Supplementary Information : T-count and T-depth of any multi-qubit unitary

Vlad Gheorghiu [*1,2], Michele Mosca [†1,2,3,4], and Priyanka Mukhopadhyay [‡1,3]

[1]Institute for Quantum Computing, University of Waterloo, Waterloo ON, Canada
[2]softwareQ Inc., Kitchener ON, Canada
[3]Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo ON, Canada
[4]Perimeter Institute for Theoretical Physics, Waterloo ON, Canada

Supplementary Note 1

The *single qubit Pauli matrices* are as follows:

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \mathrm{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Parenthesized subscripts are used to indicate qubits on which an operator acts For example, $\mathrm{X}_{(1)} = \mathrm{X} \otimes \mathbb{I}^{\otimes(n-1)}$ implies that Pauli X matrix acts on the first qubit and the remaining qubits are unchanged.

The *n-qubit Pauli operators* are : $\mathcal{P}_n = \{Q_1 \otimes Q_2 \otimes \ldots \otimes Q_n : Q_i \in \{\mathbb{I}, \mathrm{X}, \mathrm{Y}, \mathrm{Z}\}\}$.

The *single-qubit Clifford group* $\mathcal{C}_1$ is generated by the Hadamard and phase gates : $\mathcal{C}_1 = \langle \mathrm{H}, \mathrm{S} \rangle$ where

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \mathrm{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

When $n > 1$ the *n-qubit Clifford group* $\mathcal{C}_n$ is generated by these two gates (acting on any of the n qubits) along with the two-qubit $\mathrm{CNOT} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \mathrm{X}$ gate (acting on any pair of qubits).

The Clifford group is special because of its relationship to the set of n-qubit Pauli operators. Cliffords map Paulis to Paulis, up to a possible phase of -1, i.e. for any $P \in \mathcal{P}_n$ and any $C \in \mathcal{C}_n$ we have $CPC^\dagger = (-1)^b P'$ for some $b \in \{0, 1\}$ and $P' \in \mathcal{P}_n$. In fact, given two Paulis (neither equal to the identity), it is always possible to efficiently find a Clifford which maps one to the other.

Fact 1 ([1])**.** For any $P, P' \in \mathcal{P}_n \setminus \{\mathbb{I}\}$ there exists a Clifford $C \in \mathcal{C}_n$ such that $CPC^\dagger = P'$. A circuit for C over the gate set $\{\mathrm{H}, \mathrm{S}, \mathrm{CNOT}\}$ can be computed efficiently (as a function of n).

*vlad.gheorghiu@uwaterloo.ca
†michele.mosca@uwaterloo.ca
‡Corresponding author : mukhopadhyay.priyanka@gmail.com, p3mukhop@uwaterloo.ca

Fact 2. Let $Q = \sum_{P \in \mathcal{P}_n} q_P P$ be the expansion of a matrix Q in the Pauli basis. Then

$$q_P = \mathrm{Tr}\left(QP\right)/N \qquad [N = 2^n].$$

Further, if Q is a unitary then

$$\sum_{P \in \mathcal{P}_n} |q_P|^2 = 1$$

Proof. If $Q = \sum_{P \in \mathcal{P}_n} q_P P$, then taking trace on both sides and dividing by N we get the first equation.

If Q is unitary then we get the following.

$$QQ^\dagger = \mathbb{I} = \left(\sum_P q_P P\right)\left(\sum_P \overline{q_P} P\right) = \sum_P |q_P|^2 \mathbb{I} + \sum_{P \neq P'} q_P \overline{q_{P'}} P P'$$

Now taking trace on both sides and dividing by N, we get the second equation. $\square$

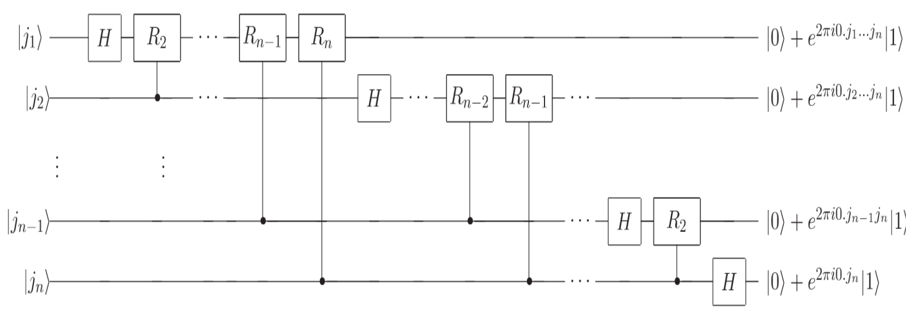
The group $\mathcal{J}_n$ is generated by the n-qubit Clifford group along with the T gate, where

$$\mathrm{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \tag{1}$$

Thus for a single qubit $\mathcal{J}_1 = \langle \mathrm{H}, \mathrm{T} \rangle$ and for $n > 1$ qubits

$$\mathcal{J}_n = \langle \mathrm{H}_{(i)}, \mathrm{T}_{(i)}, \mathrm{CNOT}_{(i,j)} : i, j \in [n] \rangle .$$

It can be easily verified that $\mathcal{J}_n$ is a group, since the H and CNOT gates are their own inverses and $\mathrm{T}^{-1} = \mathrm{T}^7$. Here we note $\mathrm{S} = \mathrm{T}^2$.



Supplementary Figure 1 : Quantum Fourier Transform circuit given in [5].

Supplementary Note 2

In this section we want to prove the following claim.

Claim 1.

$$\sum_{\hat{P}} |\overline{e_{\hat{P}}}||e_{\hat{P}'}| = \sum_{\hat{P}} |e_{\hat{P}}||e_{\hat{P}'}| \leq 2\epsilon^2 - \epsilon^4 \qquad [\hat{P}' \neq \hat{P}, \hat{P}, \hat{P}' \neq \mathbb{I}]$$

For each $\hat{P}$, there exists one $\hat{P}'$ that satisfies a certain condition.

Proof. Let us denote $|e_{\hat{P}}|$ by x_i, where $i \in 1, \ldots, N^2-1$. If $\hat{P}'$ is the Pauli that satisfies the given condition with $\hat{P}$, then we denote the corresponding variable by $x_{i'}$. We must remember that this convention of indices is adapted to identify the variables that satisfy a condition. Each of the variables $x_i \geq 0$. From Equation 11 in Theorem 3.1, we know that $\sum_i x_i^2 \leq 2\epsilon^2 - \epsilon^4$.

$$\sum_{\hat{P}} |e_{\hat{P}}||e_{\hat{P}'}| = \sum_i x_i x_{i'} \leq \sum_{i,j\neq i} x_i x_j \quad [\because x_i \geq 0]$$

So we upper bound the following optimization problem.

$$\begin{aligned} \max_{x_i} \qquad & \sum_{i,j\neq i} x_i x_j \\ \text{such that} \qquad & \sum_{i\neq 0} x_i^2 = 2\epsilon^2 - \epsilon^4 \end{aligned} \tag{2}$$

We can use Karush-Kuhn-Tucker (KKT) conditions [2, 3, 4] to solve the above optimization problem with inequality constraint. For simplicity and without loss of much generality we have used equality in the constraint and follow the Lagrangian method of optimization. Let λ is a Lagrange multiplier. The Lagrange formulations is:

$$\mathcal{L} \quad = \quad \sum_{i,j\neq i} x_i x_j + \lambda \left(\sum_{i\neq 0} x_i^2 - (2\epsilon^2 - \epsilon^4) \right)$$

To find the optimal points we have the following for each i.

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial x_i} \quad &= \quad 2\sum_{j\neq i} x_j + 2\lambda x_i = 0 \\ &\implies \quad \sum_j x_j + (\lambda - 1)x_i = 0 \\ &\implies \quad x_i = \frac{\sum_j x_j}{1-\lambda} \end{aligned} \tag{3}$$

Since this is true for each x_i, we can infer that $x_i = x_j$, where $i \neq j$ and hence

$$\begin{aligned} x_i^2 = \frac{2\epsilon^2 - \epsilon^4}{N^2-1} \qquad &\implies \quad x_i = \sqrt{\frac{2\epsilon^2-\epsilon^4}{N^2-1}}. \\ \text{and} \sum_{i,j\neq i} x_i x_j \quad &\leq \quad (N^2-1)\frac{2\epsilon^2-\epsilon^4}{N^2-1} = 2\epsilon^2 - \epsilon^4. \end{aligned} \tag{4}$$

The claim follows.

□

Supplementary References

[1] Gosset, D., Kliuchnikov, V., Mosca, M. & Russo, V. An algorithm for the T-count. *Quantum Inf Comput*, 14(15-16):1261–1276 (2014).

[2] Karush, W. Minima of functions of several variables with inequalities as side constraints. *M. Sc. Dissertation. Dept. of Mathematics, Univ. of Chicago* (1939).

[3] Kuhn, H.W. et al. Nonlinear programming. In *Proc. Second Berkeley Symp. on Math. Statist. and Probability*. The Regents of the University of California (1951).

[4] Kuhn, H.W. & Tucker, A.W. Nonlinear programming. In *Traces and emergence of nonlinear programming*, pages 247–258. Springer (2014).

[5] Nielsen, M.A. & Chuang, I.L. *Quantum Computation and Quantum Information*. Cambridge University Press (2010).