Optimal ancilla-free Clifford+T approximation of z-rotations

Neil J. Ross and Peter Selinger

Department of Mathematics and Statistics
Dalhousie University

Overview

Given a gate set $\mathcal{S}$ universal for quantum computing, the problem of decomposing a unitary operator U into a circuit over $\mathcal{S}$ is known as the *synthesis problem*. This problem can be solved exactly, if U belongs to the set of circuits generated by $\mathcal{S}$. Otherwise, it can be solved approximately, by finding a circuit U' such that $||U' - U|| < \epsilon$ for some chosen precision $\epsilon > 0$.

The synthesis problem is important for quantum computing because it significantly impacts the resources required to run a quantum algorithm. Indeed, a logical circuit, to be executed by a quantum computer, must be compiled into some universal gate set and then implemented fault-tolerantly according to an error correcting scheme. The complexity of the final physical circuit therefore crucially depends on the chosen synthesis method. In fact, in view of the considerable resources required for most quantum algorithms on interesting problem sizes, a universal gate set can be realistically considered for practical quantum computing only if, in addition to an efficient fault-tolerant implementation in some error correcting scheme, it comes equipped with a good synthesis algorithm. Here, a good synthesis algorithm is one that is efficient (e.g., runs in polynomial time) and generates a circuit whose gate count is as low as possible.

Recall that the Clifford+T gate set consists of all the Clifford operators together with the following T-gate, or $\pi/8$ gate:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

The Clifford+T gate set is universal. Because the Clifford group is finite and the Clifford gates are inexpensive with regards to error-correction, a convenient way to measure the complexity of a Clifford+T circuit is its *T-count*: the number of T gates that appear in it.

In this talk, we present an efficient algorithm for the *optimal* decomposition of any z-rotation $R_z(\theta) = e^{-i\theta Z/2}$ into ancilla-free circuits over the Clifford+T gate set. We stress that our algorithm is *literally optimal*, i.e., for any given pair (θ, ϵ) of an angle and a precision, our algorithm finds the *shortest possible* ancilla-free Clifford+T circuit such that $||U - R_z(\theta)|| < \epsilon$. To our knowledge, this is the first time an efficient optimal synthesis algorithm has been given for any gate set.

Related work

Until recently, there were two main approaches to the approximate synthesis problem: the ones based on exhaustive search, like Fowler's algorithm of [2], and the ones based on geometric methods, like the Solovay-Kitaev algorithm (e.g., [1], [3]). The methods based on exhaustive search achieve optimal circuit sizes but, due to their exponential runtimes, are impractical for small ϵ. In contrast, the well-known Solovay-Kitaev algorithm has polynomial runtime and achieves circuit sizes of $O(\log^c(1/\epsilon))$, where $c > 3$. However, the information-theoretic lower

bound for the T-count is $K + 3\log_2(1/\epsilon)$, so the Solovay-Kitaev algorithm leaves ample room for improvement.

In the last two years, number theoretic methods, and in particular Diophantine equations, have been used to define new synthesis algorithms. Along these lines, an efficient algorithm was defined in [4] which uses a small number of ancilla qubits to approximate a given single-qubit operator. Our contribution belongs to this new number-theoretic tradition.

An optimal quantum algorithm and a nearly-optimal classical algorithm

As mentioned above, our algorithm is optimal, in the sense that it outputs the shortest circuit whatsoever for any given problem instance. To achieve this optimality, we require an oracle for the efficient factorization of integers. Because of Shor's algorithm, a quantum computer can of course serve as such an oracle; it is for this reason that our optimal synthesis algorithm is actually a quantum algorithm.

However, even in the absence of a factoring oracle, we can prove under a mild number-theoretic assumption that our algorithm finds a solution of T-count $m + O(\log(\log(1/\epsilon)))$, where m is the T-count of the second-to-optimal solution. In the typical case, m is given by the information-theoretic lower bound, so that the circuit decompositions have T-count $3\log(1/\epsilon) + O(\log(\log(1/\epsilon)))$ in the typical case. We therefore also obtain a classical synthesis algorithm that is *nearly optimal* in the sense that only differs from optimal by $O(\log(\log(1/\epsilon)))$.

Finally, we remark that our algorithm is only optimal (or, in the classical case, nearly optimal) for z-rotations. Nevertheless, it can still be used to approximate an arbitrary unitary $U \in SU(2)$, by using Euler angles to decompose U into three z-rotations

$$U = R_z(\theta_1)\, H\, R_z(\theta_2)\, H\, R_z(\theta_3),$$

and then applying the algorithm to each one of the three $R_z(\theta_i)$. In this case, we achieve a T-count of $9\log(1/\epsilon) + O(1)$ in the quantum case, and $9\log(1/\epsilon) + O(\log(\log(1/\epsilon)))$ in the classical case.

Sketch of the algorithm

We briefly outline some of the main ideas of the algorithm. The inputs are an angle θ and a precision ϵ, and the goal is to approximate $R_z(\theta)$ up to ϵ by the shortest possible Clifford+T circuit. We know from [5] that an operator U is in the Clifford+T group if and only if it is of form

$$U = \begin{pmatrix} u & -t^\dagger \omega^\ell \\ t & u^\dagger \omega^\ell \end{pmatrix},$$

where ℓ is an integer, $\omega = e^{i\pi/4}$ and u, t belong to the ring $\mathbb{D}[\omega] = \mathbb{Z}[1/\sqrt{2}, i]$. Moreover, [5] also contains an algorithm for the exact synthesis of such matrices into Clifford+T circuits. It can be shown that in fact a Clifford+T gate U is a solution to the approximate synthesis problem for θ and ϵ only if it is of the form

$$U = \begin{pmatrix} u & -t^\dagger \\ t & u^\dagger \end{pmatrix}. \tag{1}$$

Furthermore, the T-count for U is a function of the so-called *least denominator exponent* of u, which is the power of $\sqrt{2}$ occurring in the denominator of u. Therefore, if we find u in $\mathbb{D}[\omega]$ such that

(i) there exists $t \in \mathbb{D}[\omega]$ such that $u^\dagger u + t^\dagger t = 1$,

(ii) the matrix of the form (1) constructed using t and u satisfies $||U - R_z(\theta)|| \leq \epsilon$, and

(iii) the least denominator of u is minimal,

then we can apply the exact synthesis algorithm to U to optimally solve the approximate synthesis problem for θ and ϵ.

The key point here is that the inequality in (ii) depends only on u (not on t). Moreover, the inequality in (ii) can be reformulated as a problem of the form $u \in A$ and $u^\bullet \in B$, where A and B are fixed convex subsets of the complex plane depending only on θ and ϵ, and where $(-)^\bullet$ is the automorphism of the ring $\mathbb{D}[\omega]$ obtained by mapping $\sqrt{2}$ to $-\sqrt{2}$. We call such a problem a *two-dimensional grid problem*. We formulate a general algorithm for solving one- and two-dimensional grid problems efficiently. The main technical ingredient that makes our solution efficient is an iterative process for normalizing two-dimensional grid problems.

Using this algorithm, we enumerate the solutions u to inequality (ii) in order of increasing least denominator exponent. For each such solution u we attempt to solve the Diophantine equation

$$u^\dagger u + t^\dagger t = 1.$$

If the equation can be solved, then we have found a Clifford+T approximation U of $R_z(\theta)$, and we can use the exact synthesis algorithm to write U as a Clifford+T circuit.

This talk describes work developed in [6, 7]. A detailed presentation of the algorithm can be found in [6].

References

[1] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1):81–95, Jan. 2006. Also available from `arXiv:quant-ph/0505030`.

[2] A. G. Fowler. Constructing arbitrary Steane code single logical qubit fault-tolerant gates. *Quantum Information and Computation*, 11(9–10):867–873, 2011. Also available from `arXiv:quant-ph/0411206`.

[3] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. Graduate Studies in Mathematics 47. American Mathematical Society, 2002.

[4] V. Kliuchnikov, D. Maslov, and M. Mosca. Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits. *Phys. Rev. Lett.*, 110:190502 (5 pages), 2013. Also available from `arXiv:1212.0822v2`.

[5] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. *Quantum Information and Computation*, 13(7–8):607–630, 2013. Also available from `arXiv:1206.5236v4`.

[6] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. `arXiv:1403.2975`, 2014.

[7] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information and Computation*, 2014. To appear. Also available from `arXiv:1212.6253`.