

# Optimising T-count is NP-hard

John van de Wetering<sup>1</sup> and Matt Amy<sup>2</sup>

<sup>1</sup>University of Amsterdam

<sup>2</sup> Simon Fraser University

February 21st 2023

In this short note we show that Boolean satisfiability reduces to finding the optimal number of T gates of a quantum circuit, and hence that optimising T-count is NP-hard. We show that the same argument extends to optimising the number of Toffoli gates in a reversible classical circuit, and we furthermore find an upper bound to the T-count problem of  $\text{NP}^{\text{NQP}}$ .

The number of T gates in a quantum circuit, known as the T-count, is an important metric for how costly it will be to implement this quantum circuit in a fault-tolerant architecture. There have hence been a multitude of results, both heuristics and optimal algorithms, for optimising the T-count of a given circuit or unitary [1, 2, 4–8, 10]. While it is known that optimising CNOT+T circuits is equivalent to Reed-Muller decoding [2] and symmetric 3-tensor factorisation [7], which are known hard problems, to our knowledge no hardness result is known for optimising the T-count of a general Clifford+T circuit. We will demonstrate here a simple argument that shows that this problem is at least NP-hard.

Let the T-COUNT problem be defined as follows: given a Clifford+T circuit implementing a unitary  $U$  and integer  $k$ , determine whether there exists a Clifford+T circuit implementing  $U$  using at most  $k$  T gates. Note that the optimisation version of the problem reduces to the T-COUNT problem via a binary search running logarithmically in the length of the circuit. We can now state our main result.

**Theorem 1.** T-COUNT is NP-hard under polynomial-time Turing reductions.

We establish NP-hardness by reduction from Boolean satisfiability. Let  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  be some Boolean function, given as a Boolean expression. Using standard techniques we can build the classical oracle  $U_f$  implementing  $U_f |\vec{x}, y\rangle = |\vec{x}, y \oplus f(\vec{x})\rangle$ . Note that  $U_f$  is an  $(n+1)$ -qubit quantum circuit which can be constructed as a  $\text{poly}(n)$  size Clifford+T circuit (which requires potentially one borrowed ancilla). Consider then the following quantum circuit  $C_f$ :

$$\begin{array}{c} \vdots \\ \text{---} \\ \vdots \end{array} \boxed{C_f} \begin{array}{c} \vdots \\ \text{---} \\ \vdots \end{array} = \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{U_f} \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{U_f} \begin{array}{c} \vdots \\ \text{---} \\ \vdots \end{array} \quad (1)$$

$\begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{T^\dagger} \oplus \boxed{T} \oplus \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array}$

It is straightforward to verify that  $C_f$  implements the diagonal operation

$$C_f |\vec{x}, y\rangle = e^{i\frac{\pi}{4}(1-2y)f(\vec{x})} |\vec{x}, y\rangle.$$

John van de Wetering: [john@vdwetering.name](mailto:john@vdwetering.name), <http://vdwetering.name>

Matt Amy: [meamy@sfu.ca](mailto:meamy@sfu.ca), <https://www.cs.sfu.ca/~meamy/>

Now, if  $f$  is not satisfiable, then  $f(\vec{x}) = 0$  for all  $\vec{x}$ , and hence we see that  $C_f = \text{id}$ . Additionally, if  $f$  is satisfiable for all  $\vec{x}$ , then we have

$$C_f |\vec{x}, y\rangle = e^{i\frac{\pi}{4}(1-2y)} |\vec{x}, y\rangle = e^{i\frac{\pi}{4}} e^{-i\frac{\pi}{2}y} |\vec{x}, y\rangle = e^{i\frac{\pi}{4}} (I_n \otimes S^\dagger) |\vec{x}, y\rangle.$$

So, up to global phase,  $C_f$  is just an  $S^\dagger$  gate in this case, and hence Clifford. In either case  $C_f$  is Clifford, so that the minimal T-count of  $C_f$  is zero.

Now suppose  $f$  is satisfiable, but that not every input is a solution. Then there exist  $\vec{z}_1$  and  $\vec{z}_2$  such that  $f(\vec{z}_1) = 1$  and  $f(\vec{z}_2) = 0$ . Then it is easy to see that

$$C_f |\vec{z}_1, 0\rangle = e^{i\frac{\pi}{4}} |\vec{z}_1, 0\rangle \quad \text{and} \quad C_f |\vec{z}_2, 0\rangle = |\vec{z}_2, 0\rangle.$$

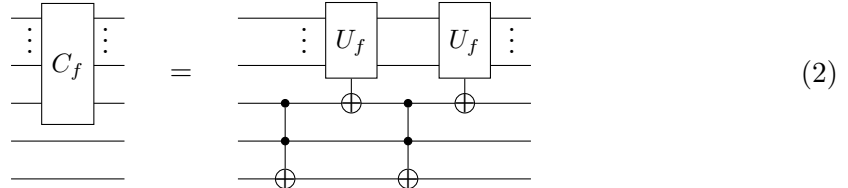
We can now observe that  $C_f$  is non-Clifford by considering the action of  $C_f$  on the  $n$ -qubit Pauli  $X^{\vec{z}_1 \oplus \vec{z}_2} := X^{(\vec{z}_1 \oplus \vec{z}_2)_1} \otimes \dots \otimes X^{(\vec{z}_1 \oplus \vec{z}_2)_n}$ . In particular,

$$C_f^\dagger X^{\vec{z}_1 \oplus \vec{z}_2} C_f |\vec{z}_1, 0\rangle = e^{i\frac{\pi}{4}} C_f^\dagger X^{\vec{z}_1 \oplus \vec{z}_2} |\vec{z}_1, 0\rangle = e^{i\frac{\pi}{4}} C_f^\dagger |\vec{z}_2, 0\rangle = e^{i\frac{\pi}{4}} |\vec{z}_2, 0\rangle,$$

and hence  $C_f^\dagger X^{\vec{z}_1 \oplus \vec{z}_2} C_f$  is not a member of the  $n$ -qubit Pauli group. By definition  $C_f$  is non-Clifford and so its minimal T-count over Clifford+T is necessarily greater than 0.

To complete the reduction, given a Boolean expression  $f$  build  $C_f$  as above in poly time and determine whether a T-count 0 implementation exists. If the minimal T-count is greater than 0,  $f$  is non-constant and hence satisfiable. If instead the minimal T-count is 0, then either  $f$  is not satisfiable or it is always satisfiable. We can distinguish between these two cases by evaluating  $f(0 \dots 0)$ . If  $f(0 \dots 0) = 1$ , then  $f$  is satisfiable, and otherwise we conclude that it must not be satisfiable.

We can use a very similar argument to the one above to show that the problem of TOFFOLI-COUNT, determining the minimal number of Toffoli gates needed to write down a classical reversible circuit (i.e. a quantum circuit consisting of NOT, CNOT and Toffoli gates), is also NP-hard. We then replace the  $C_f$  of Eq. (1) by the following:



Again if  $f$  is not satisfiable,  $C_f$  implements the identity, and if it is always satisfiable, then it implements a CNOT on the bottom two qubits. In both cases the Toffoli-count is zero. Otherwise if  $f(\vec{z}_1) = 1$  and  $f(\vec{z}_2) = 0$  we can check that  $C_f^\dagger X^{\vec{z}_1 \oplus \vec{z}_2} C_f |\vec{z}_1, x, y, z\rangle = |\vec{z}_2, x, y, y \oplus z\rangle$ , so that  $C_f$  is not Clifford, and hence its Toffoli count is not zero.

These arguments show that T-COUNT and its associated optimisation problem are at least NP-hard (and the same for TOFFOLI-COUNT). Let us also demonstrate a simple upper bound to the T-COUNT problem.

**Proposition 2.** The T-COUNT problem is contained in  $\text{NP}^{\text{NQP}}$ .

We first recall that determining whether two poly-size quantum circuits are exactly equal is a coNQP-complete problem [9] (non-deterministic quantum polynomial time). Note that a QMA oracle is not enough since we care about exact equality. Now to determine whether a given  $n$ -qubit circuit  $C$  has an implementation with at most  $k$  T gates, we realise first that such a circuit can be constructed using  $k$  Pauli exponentials, at a cost of  $O(kn)$  gates, and some Clifford circuit, containing  $O(n^2/\log n)$  gates. Hence, we can

non-deterministically choose a circuit with up to  $k$  Pauli exponentials and some Clifford circuit at the end in poly-time, and then use an NQP oracle to determine whether this circuit is equal to  $C$ . Hence T-COUNT is in  $\text{NP}^{\text{NQP}}$ .

Note that classical Boolean circuit minimisation is complete for  $\Sigma_2^P := \text{NP}^{\text{NP}}$  [3], so that the only difference with this bound is that we replace the coNP problem of determining whether Boolean circuits are equal, with the coNQP problem of doing the same for quantum circuits.

**Acknowledgments:** The authors wish to thank Robin Kothari for pointing out that our original upper bound to the T-count problem of  $\text{NP}^{\text{NP}^{\#P}}$  can be improved to  $\text{NP}^{\text{NQP}}$ , and Tuomas Laakkonen for suggesting that our hardness argument might also apply to Toffoli gate optimisation.

## References

- [1] Matthew Amy, Dmitri Maslov, and Michele Mosca. Polynomial-time T-depth optimization of Clifford+ T circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, 2014.
- [2] Matthew Amy and Michele Mosca. T-count optimization and Reed-Muller codes. *Transactions on Information Theory*, 2019.
- [3] David Buchfuhrer and Christopher Umans. The complexity of boolean formula minimization. *Journal of Computer and System Sciences*, 77(1):142–153, 2011.
- [4] Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:23, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
- [5] Vlad Gheorghiu, Michele Mosca, and Priyanka Mukhopadhyay. A (quasi-) polynomial time heuristic algorithm for synthesizing t-depth optimal circuits. *npj Quantum Information*, 8(1):110, 2022.
- [6] Vlad Gheorghiu, Michele Mosca, and Priyanka Mukhopadhyay. T-count and t-depth of any multi-qubit unitary. *npj Quantum Information*, 8(1):141, 2022.
- [7] Luke E Heyfron and Earl T Campbell. An efficient quantum compiler that reduces T count. *Quantum Science and Technology*, 4(015004), 2018.
- [8] Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Physical Review A*, 102:022406, 8 2020.
- [9] Yu Tanaka. Exact non-identity check is nqp-complete. *International Journal of Quantum Information*, 8(05):807–819, 2010.
- [10] Fang Zhang and Jianxin Chen. Optimizing T gates in Clifford+T circuit as  $\pi/4$  rotations around Paulis. Preprint, 2019.