Quantum Computing
WS 2009/10

Prof. Dr. Erich Grädel

Mathematische Grundlagen der Informatik
RWTH Aachen

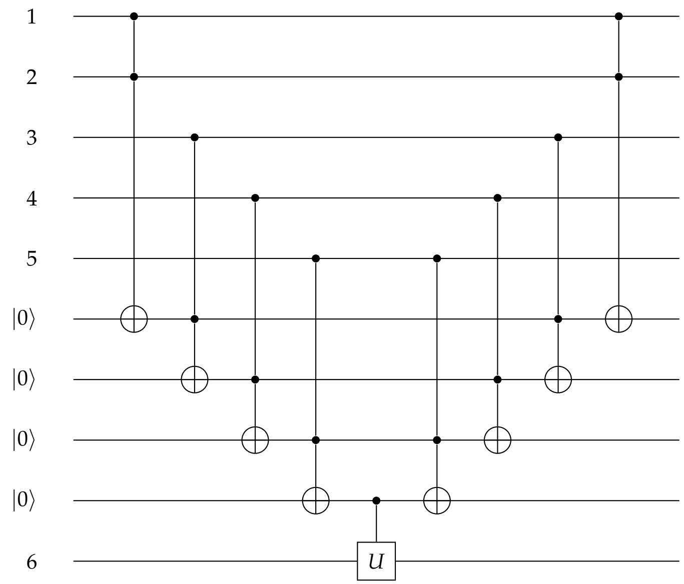
Contents

2 Universal Quantum Gates

Consider the *n-ary* controlled operation c^n-U defined by

$$\mathrm{c}^n\text{-}U|i_1 \dots i_n j\rangle = |i_1 \dots i_n\rangle \otimes \begin{cases} U|j\rangle & \text{if } i_1, \dots, i_n = 1, \\ |j\rangle & \text{otherwise.} \end{cases}$$

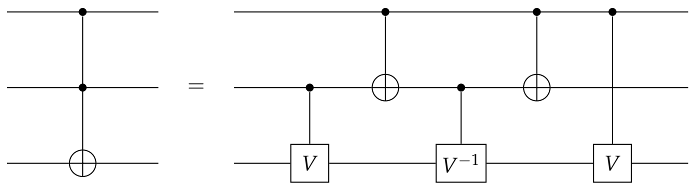
How can we implement a complicated operation such as c^n-U using simple gates such as Tf and c-U? The idea is to introduce a certain number of *control qubits*, which are initially set to 0. Then, we can implement c^n-U as follows (the right part of the array resets the work qubits to 0):



In fact, we can build up the Toffoli gate Tf from the two-qubit gates c-V, c-V^{-1} and c-$M_\neg$, where

$$V = \sqrt{M_\neg} = \frac{1}{2}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix},$$

as follows:



To see this, note that the gate on the right maps $|ijk\rangle$ to $|ij\rangle \otimes |f(i,j,k)\rangle$, where

$$|f(i,j,k)\rangle = \begin{cases} |k\rangle & \text{if } |ij\rangle = |00\rangle, \\ V^{-1}V|k\rangle = |k\rangle & \text{if } |ij\rangle = |01\rangle, \\ VV^{-1}|k\rangle = |k\rangle & \text{if } |ij\rangle = |10\rangle, \\ VV|k\rangle = |k \oplus 1\rangle & \text{if } |ij\rangle = |11\rangle \end{cases}$$
$$= |ij \oplus k\rangle.$$

Lemma 2.1. Tf is computable by a QGA over $\{\mathrm{H}, \text{c-}M_\neg, \mathrm{S}, \mathrm{T}, \mathrm{T}^{-1}\}$ (see Figure 2.1).

Proof. By calculation. Q.E.D.

The general question here is which gates are sufficient for building arbitrary unitary transformations. We will show that a QGA can be *approximated* arbitrarily well by a QGA that consists of Hadamard, CNOT and T gates only. More precisely, we will show that

(1) every unitary transformation U can be written as a product $U = U_m \ldots U_1$ of unitary operators U_i that operate nontrivially only on a two-dimensional subspace of H_{2^n} (generated by two vectors of the standard basis).

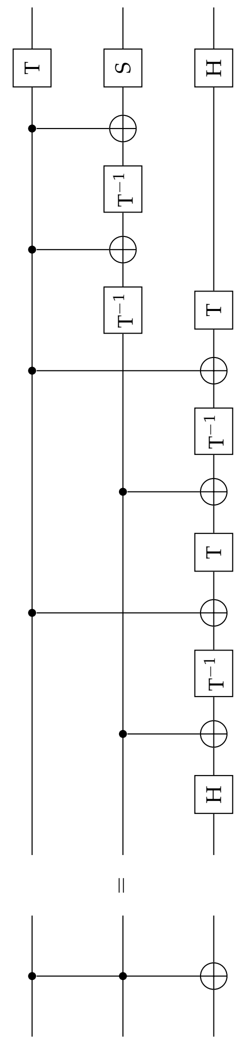


Figure 2.1. An implementation of the Toffoli gate over $\{\mathrm{H}, \text{c-}M_\neg, \mathrm{S}, \mathrm{T}, \mathrm{T}^{-1}\}$.

(2) every unitary transformation can be composed from CNOT and quantum gates that operate on one qubit only;

(3) 1-qubit quantum gates can be approximated arbitrarily well using H and T.

To prove (1), consider a unitary transformation $U : H_m \to H_m$ described by a unitary $(m \times m)$-matrix.

Lemma 2.2. U is a product of unitary matrices of the form

$$\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & a & & c & & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & b & & d & & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}.$$

Proof. Consider, for instance, $m = 3$ and

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}.$$

If $b = 0$, set $U_1 = \mathrm{I}$. Otherwise, set

$$U_1 = \begin{pmatrix} \frac{a^*}{\delta} & \frac{b^*}{\delta} & \\ \frac{b}{\delta} & -\frac{a}{\delta} & \\ & & 1 \end{pmatrix},$$

where $\delta = \sqrt{|a|^2 + |b|^2}$. The matrix U_1 is unitary, and $U_1 \cdot U$ is of the form

$$U_1 \cdot U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}.$$

If $c' = 0$, set $U_2 = \begin{pmatrix} a'^* & & \\ & 1 & \\ & & 1 \end{pmatrix}$. Otherwise, set

$$U_2 = \frac{1}{\sqrt{|a'|^2 + |c'|^2}} \begin{pmatrix} a'^* & 0 & c'^* \\ 0 & 1 & 0 \\ c' & 0 & -a' \end{pmatrix}.$$

The matrix $U_2 U_1 U$ is unitary and of the form

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ c' & f'' & j'' \end{pmatrix}.$$

Since $U_2 U_1 U$ is unitary, we have $d'' = g'' = 0$. Finally, set

$$U_3 = \begin{pmatrix} 1 & & \\ & e''^* & f''^* \\ & h''^* & j''^* \end{pmatrix}.$$

We have $U_3 U_2 U_1 U = \mathrm{I}$, so $U = U_1^* U_2^* U_3^*$, and each U_i^* is of the desired form.

In general, we are able to find matrixes $U_1, \ldots, U_k$ of the desired form such that $U_k \ldots U_1 U = \mathrm{I}$, where $k \leq (m-1) + (m-2) + \cdots + 1 = \frac{m(m-1)}{2}$. Q.E.D.

Corollary 2.3. A unitary transformation on n qubits is equivalent to a product of at most $2^{n-1}(2^{n-1} - 1)$ unitary matrices that operate nontrivially only on a 2-dimensional subspace of H_{2^n} (generated by two vectors of the standard basis).

Remark 2.4. The exponential blowup incurred by this translation is not avoidable.

We can now turn towards proving (2).

Lemma 2.5. Let $U : H_{2^n} \to H_{2^n}$ be a unitary transformation that operates nontrivially only on the subspace of H_{2^n} generated by $|x\rangle = |x_1 \ldots x_n\rangle$ and $|y\rangle = |y_1 \ldots y_n\rangle$. Then U is a product of CNOT and 1-qubit gates.

Proof (Sketch). Let V be the nontrivial, unitary (2×2)-submatrix of U. V can be viewed as a 1-qubit gate. Recall that, for each n, the operation C^n-V can be implemented using Tf (which can be built from CNOT and single qubit gates) and C-V. The gate C-V, on the other hand, can be implemented using CNOT and single qubit operations (see Nielsen & Chuang, *Quantum Computation and Quantum Information*, Section 4.3).

Fix a sequence $|z_1\rangle, \ldots, |z_m\rangle$ of basis vectors such that $|z_1\rangle = |x\rangle$, $|z_m\rangle = |y\rangle$, and $|z_i\rangle$ differs from $|z_{i+1}\rangle$ on precisely one qubit. The idea is to implement U as a product $U = P_1 \cdots P_{m-1}(\mathrm{C}^*\text{-}V)P_{m-1} \cdots P_1$. The matrix P_i maps $|z_i\rangle$ to $|z_{i+1}\rangle$ and vice versa, and C^*-V is the operation of V on the qubit that distinguishes $|z_{m-1}\rangle$ and $|z_m\rangle$, controlled by all other qubits. Note that $P_{m-1} \cdots P_1$ maps $|x\rangle$ to $|y\rangle$, and $P_1 \cdots P_{m-1}$ maps $|y\rangle$ back to $|x\rangle$. As we have seen, C^*-V and each P_i can be implemented using CNOT and 1-qubit gates. Q.E.D.

Finally, we can discuss (3), the reduction of arbitrary 1-qubit gates to H and T. Note that there exist uncountably many unitary transformations $U : H_{2^n} \to H_{2^n}$, but from a finite (or even countably infinite) set of gates, we can only compose countably many QGAs. Hence, there is no way of representing every 1-qubit gate *exactly* using a fixed finite set of gates. However, an *approximation* is possible! For two unitary transformations U and V, we define

$$\mathrm{E}(U, V) := \max_{\||\psi\rangle\|=1} \|(U - V)|\psi\rangle\|.$$

Theorem 2.6 (Solvay-Kitaev)**.** For every QGA U consisting of m CNOT or 1-qubit gates and for every $\varepsilon > 0$, there exists a QGA V of size $\mathrm{O}(m \cdot \log^c \frac{m}{\varepsilon})$, $c \approx 2$, consisting of CNOT, H and T gates only such that $\mathrm{E}(U, V) \leq \varepsilon$.