Reducing the T-count of quantum C^n-NOT gates

Andrew Allen

Department of Mathematics and Statistics, Dalhousie University

August 2023

1 Introduction

The Clifford + T gate set can used to logically implement any quantum gate, either exactly or to an arbitrary degree of accuracy. The physical implementation of the T gate represents a significant resource cost compared to those of the Cliffords, particularly in the context of fault-tolerant computing. Therefore, it is of interest to minimize the *T-count*, defined as the number of T gates used in the implementation of a particular gate or family of gates. If one is concerned with time costs in particular, then they may instead consider the *T-count*, defined as the number of T gates *up to parallelization*. I focused on the T-count for my research.

An important gate family is the C^n-NOT gates. The effect of one of these gates is to flip the target qubit from $|0\rangle$ to $|1\rangle$ (or vice versa) if all n control bits are in the $|1\rangle$ state. Figure 1 depicts a generalized version for n qubits. C^n-NOT gates have analogues in reversible classical computing, so they are used to implement reversible classical functions in the quantum context. Thus, it is useful to reduce the T-count for these gates.

This was the goal of my project. In particular, I focused on what optimizations could be made by using measurements. I focus on measurement because it has allowed for notable constructions of the C^n-NOT family within the past decade — specifically, a Toffoli construction with T-count 4, which extends to a C^n-NOT construction with T-count $4n-4$; and a C^3-NOT construction with T-count 6, which further reduces the C^n-NOT T-count to

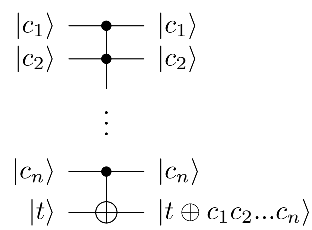


Figure 1: A C^n-NOT gate. The product $c_1c_2...c_n$ is added to the target qubit state, modulo 2. Gates of this type are used to implement classical reversible functions in the quantum context.

$4n-6$. I have studied these circuits to gain insight as to how they work, based on which I have attempted to find further reductions. This report details what I have learned while doing so.

2 Reducing T-count of the Toffoli from 7 to 4

We first consider advancements that brought the T-count for the Toffoli from 7 to 4. In 2012, Selinger [10] published a doubly-controlled $-iX$ circuit that uses 4 T gates (Fig. 2). This circuit achieves the effect of a Toffoli, except it also contributes a global phase of -i if the target qubit is flipped. Jones' circuit (Fig. 3) [7] realizes a true Toffoli by using Selinger's gate to target an ancilla, correcting the phase with an S gate, then copying the c_1c_2 product to the target input qubit. The an-

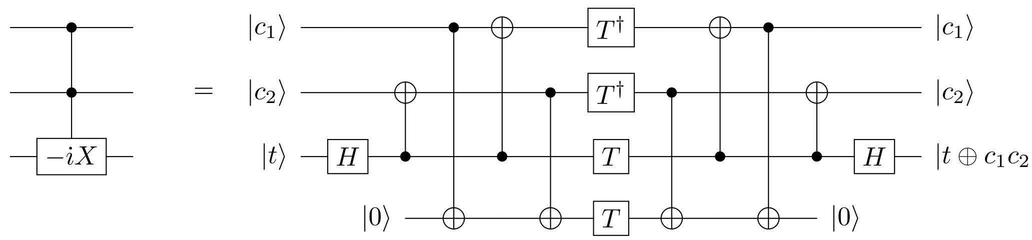


Figure 2: Selinger's [10] doubly-controlled $-i$X gate, implemented with 4 T gates. This gate achieves the effect of a Toffoli and contributes a global phase of i to the target qubit if both controls are $|1\rangle$.

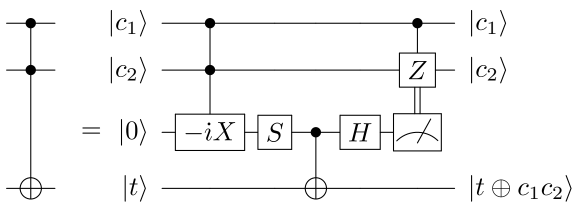


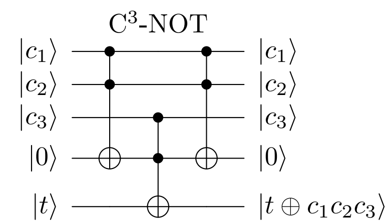
Figure 3: Jones' [7] Toffoli circuit, implemented with 4 T gates. It works by 1.) targeting an ancilla with a doubly-controlled $-i$X gate, then correcting the i phase with an S gate; 2.) XORing the c_1c_2 product onto the target qubit with a CNOT; then 3.) uncomputing the ancilla with a Hadamard and measurement-controlled CZ gate.

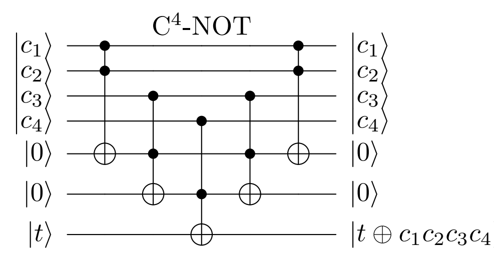
cilla is then uncomputed by a Hadamard followed by a measurement-controlled CZ gate on the control qubits. By measuring the ancilla, the uncomputation step achieves the effect of a second Toffoli without contributing to the circuit's T-count. This can be seen by deferring the measurement past the control and introducing a second Hadamard just before measurement.

The combination of Selinger and Jones' contributions allows the implementation of the Toffoli with only 4 T gates. This count is minimal as shown by Jiang and Wang [6], who used the stabilizer extent monotone to establish a lower bound on the T-count for CCZ—and by extension, the Toffoli (I round up from their value of 3.6349 to the nearest whole number). Before Jones' circuit, the prior upper bound for the Toffoli T-count was 7. Interestingly, Gosset et al. [5] showed that this count is minimal when ancillas and measurements are disallowed. Therefore, we have seen an example in which measurement allows for an optimization that may not have been otherwise possible.

We will now establish an initial upper bound on the T-count for C^n-NOT by providing a circuit. We stand at a reasonable starting point, as we can construct C^n-NOT entirely of Toffolis (since the Toffoli is universal for reversible classical computing), and we have a T-count for the Toffoli that is in some sense minimal.

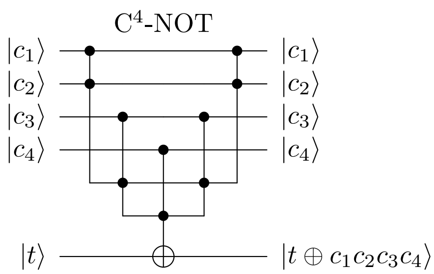
The following are circuits for 3 and 4 controls, respectively:





Generalizing this pattern, a circuit for n controls requires $2n-3$ Toffolis. At 4 T gates per Toffoli, we obtain an upper bound on the C^n-NOT T-count of $8n-12$. This count is already favorable, as it only grows linearly as controls are added.

Furthermore, Gidney's "temporary logical-AND" construction [3] allows this count to be reduced by almost half. His construction (Fig. 4) hinges on his observation that the uncomputation step from Jones' Toffoli can be delayed, allowing the c_1c_2 ancilla to be used for computations elsewhere before being returned to $|0\rangle$. Gidney extends this idea to C^n-NOT by modifying the previous circuit pattern to produce the following (demonstrated with 4 controls):



Each pair of Toffolis on the same wires from the previous circuit is replaced by a temporary logical-AND. Since each logical-AND can be computed and uncomputed for the T-count of only one Toffoli, we effectively almost half the T-count of the entire circuit (the "almost" comes from fact that the central Toffoli on the target qubit remains from the previous construction). Precisely, the new count is 4 T times $n-1$ Toffolis for $4n-4$ T.

3 C^3-NOT with 6 T gates

In 2021, Gidney and Jones [4] published a 6-T C^{3}Z circuit. By conjugating the circuit with Hadamards on the desired qubit, we obtain a 6-T C^3-NOT. We thus save 2 T from the previous state-of-the-art C^3-NOT circuit, which was obtained from the general C^n-NOT construction using temporary ANDs. This new T-count coincides with the lower bound calculated by [6] for C^{3}Z via the stabilizer extent monotone, so the count is minimal (again, I round up from their value of 5.1226). There does not seem to be an obvious way to produce a delayed uncomputation step, a la Jones' Toffoli.

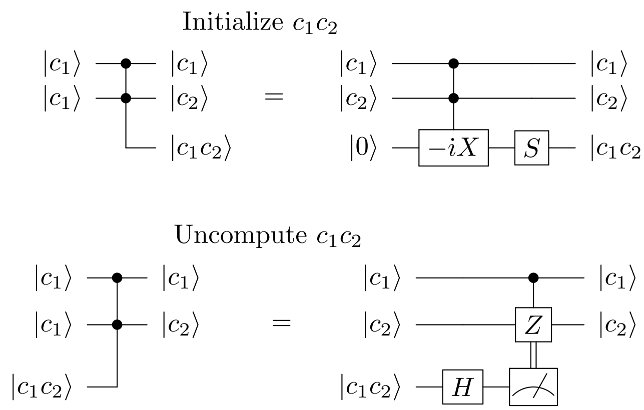


Figure 4: Gidney's [3] 4-T "Temporary logical-AND" construction, consisting of two circuits extended from Jones' Toffoli [7]. The first circuit computes the product c_1c_2 onto an ancilla, and the second circuit uncomputes it. The product can be copied from the wire between the two circuits and used for other computations.

Furthermore, Gidney and Jones noted that their C^3-NOT circuit also reduces the overall C^n-NOT from $4n-4$ to $4n-6$, since C^3-NOT can replace the central Toffoli and the adjacent temporary AND. This brings us to the state-of-the-art count for C^n-NOT.

4 Attempts at further T-count reduction

I have attempted to further reduce the T-count for C^n-NOT, though I have not been successful at the time of writing. Approaches I have tried include:

- Extending the C^{3}Z circuit to more controls / finding other ways to nest it in the C^n-NOT circuit. Like Gidney and Jones, I could not find a circuit with a lower T-count than the state-of-the-art.
- Connecting multiple 4-T Toffolis on the same wire to cause T gate cancellations—also inspired by the C^{3}Z circuit. I did not find a

way to use this trick that produces a useful circuit.

- Using T gates to produce global ω-phases that simplify to -1. This approach is motivated by Selinger's explanation of his CC($-i$Z) circuit. I could not find a way to extend it to more than two controls.

5 Other potential approaches

ZX calculus has been used in prior research to make T-count optimizations to C^n-NOT, so perhaps this area could provide more insight. Examples are [8] and [2].

It may also be interesting to investigate lower bounds on the T-count in order to quantify how much further this metric can be optimized. Rai [9] has established lower bounds of $n+1$ and $2n-2$ using the stabilizer nullity and dyadic monotones, respectively. The latter bound assumes that any measurements have $1/2$ probability. Rai identifies the unitary stabilizer nullity [6] and stabilizer extent [1] as other monotones that could be investigated.

Acknowledgements

I would like to thank Dr. Neil J. Ross and Dr. Peter Selinger for making this project possible. I would also like to thank Dr. Andre Kornell and Dr. Frank Fu for being my supervisors for this project and for teaching me much about quantum computing. Finally, thank you to Dr. Dongho Lee and Dr. Christopher Dean for what they have taught me as well.

References

[1] Michael Beverland, Earl Campbell, Mark Howard, and Vadym Kliuchnikov. Lower bounds on the non-Clifford resources for quantum computations. *Quantum Science and Technology*, 5(3):035009, Jun 2020. https://doi.org/10.1088%2F2058-9565%2Fab8963.

[2] Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and effective techniques for T-count reduction via spider nest identities, 2020. https://arxiv.org/abs/2004.05164.

[3] Craig Gidney. Halving the cost of quantum addition. *Quantum*, 2:74, Jun 2018. https://doi.org/10.22331%2Fq-2018-06-18-74.

[4] Craig Gidney and N. Cody Jones. A CCCZ gate performed with 6 T gates, 2021. https://arxiv.org/abs/2106.11513.

[5] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. An algorithm for the T-count, 2013. https://arxiv.org/abs/1308.4134.

[6] Jiaqing Jiang and Xin Wang. Lower bound for the T count via unitary stabilizer nullity. *Physical Review Applied*, 19(3), Mar 2023. https://doi.org/10.1103%2Fphysrevapplied.19.034052.

[7] Cody Jones. Low-overhead constructions for the fault-tolerant Toffoli gate. *Physical Review A*, 87(2), Feb 2013. https://doi.org/10.1103%2Fphysreva.87.022328.

[8] Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Physical Review A*, 102(2), Aug 2020. https://doi.org/10.1103%2Fphysreva.102.022406.

[9] Ravi Rai. Lower Bounds for Quantum Circuits. 2021. http://hdl.handle.net/10222/81044.

[10] Peter Selinger. Quantum circuits of T-depth one. *Physical Review A*, 87(4), Apr 2013. https://doi.org/10.1103%2Fphysreva.87.042302.