A Resource-Optimal Canonical Form for Single-qubit Quantum Circuits

Alex Bocharov[1] * Krysta M. Svore[1] †

[1] *Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA 98052 USA*

Abstract. Determining the optimal implementation of a quantum gate is critical for designing a quantum computer. We consider the crucial task of efficiently decomposing a general single-qubit quantum gate into a sequence of fault-tolerant quantum operations. For a given single-qubit circuit, we construct an optimal gate sequence consisting of fault-tolerant Hadamard (H) and $\pi/8$ rotations (T). Our scheme is based on a novel canonical form for single-qubit quantum circuits and the corresponding rules for exactly reducing a general single-qubit circuit to our canonical form. The result is optimal in the number of T gates. We demonstrate that a precomputed ϵ-net of canonical circuits in combination with our scheme lowers the depth and number of T gates of approximation circuits by up to three orders of magnitude compared to previously reported results.

Keywords: quantum computation, quantum circuits

1 Introduction

Quantum algorithms can be described by unitary transformations and projective measurements of a quantum state vector. A unitary transformation can be described by a sequence of unitary matrices, each of which we call a quantum gate. A sequence of one or more quantum gates is called a quantum circuit. A quantum circuit representing a quantum algorithm uses general quantum gates, despite potential challenges with their physical implementations. Therefore, a scalable quantum computer will require processing a general quantum gate into a fault-tolerant, implementable sequence of gates. Various techniques for decomposing quantum gates into a sequence of gates drawn from a discrete gate set are known [1, 2, 3]. However, it is crucial that the resulting gate sequence be optimal in resources such as circuit depth, the number of gates, or the number of qubits are minimized. Achieving lower complexity gate sequences is necessary in order to achieve shorter execution time as well as a smaller probability of error.

Decomposition of a single-qubit quantum circuit most often results in a gate sequence that is approximately equal to the original gate, while exact equivalence is achieved in rare cases. When exact equivalence is not possible or when the circuit must be resource-optimized at the expense of precision, the Solovay-Kitaev theorem [3] guarantees that any single-qubit circuit can be approximated to precision ϵ with a gate sequence of depth $\Theta(\log^c(1/\epsilon))$, where c is a small constant. Dawson and Nielsen [4] developed an algorithm to find an approximation with precision ϵ, which begins with a base approximation to a single-qubit circuit and proceeds recursively, resulting in a circuit that grows in depth as $O(5^n)$, where n depends on the level of precision. Optimizing the base approximation is therefore especially important. Fowler gives an exponential-time algorithm (albeit much faster than brute-force search) for improving the base circuit [5] that finds its depth-optimal ϵ-approximation.

Here, we address the challenge of optimally decomposing quantum circuits that act on a single qubit. To produce optimal gate sequences, we derive a *canonical form* for single-qubit unitaries and corresponding rules for reducing a single-qubit circuit into our canonical form. Our canonical form is similar in spirit to the normal form for single-qubit circuits given by Matsumoto and Amano [6]. However, their normal form is expressed in $SU(2)$, while our canonical form uses group identities in the projective special unitary group $PSU(2)$, allowing further circuit optimization. We then develop an algorithm for finding an exact, resource-optimal decomposition of a single-qubit gate, if it exists; if it does not exist, our algorithm finds an approximation with precision ϵ that significantly reduces the resource cost of the circuit. Our scheme can be used for the base approximation in the Dawson-Nielsen algorithm. We choose to decompose into Hadamard (H) and $\pi/8$ (T) rotations, denoted as $\{H, T\}$, since these gates can be implemented fault-tolerantly in high-threshold codes. We minimize the number of T gates, called the T-count, since the fault-tolerant implementation of T is significantly more expensive than the H gate. Our approach simultaneously reduces circuit depth.

2 A Resource-Optimal Canonical Form

We use . to represent gate composition, $\{\cdot\}$ to indicate the basis elements of a group, and $\langle\cdot\rangle$ to indicate the group generated by those elements, where elements are single-qubit gates. We start with $PSU(2)$ representations of the Hadamard gate H and the $\pi/8$-gate T:

$$H = \begin{bmatrix} i/\sqrt{2} & i/\sqrt{2} \\ i/\sqrt{2} & -i/\sqrt{2} \end{bmatrix}, T = \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{+i\pi/8} \end{bmatrix}.$$

The Phase gate $S = T^2$ and the Hadamard gate H together generate a 24-element subgroup in $PSU(2)$. We denote this group, the Clifford group, as $\mathcal{C}$.

The $\langle T, H\rangle$ group allows an alternative set of two generators, which we call *s*yllables, each of which are composed of two quantum gates: $TH = T.H$, and $SH = S.H$. In $PSU(2)$, TH has infinite order and SH has order 3: $SH.SH.SH = (SH)^3 = I$.

*alexeib@microsoft.com

†ksvore@microsoft.com

We define a non-empty circuit in $\langle TH, SH\rangle$ to be *normalized* if it ends with TH and does not explicitly contain $(SH)^2$. A *normalized* circuit is either the identity I or a non-empty normalized circuit. In other words, a normalized circuit is either the identity I or follows one of two patterns: $n.TH$ or $n.SHTH$, where n is a shorter normalized circuit. The T-*count* of a normalized circuit is defined as the number of TH syllables in that circuit. A normalized circuit is said to be *canonical* if it does not contain SH earlier than the fifth syllable. Thus the shortest canonical circuit that contains SH is $(TH)^4.SH.TH$.

We develop a constructive proof that each $\langle H, T\rangle$ circuit U can be efficiently represented as $U = g_1.c.g_2$, where c is a canonical circuit and $g_1, g_2 \in \mathcal{C}$:

Theorem 1 *If c_1, c_2 are $\mathcal{C}$-equivalent canonical circuits, i.e., $\exists g_1, g_2 \in \mathcal{C}$ such that c_2 and $g_1.c_1.g_2$ evaluate to the same gate in $PSU(2)$, then c_1 and c_2 are equal as $\langle TH, SH\rangle$ circuits.*

It follows that T-count is an invariant of the gate represented by a canonical circuit. There are exactly 2^{k-4} canonical circuits with T-count k. Our canonical form minimizes the T-count of the circuit and optimizes for circuit depth. We can scalably search a collection of canonical circuits on a classical computer due since we prove that canonical circuits with distinct T-counts evaluate to unitary matrices with distinct matrix traces (proofs given in full paper). This implies that if several canonical circuits have the same trace value, they have the same T-count, reducing the search for a more optimized circuit to searching over different trace values.

3 Single-Qubit Circuit Approximation

We approximate a single-qubit circuit by first building a database of canonical circuits by iterating over T-count. We compute precision ϵ between two circuits with the trace distance. Given a single-qubit gate $U \in PSU(2)$, U can be ϵ-approximated with an $\langle H, T\rangle$ circuit with T-count $< t$ if and only if one of the gates in the double coset $\mathcal{C}.U.\mathcal{C} = \{g_1.U.g_2 \,|\, g_1, g_2 \in \mathcal{C}\}$ can be ϵ-approximated by a canonical circuit with T-count $< t$. The optimal ϵ-approximation of U under a certain T-count t is immediately derived from the optimal ϵ-approximation of *some* gate $G \in \mathcal{C}.U.\mathcal{C}$ under T-count t.

We built three ϵ-nets for $\epsilon = 0.002$ of circuits with T-count $< 24, 25, 26$, respectively. The performance of our ϵ-nets within a Solovay-Kitaev algorithm is shown in Fig. 1, which plots the T-count versus ϵ, averaged over the approximation of $10,000$ random unitary gates, for three levels of recursion, for our method and the baseline from [4]. Axes are plotted on the log scale. For a given precision ϵ, we produce gate sequences with up to three orders of magnitude fewer Ts than the baseline approach. For a given T-count, we achieve gate sequences that are up to three orders of magnitude more precise than the baseline approach.

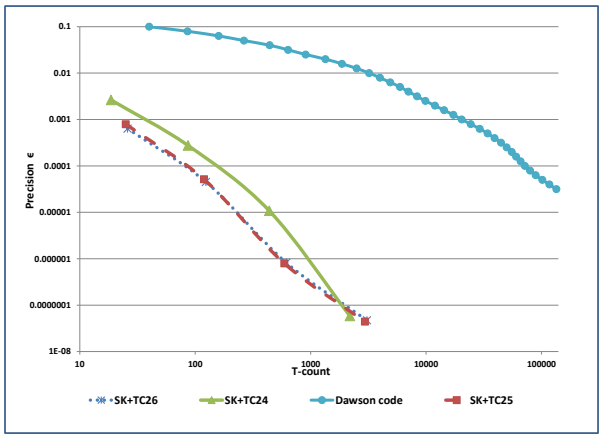

Figure 1: T-count versus mean precision ϵ (trace distance) of the approximation of $10,000$ random unitaries, for recursion levels $n = 0, 1, 2, 3$, indicated by markers.

4 Conclusion

We have defined a resource-optimal canonical form and rules to reduce a single-qubit circuit to our canonical form. Our scheme produces a gate sequence with a minimal number of T gates that is exactly equivalent to the input gate, and it can be used determine a resource-optimal base approximation. When using our technique within the Dawson-Nielsen algorithm, we achieve up to three orders of magnitude improvement in both precision and T-count over the baseline. A future direction is to generalize the definition of a canonical form to other libraries of gates and to extend the form to n-qubit circuits. Another direction is to determine if for a slight decrease in precision ϵ there exists an ϵ-approximate circuit that requires even fewer resources.

References

[1] P.O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On Universal and Fault-tolerant Quantum Computing. `arXiv:quant-ph/9906054`, 1999.

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary Gates for Quantum Computation. *Phys. Rev. A*, 52(3457), 1995.

[3] A. Kitaev, A.H. Shen, and M.N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, Providence, RI, 2002.

[4] C. Dawson and M. Nielsen. The Solovay-Kitaev Algorithm. *Quantum Inf. and Comp.*, 6(1):81–95, 2006.

[5] A.G. Fowler. Constructing Arbitrary Steane Code Single Logical Qubit Fault-Tolerant Gates. *Quantum Inf. and Comp.*, 11:867–873, 2011.

[6] K. Matsumoto and K. Amano. Representation of Quantum Circuits with Clifford and $\pi/8$ Gates. `arXiv:0806.3834`, 2008.