suppose $E_{|+\rangle}$ is nonzero. Then

$$\frac{E_{|0\rangle}}{E_{|+\rangle}}$$

is a rational number.

Proof. The expected value of the observable X on the first qubit of $|\psi\rangle$ is

$$\begin{aligned} E_{|\phi\rangle} &= \langle\psi|\,(X \otimes I \otimes \cdots \otimes I)\,|\psi\rangle \\ &= \langle\phi,0,\ldots,0|\;U^\dagger(X \otimes I \otimes \cdots \otimes I)U\;|\phi,0,\ldots,0\rangle. \end{aligned} \tag{16}$$

We analyze the structure of $U^\dagger(X \otimes I \otimes \cdots \otimes I)U$. Since U is of T-depth one, it can be written as $U = U_1 \circ U_2 \circ U_3$, where U_1 and U_3 are Clifford circuits and $U_2 = T \otimes \cdots \otimes T \otimes I \otimes \cdots \otimes I$. Since U_1 is Clifford, we know that $U_1^\dagger(X \otimes I \otimes \cdots \otimes I)U_1$ is a Pauli operator

$$U_1^\dagger(X \otimes I \otimes \cdots \otimes I)U_1 = \pm A_1 \otimes \cdots \otimes A_n, \tag{17}$$

where each $A_i \in \{X,Y,Z,I\}$. Using the relations

$$T^\dagger I T = I, \quad T^\dagger Z T = Z,$$
$$T^\dagger X T = \frac{1}{\sqrt{2}}X - \frac{1}{\sqrt{2}}Y, \quad T^\dagger Y T = \frac{1}{\sqrt{2}}X + \frac{1}{\sqrt{2}}Y,$$

we find that

$$\begin{aligned} U_2^\dagger(\pm A_1 \otimes \cdots \otimes A_n)U_2 &\\ = \pm(T^\dagger A_1 T) \otimes \cdots \otimes \left(T^\dagger A_{n_1} T\right) \otimes A_{n_1+1} \otimes \cdots \otimes A_n &\\ = \lambda P_1 + \lambda P_2 + \cdots + \lambda P_m, & \end{aligned} \tag{18}$$

where each P_j is an n-qubit Pauli operator. The key observation here is that the *same* factor λ occurs in front of each (possibly signed) summand, and λ is independent of $|\phi\rangle$. In fact, we have $\lambda = (\frac{1}{\sqrt{2}})^k$, where k is the number of times the operators X and Y occur among $A_1, \ldots, A_{n_1}$. Let

$$Q_j = U_3^\dagger \; P_j \; U_3. \tag{19}$$

Since U_3 is Clifford, this is again some Pauli operator, say

$$Q_j = (-1)^{q_j} B_{j,1} \otimes \cdots \otimes B_{j,n}. \tag{20}$$

Combining (17) through (20), we find

$$\begin{aligned} U^\dagger(X \otimes I \otimes \cdots \otimes I)U &= \lambda Q_1 + \lambda Q_2 + \cdots + \lambda Q_m \\ &= \lambda \sum_{j=1}^{m} (-1)^{q_j} B_{j,1} \otimes \cdots \otimes B_{j,n}. \end{aligned} \tag{21}$$

Combining this with Eq. (16), we get

$$E_{|\phi\rangle} = \lambda \sum_{j=1}^{m} (-1)^{q_j} \langle\phi|B_{j,1}|\phi\rangle \; \langle 0|B_{j,2}|0\rangle \cdots \langle 0|B_{j,n}|0\rangle. \tag{22}$$

Since each $B_{j,i} \in \{X,Y,Z,I\}$ is a Pauli operator, it follows that $E_{|\phi\rangle}/\lambda$ is rational (indeed, an integer) for $|\phi\rangle \in \{|0\rangle,|+\rangle\}$. The claim then immediately follows. ■

Proof of Theorem 5.1. For $U = THT$, we compute

$$U^\dagger X U = \frac{1}{2}X + \frac{1}{2}Y + \frac{1}{\sqrt{2}}Z,$$

and therefore

$$E_{|0\rangle} = \langle 0|U^\dagger X U|0\rangle = \frac{1}{\sqrt{2}}$$

and

$$E_{|+\rangle} = \langle +|U^\dagger X U|+\rangle = \tfrac{1}{2}.$$

Since $E_{|0\rangle}/E_{|+\rangle}$ is irrational, the claim immediately follows from Proposition 5.1. ■

VI. CONCLUSION

We found a class of circuits whose T-depth can be reduced to one, by using a sufficient number of ancillas. We also showed that there are circuits whose T-depth cannot be reduced to one, regardless of the number of ancillas used. It remains an open problem how to determine the minimal T-depth or T-count of any given Clifford + T circuit.

ACKNOWLEDGMENTS

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). This research was also supported by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract No. D11PC20168 The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the US Government.

[1] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger, in *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)* (IEEE Computer Society, Los Alamitos, CA, 2006), pp. 411–419.

[2] V. Kliuchnikov, D. Maslov, and M. Mosca, Quantum Inf. Comput. (to appear), arXiv:1206.5236.

[3] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, arXiv:1206.0758.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2002).