Lower T-count with faster algorithms

arXiv:2407.08695

Vivien Vandaele[1,2]

[1]Eviden Quantum Lab, Les Clayes-sous-Bois, France
[2]Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Abstract

Among the cost metrics characterizing a quantum circuit, the T-count stands out as one of the most crucial as its minimization is particularly important in various areas of quantum computation such as fault-tolerant quantum computing and quantum circuit simulation. In this work, we contribute to the T-count reduction problem by proposing efficient T-count optimizers with low execution times. In particular, we greatly improve the complexity of `TODD`, an algorithm currently providing the best T-count reduction on various quantum circuits. We also propose some modifications to the algorithm which are leading to a significantly lower number of T gates. In addition, we propose another algorithm which has an even lower complexity and that achieves a better or equal T-count than the state of the art on most quantum circuits evaluated. We also prove that the number of T gates in the circuit obtained after executing our algorithms on a Hadamard-free circuit composed of n qubits is upper bounded by $n(n+1)/2+1$, which is the best known upper bound achievable in polynomial time. From this we derive an upper bound of $(n+1)(n+2h)/2+1$ for the number of T gates in a Clifford+T circuit where h is the number of internal Hadamard gates in the circuit, i.e. the number of Hadamard gates lying between the first and the last T gate of the circuit.

1 Introduction

The T gate has a high fault-tolerant implementation cost in most quantum error correcting codes. Consequently, the T-count minimization problem is an important problem to tackle in order to improve the feasibility and efficiency of fault-tolerant quantum computing.

The algorithms achieving the best T-count reduction are foremostly designed for the restricted class of $\{\mathrm{CNOT}, S, T\}$ circuits. The problem of T-count optimization for this class of circuits has been well defined by showing its equivalence with the problem of decoding Reed-Muller codes [1]. In particular, it was demonstrated that the codewords of the punctured Reed-Muller code of length 2^n-1 and order $n-4$ are generating the complete set of identities that can be used to optimize the number of T gates in $\{\mathrm{CNOT}, S, T\}$ circuits. Reducing the number of T gates can then be done by finding relevant identities in this large set. For example it has been shown that a particular subset of identities, called spider nest identities, can be efficiently exploited to reduce the number of T gates [2–5]. An effective way to find relevant identities that can be applied to reduce the number of T gates was given by the `TODD` algorithm [6]. However, an important drawback of the `TODD` algorithm is its complexity of $\mathcal{O}(n^3m^5)$ where n is the number of qubits and m is the number of T gates in the initial circuit, which makes it impractical for circuits of large size. In this work, we show how the complexity of the `TODD` algorithm can be reduced to $\mathcal{O}(n^4m^3)$, where

$n \leq m$. In addition, we propose some modifications to the TODD algorithm which are resulting in a significantly improved reduction in the number of T gates. We also propose another algorithm which has an even lower complexity of $\mathcal{O}(n^2 m^3)$ and that achieves better results than the original TODD algorithm on most quantum circuits evaluated. We also prove our algorithms are producing quantum circuits in which the T-count is upper bounded by $(n^2+n)/2+1$, where n is the number of qubits. We extend our results for minimizing the number of $R_Z(\pi/2^d)$ gates, where d is a non-negative integer. We demonstrate an upper bound for the number of $R_Z(\pi/2^d)$ gates in a Clifford+$\{R_Z(\pi/2^d), R_Z(2\pi/2^d)\}$ circuit. For Clifford+T circuits we obtain an upper bound of $(n+1)(n+2h)/2+1$ for the number of T gates, which can be satisfied in polynomial time and without any ancillary qubit, and where h is the number of internal Hadamard gates in the circuit.

2 Main results

The problem of minimizing the number of T gates in a $\{\text{CNOT}, S, T\}$ circuit corresponds to the following third order symmetric tensor rank decomposition (3-STR) problem [6].

Problem 1 (3-STR)**.** *Let $\mathcal{A} \in \mathbb{Z}_2^{(n,n,n)}$ be a symmetric tensor such that*

$$\mathcal{A}_{\alpha,\beta,\gamma} = \mathcal{A}_{\alpha',\beta',\gamma'} \tag{1}$$

for all α, β, γ and α', β', γ' satisfying the set equality $\{\alpha, \beta, \gamma\} = \{\alpha', \beta', \gamma'\}$. Find a Boolean matrix P of size $n \times m$ such that

$$\mathcal{A}_{\alpha,\beta,\gamma} = |P_\alpha \wedge P_\beta \wedge P_\gamma| \pmod 2 \tag{2}$$

for all α, β, γ satisfying $0 \leq \alpha \leq \beta \leq \gamma < n$, with minimal m.

We will refer to the Boolean matrix P as the parity table. Note that if P contains two identical columns, then Equation 2 would still be satisfied if we remove these two columns from P. Then, a common way of tackling this problem is to start from a parity table P satisfying Equation 2, and to find some vectors $\boldsymbol{z}$ and $\boldsymbol{y}$ such that

$$|P'_\alpha \wedge P'_\beta \wedge P'_\gamma| \equiv |P_\alpha \wedge P_\beta \wedge P_\gamma| \pmod 2 \tag{3}$$

where $P' = P \oplus \boldsymbol{z}\boldsymbol{y}^T$ contains at least two identical columns. To find these two vectors $\boldsymbol{z}$ and $\boldsymbol{y}$, we propose the following theorem.

Theorem 1. *Let P be a parity table of size $n \times m$ and $P' = P \oplus \boldsymbol{z}\boldsymbol{y}^T$ where $\boldsymbol{z}$ and $\boldsymbol{y}$ are vectors of size n and m respectively such that*

$$|\boldsymbol{y}| \equiv 0 \pmod 2 \tag{4}$$

$$|P_\alpha \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{5}$$

$$|P_\alpha \wedge P_\beta \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{6}$$

for all $0 \leq \alpha < \beta < n$. Then we have

$$|P'_\alpha \wedge P'_\beta \wedge P'_\gamma| \equiv |P_\alpha \wedge P_\beta \wedge P_\gamma| \pmod 2 \tag{7}$$

for all $0 \leq \alpha \leq \beta \leq \gamma < n$.

On the basis of this theorem, we can derive an algorithm for optimizing the number of T gates in a $\{\mathrm{CNOT}, S, T\}$ circuit. This algorithm has a complexity of $\mathcal{O}(n^2m^3)$, which is much lower than the $\mathcal{O}(n^3m^5)$ complexity of the `TODD` algorithm [6]. We show that our algorithm provides equivalent or better results in the T-count than the `TODD` algorithm in almost all quantum circuits evaluated in our benchmarks. Furthermore, our algorithm can be used to prove the following theorem:

Theorem 2. *The number of T gates in an n-qubits $\{\mathrm{CNOT}, T, S\}$ circuit can be upper bounded by*

$$2\lfloor (n^2+n)/4 \rfloor + 1 \leq (n^2+n)/2+1 \tag{8}$$

in polynomial time.

Note that this upper bound is asymptotically better than the previously best known upper bound of $(n^2+3n-14)/2$ [7].

The key mechanism of the `TODD` algorithm rests on the following theorem, which was first proven in Reference [6].

Theorem 3. *Let P be a parity table of size $n \times m$ and $P' = P \oplus \boldsymbol{z}\boldsymbol{y}^T$ where $\boldsymbol{z}$ and $\boldsymbol{y}$ are vectors of size n and m respectively such that*

$$|\boldsymbol{y}| \equiv 0 \pmod 2 \tag{9}$$

$$|P_\alpha \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{10}$$

$$|[z_\alpha(P_\beta \wedge P_\gamma) \oplus z_\beta(P_\alpha \wedge P_\gamma) \oplus z_\gamma(P_\alpha \wedge P_\beta)] \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{11}$$

for all $0 \leq \alpha < \beta < \gamma < n$. Then we have

$$|P'_\alpha \wedge P'_\beta \wedge P'_\gamma| \equiv |P_\alpha \wedge P_\beta \wedge P_\gamma| \pmod 2 \tag{12}$$

for all $0 \leq \alpha \leq \beta \leq \gamma < n$.

Instead of solving this system of equations, we show that we can rely on the following simpler system of equations to efficiently find the vectors $\boldsymbol{z}$ and $\boldsymbol{y}$ satisfying the Equations 10 and 11 of Theorem 3. This leads to an algorithm equivalent to the `TODD` algorithm, but which has an improved complexity of $\mathcal{O}(n^4m^3)$.

Theorem 4. *Let P be a parity table of size $n \times m$, and let $\boldsymbol{z}$ and $\boldsymbol{y}$ be vectors of size n and m respectively and such that $|\boldsymbol{y}| \equiv 0 \pmod 2$. Let L and X be matrices with rows labelled by $(\alpha\beta)$ such that*

$$L_{\alpha\beta} = P_\alpha \wedge P_\beta \tag{13}$$

$$X_{\alpha\beta,\gamma} = z_\alpha \delta_{\beta\gamma} \oplus z_\beta \delta_{\alpha\gamma} \tag{14}$$

for all α, β, γ satisfying $0 \leq \alpha \leq \beta < n$ and $0 \leq \gamma < n$, and where δ is the Kronecker delta defined as follows:

$$\delta_{\alpha\beta} = \begin{cases} 0 & \text{if } \alpha \neq \beta, \\ 1 & \text{if } \alpha = \beta. \end{cases} \tag{15}$$

There exists $\boldsymbol{y}'$ such that $L\boldsymbol{y} \oplus X\boldsymbol{y}' = \boldsymbol{0}$ if and only if the following conditions are satisfied:

$$|P_\alpha \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{16}$$

$$|[z_\alpha(P_\beta \wedge P_\gamma) \oplus z_\beta(P_\alpha \wedge P_\gamma) \oplus z_\gamma(P_\alpha \wedge P_\beta)] \wedge \boldsymbol{y}| \equiv 0 \pmod 2 \tag{17}$$

for all $0 \leq \alpha \leq \beta \leq \gamma < n$.

The conditions given by Equations 10 and 11 of Theorem 3 are sufficient for Equation 12 to hold but they are not necessary. We also provide a theorem which gives necessary and sufficient conditions for Equation 12 to be satisfied.

References

[1] Matthew Amy and Michele Mosca. T-count optimization and Reed–Muller codes. *IEEE Transactions on Information Theory*, 65(8):4771–4784, 2019.

[2] Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Techniques to Reduce $\pi/4$-Parity-Phase Circuits, Motivated by the ZX Calculus. *arXiv preprint arXiv:1911.09039*, 2019.

[3] Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158, pages 11:1–11:23, 2020.

[4] Anthony Munson, Bob Coecke, and Quanlong Wang. AND-gates in ZX-calculus: spider nest identities and QBC-completeness. *arXiv preprint arXiv:1910.06818*, 2019.

[5] Witalis Domitrz. On the Verge to Improve Technique of T-count Reduction via Spider Nest Identities. Master's thesis, University of Oxford, 2021.

[6] Luke E Heyfron and Earl T Campbell. An efficient quantum compiler that reduces T count. *Quantum Science and Technology*, 4(1):015004, 2018.

[7] Earl T Campbell and Mark Howard. Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost. *Physical Review A*, 95(2):022316, 2017.