Quantum Circuits for Isometries

Raban Iten, Roger Colbeck, Jonathan Home, and Matthias Christandl

(Dated: 8th December 2014)

Every quantum gate can be decomposed into a sequence of single-qubit gates and Controlled-NOT (C-NOT) gates [1]. In many implementations, single-qubit gates are relatively 'cheap' to perform compared to C-NOTs, (for example, single-qubit gates may be technically simpler to construct, or less susceptible to noise). It is hence desirable to minimize the number of C-NOT gates required to implement a circuit.

Previous work has looked at C-NOT-efficient synthesis of arbitrary quantum gates and state preparation (see for example [2, 3] and references therein). Here we consider the generalization to arbitrary isometries from m qubits to n qubits. We derive a theoretical lower bound on the number of C-NOT gates required to decompose an isometry for arbitrary m and n, and give an explicit gate decomposition that achieves this bound up to a factor of about two in the leading order. We also perform some bespoke optimizations in the case of small m and n.

Experimental groups strive to demonstrate their ability to control a small number of qubits, and the ultimate demonstration would be to the ability to do any quantum operation on them. Since any such operation can be implemented via an isometry followed by partial trace (using Stinespring's theorem), our decomposition scheme for isometries points towards an efficient way to synthesize quantum operations (complementing an existing approach [4, 5]), and could also be used in the construction of arbitrary POVMs.

A quantum gate on n qubits can be represented by a $2^n \times 2^n$ unitary matrix. In the case of state preparation we only need to rotate one input state (conventionally $|0\rangle^{\otimes n}$) to the state we are trying to prepare. The sequence of gates we use to do this will correspond to a general unitary matrix, but, for state preparation, we are only interested in the first (working in the computational basis) column of this matrix and the others can be arbitrary. In the more general case, $n - m$ qubits start in the basis state $|0\rangle$ and the state of the other m qubits is arbitrary. Mathematically, this corresponds to an isometry from m qubits to n qubits or alternatively we can think of such an operator as a unitary $2^n \times 2^n$ matrix, where we are only interested in the first 2^m columns.

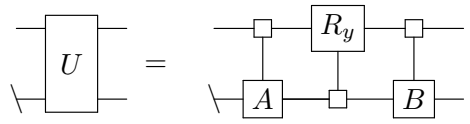
A parameter counting argument has been used to find a theoretical lower bound on the number of C-NOT gates required to implement arbitrary quantum gates [6, 7] and for state preparation [3], and is readily extended to the case of isometries (see Table I). In the case of synthesis of arbitrary

	State preparation	$1 \leqslant m \leqslant n-2$ to n Iso. (CCD)	$n-1$ to n Iso. (CSD)	Arbitrary n-qubit gate
#C-NOT	$\frac{23}{24}2^n - 2\cdot 2^{\frac{n}{2}} + \frac{5}{3}$, n even [3] $\frac{23}{24}2^n - \frac{3}{2}2^{\frac{n+1}{2}} + \frac{4}{3}$, n odd	$2^{m+n} - \frac{1}{24}2^n + \mathcal{O}\left(n^2\right)2^m$	$\frac{23}{64}4^n - \frac{5}{4}2^n + 1$	$\frac{23}{48}4^n - \frac{3}{2}2^n + \frac{4}{3}$ [2]
LB	$\lceil \frac{1}{2}\left(2^n - n - 1\right)\rceil$ [3]	$\lceil \frac{1}{2}2^{m+n} - \frac{1}{4}\left(2^{2m} + 2n + m + 1\right)\rceil$	$\lceil \frac{3}{16}\left(4^n - 4n\right)\rceil$	$\lceil \frac{1}{4}\left(4^n - 3n - 1\right)\rceil$ [6, 7]

TABLE I: Best known C-NOT counts for m to n isometries for large n and lower bounds. As is to be expected, the number of required C-NOT gates increases if m increases. Or in other words, the cost of the computation is found to be lower when more of the input data is fixed. Abbreviations: LB: Lower bound; CCD: Column by Column Decomposition of an isometry (our first technique); CSD: Decomposition of an isometry using the Cosine-Sine Decomposition (our second technique).

quantum gates, the minimum number of C-NOT gates is achieved using a powerful matrix decomposition, the Cosine-Sine Decomposition (CSD) [2]. This states that every $2^n \times 2^n$ unitary matrix U can be decomposed into $2^{n-1} \times 2^{n-1}$ unitaries A_0, A_1, B_0, B_1 and real diagonal matrices C and S satisfying $C^2 + S^2 = I$ as follows (in both matrix and circuit form):

$$U = \begin{pmatrix} B_0 & \\ & B_1 \end{pmatrix} \left(\begin{array}{c|c} C & -S \\ \hline S & C \end{array}\right) \begin{pmatrix} A_0 & \\ & A_1 \end{pmatrix}$$



The backslash in the circuit equivalence denotes that the second wire carries $n-1$ qubits and the unfilled square denotes a uniform control, e.g. the first gate on the right hand side of the circuit equivalence performs the operation A_0 if the upper qubit is in the state $|0\rangle$ and A_1 if it is in the state $|1\rangle$ (cf. [2] for more details). In [2], it is shown how this can be used to achieve the C-NOT count in the final column of Table I, roughly twice the lower bound. This technique also corresponds to a simple and constructive proof of the universality of single-qubit and C-NOT gates.

In the case of state preparation the best known decomposition [3] has been found using the Schmidt decomposition, and the resulting count is again about twice that of the theoretical lower bound (see the first column of Table I).

We introduce a decomposition scheme for an arbitrary isometry V from m to n qubits using about twice the number of C-NOT gates required by the theoretical lower bound for large n (analogously to the best known decompositions for arbitrary quantum gates and for state preparation). Our decomposition generates the isometry column by column. Note that V can be described by a $2^n \times 2^m$ matrix, which can instead be represented by a $2^n \times 2^n$ unitary matrix $G^\dagger$ by writing $V = G^\dagger I_{2^n \times 2^m}$, where $I_{2^n \times 2^m}$ denotes the first 2^m columns of the $2^n \times 2^n$ identity matrix. Note that $G^\dagger$ is not unique (unless $m = n$).

We decompose a gate of the form $G^\dagger$ in terms of C-NOTs and single-qubit gates. Since a C-NOT gate is inverse to itself and the inverse of a single-qubit gate is another single-qubit gate,

this is equivalent to an analogous decomposition of a quantum gate G satisfying $I_{2^n\times 2^m} = GV$. Our technique works by constructing a sequence of unitary matrices that when applied to V successively bring it closer to $I_{2^n\times 2^m}$. We do this in a column by column fashion, first choosing a sequence of quantum gates, corresponding to G_0 that get the first column right, i.e., $G_0V|0\rangle^{\otimes m} = I_{2^n\times 2^m}|0\rangle^{\otimes m} = |0\rangle^{\otimes n}$. We then use G_1 to get the second column right without affecting the first, i.e., $G_1G_0V(|0\rangle^{\otimes(m-1)}\otimes|1\rangle) = I_{2^n\times 2^m}(|0\rangle^{\otimes(m-1)}\otimes|1\rangle) = |0\rangle^{\otimes(n-1)}\otimes|1\rangle$ and $G_1G_0V|0\rangle^{\otimes m} = G_1|0\rangle^{\otimes n} = |0\rangle^{\otimes n}$, and so on. For the first column a decomposition scheme for state preparation can be used (in reverse). However, this idea does not work for the second column, since the operator performing the inverse of state preparation on the second column wouldn't act trivially on $|0\rangle^{\otimes n}$ in general. We therefore introduce a modified technique that takes this into account while only slightly increasing the number of C-NOT gates needed over that required for state preparation on each column. This technique borrows a decomposition scheme for uniformly controlled gates from [8]. We describe this technique in our work and give a rigorous proof that it works for arbitrary isometries in the Appendix. This proof can also be seen as an alternative way to [1] to prove the universality of the gate library containing single-qubit and C-NOT gates.

Remark: In the cases $m = n$ and $m = n - 1$, it turns out that there is a more efficient decomposition based on the CSD. In the case $m = n$, this is exactly the deomposition used in [2] for arbitrary gate synthesis. For $m = n - 1$ an adaptation of this technique can be used to give a lower C-NOT count than our first method. This is also displayed in Table I.

Since the number of qubits which are manageable in physical experiments is still quite small, we have also tailored optimizations of these techniques in the case of small n. In particular one can use our decomposition schemes for isometries to lower the up to date lowest known C-NOT count for state preparation on five qubits from 26 to 19 C-NOT gates.

---

[1] A. Barenco et al., Physical Review A **52**, 3457 (1995).

[2] V. V. Shende, S. S. Bullock, and I. L. Markov, IEEE Trans. Computer-Aided Design **25**, 1000 (2006).

[3] M. Plesch and Č. Brukner, Phys. Rev. A **83**, 032302 (2011).

[4] D.-S. Wang, D. W. Berry, M. C. de Oliveira, and B. C. Sanders, Phys. Rev. Lett. **111**, 130504 (2013).

[5] D.-S. Wang and B. C. Sanders, URL `http://arxiv.org/abs/1407.7251`.

[6] V. V. Shende, I. L. Markov, and S. S. Bullock, Physical Review A **69**, 062321 (2004).

[7] V. V. Shende et al., in *Proc. Design, Automation, and Test Eur.* (2004), vol. 2, pp. 980–985.

[8] V. Bergholm et al., Phys. Rev. A **71**, 052330 (2005).