Factoring k-controlled-unitaries into $4k^2$ controlled gates without ancillas

Jacob Biamonte[1], Nike Dattani[2] and Mauro E.S. Morales[1]
[1]Deep Quantum Labs
Skolkovo Institute of Science and Technology
3 Nobel Street, Moscow, Russia 121205
[2]HPQC Labs
National Research Council of Canada
100 Sussex Drive, Ottawa, Canada K1A 0R6

October 28, 2018

Abstract

We aim to find factorizations of k-controlled unitary gates into a sequence of two-body gates. For example, the well-studied case in which the unitary is the NOT-gate and for $k = 2$, can be realized over a variety of circuit families. The most common is perhaps the basis $\{CV, CNOT\}$ where $CV^2 = CNOT$.

1 Introduction to the problem

2 Factorization by group commutators

Our method is inspired by a Toffoli factorization first appearing in the book [1].

Remark 1 (Paulis' group algebra) *The complete properties of the Hermitian Pauli (group-) algebra can be derived from the following identity.*[1]

$$\sigma_i \sigma_j = \mathbb{1}\delta_{ij} + \imath \epsilon^{ijk} \sigma_k \tag{1}$$

[1]We denote the complex unit as $\imath^2 = -1$.

We will interchange the notation $\sigma_0 = \mathbb{1}$, $\sigma_1 = X$, $\sigma_2 = Y$, $\sigma_3 = Z$.

Definition 1 (Group commutator) *Let unitaries* U, $K \in End\{\mathcal{C}\}$, *then the group commutatory of* U *and* K *is defined as*

$$[U, K] = UKU^\dagger K^\dagger \tag{2}$$

Lemma 1 *For* $i \neq j$

$$\sigma_i e^{-\imath t\sigma_j}\sigma_i = e^{\imath t\sigma_j} \tag{3}$$

Lemma 2 *For* $i \neq j$ *and using 1*

$$[\sigma_i, e^{-\imath t\sigma_j}] = \sigma_i e^{-\imath t\sigma_j}\sigma_i e^{\imath t\sigma_j} = e^{\imath 2t\sigma_j} \tag{4}$$

Definition 2 (Controlled gates) *Denote by* $\Lambda_{ij}(U)$ *the gate* U *acting on qubit* j *and controlled by qubit* i. *Specifically let* X_{ij} *be the controlled-not gate and let* V_{ij} *be the square-root of* X_{ij}. *With slight abuse of notation, we can consider qubit with label* j *to be in state* $|j\rangle$.

Lemma 3 (Toffoli gate) *The Toffoli gate has a factorization into four control gates viz.*

$$Z^a_{ac}(V^\dagger)^b_{bc}Z^a_{ac}V^b_{bc} = X^{a\wedge b}_c \tag{5}$$

where $\sqrt{X} = V$.

Example 1 (CCCNOT gate in 10-controlled gates)

Lemma 4 k*-controlled* U *factors into* $2 \times \lceil k/2\rceil$*-controlled-*$X$ $+ 2 \times \lfloor k/2\rfloor$*-controlled-*$\sqrt{Z}$ *gates.*

Lemma 5 (Recurrence) *Let* $g(l)$ *be monotonic increasing on* $l \geq 1$ *and count the number of control gates. So* $g(2) = 4$ *(Toffoli) and*

$$g(l) = 2g(\lceil l/2\rceil) + 2g(\lfloor l/2\rfloor) \tag{6}$$

If l *is even then* $\lceil l/2\rceil = \lfloor l/2\rfloor$. *If* l *is odd then* $\lceil l/2\rceil = \lfloor l/2\rfloor + 1$. *Hence*

$$g(l) \leq 2g(\lfloor l/2\rfloor) + 2g(\lfloor l/2\rfloor + 1) \tag{7}$$

Note that $0 \leq x - \lfloor x\rfloor \leq 1$ *and so*

$$g(l) \leq 2g(l/2) + 2g(l/2+1) \leq 4g(l/2+1) \leq 4g\left(\frac{l+2}{2}\right) \tag{8}$$

The r.h.s. above is motivated by boundary conditions on the recurrence, which is solved as $g(l) = 4(n-1)^2$. [2].

Lemma 6 (Lower bound for scaling of g***)*** *Let* $g(l)$ *count the number of gates required for the decomposition given in the text. Its definition given by initial conditions* $g(1) = 1$, $g(2) = 4$ *and the following recursion*

$$g(l) = \begin{cases} 4g(l/2) & l\,even \\ 2g(\lfloor l/2 \rfloor) + 2g(\lfloor l/2 \rfloor + 1) & l\,odd \end{cases}$$

We prove that for every $l \geq 1$ *we have* $l^2 \leq g(l)$. *We proceed by strong induction. Note first that* $1^2 \leq g(1)$ *and* $2^2 \leq g(2)$. *Assume that the property holds for* $g(l-1), g(l-1), ..., g(1)$. *Consider the cases* l *even and* l *odd separately. For* l *even we have*

$$g(l) = 4g(l/2) \geq 4(l/2)^2 = l^2 \tag{9}$$

Now for l *odd we have*

$$g(l) \geq 2(\lfloor l/2 \rfloor)^2 + 2(\lfloor l/2) \rfloor + 1)^2 \geq 2(\lfloor l/2 \rfloor)^2 + l^2 \geq l^2 \tag{10}$$

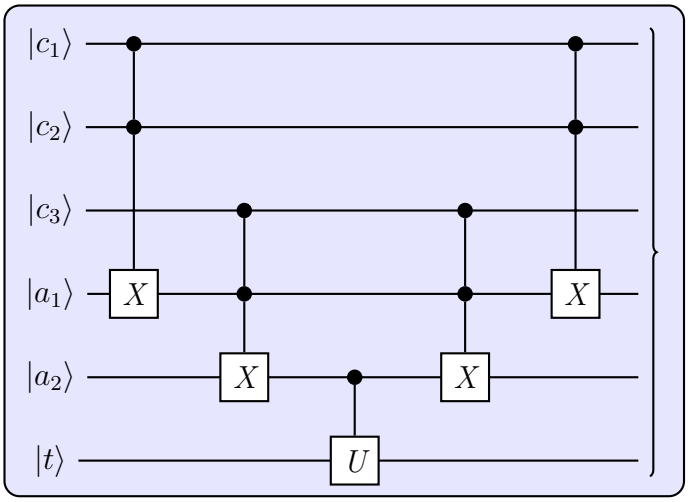
Since for every $l > 0$ $g(l) \geq l^2$ *we conclude* $g(l) = \Omega(l^2)$.

3 Comparison with other methods

3.1 The naive approach

- *2-qubit gates:* $12(k-1)$,
- *1-qubit gates:* $18(k-1)$,
- *TOTAL gates:* $30(k-1)$,
- *Auxiliary qubits:* $k-1$.

[2] I think this is probably wrong. The idea is this. We need to bound the relationship, and then solve it. But in making the bound, we don't want to mess with the boundaries of the recurrence (I might have done that



3.2 Craig Gidney (we'll name it properly after)

- *2-qubit gates:* $8(k-2)+1$,
- *1-qubit gates:* $k-2$,
- *TOTAL gates:* $9(k-2)$,
- *Auxiliary qubits:* $k-1$.

4 Conclusion

References

[1] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. Classical and Quantum Computation. *American Mathematical Society, Boston, MA, USA, 2002.*