MIT 2.111/8.411/6.898/18.435 Quantum Information Science I *Fall, 2010*
Sam Ocko
October 26, 2010

Problem Set # 6 Solutions

1. **Building controlled-U from U**

   (a)

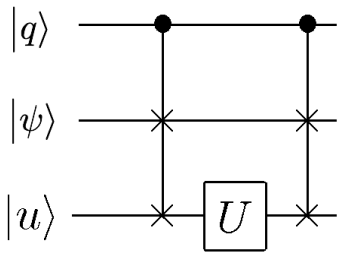


FIG. 1. Circuit which implements a controlled-U gate. $U|u\rangle = |u\rangle$

   (b) We may use a similar construction when $U|u\rangle = e^{i\phi}|u\rangle$ for a known ϕ. We just need to correct this phase appropriately.

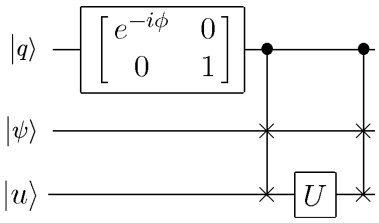


FIG. 2. Circuit which implements a controlled-U gate. $U|u\rangle = e^{i\phi}|u\rangle$

   (c) We can't do a similar procedure for an unknown ϕ because we don't know how much a phase we would need to implement. Note that we could estimate ϕ through phase estimation.

2. **Gottesman Knill**.

   (a) We first show that Hadamards and phase gates can be used to perform any single-qubit normalizer operation where $UZU^\dagger = Z$. For this to be true, U must have only diagonal terms, so to within an arbitrary phase:

$$U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

We also know that for U to be a normalizer

$$UXU^\dagger = \begin{pmatrix} 0 & e^{-i\phi} \\ e^{i\phi} & 0 \end{pmatrix} = \pm X, \pm Y$$

Therefore, $e^{i\phi} = \pm 1, \pm i$, so U is some product of phase gates to within a global phase.

Lemma: Given any Pauli operator g, there is some product of Hadamards and phase gates N s.t. $NgN^\dagger = Z$.

Given any single-qubit unitary in the normalizer subgroup U, there exists some element g of the Pauli group s.t. $UgU^\dagger = Z$. Using the lemma, we may write $U = VN$, so $UgU^\dagger = VNgN^\dagger V^\dagger = VZV^\dagger = Z$. Therefore, since V must be some product of phase gates and N is some product of Hadamards and phase gates, $U = VN$ is some product of Hadamards and phase gates.

Therefore, Hadamard and phase gates can be used to perform any normalizer operation on a single qubit

(b) The circuit applies a unitary operation $\bar{U}$ which we want to prove is equal to U. To do so, we show case by case that $\langle\sigma|\bar{U}|\gamma\rangle \otimes |\psi\rangle = \langle\sigma|U|\gamma\rangle \otimes |\psi\rangle \; \forall \sigma, \gamma, |\psi\rangle$, which then shows that $\bar{U} = U$. To do so, we use a few identities

$$UZ_1 = X_1 \otimes g \cdot U, X_1 U = g \cdot UZ_1$$
$$UX_1 = Z_1 \otimes g' \cdot U, Z_1 U = g' \cdot UX_1$$

$$\bar{U}Z_1 = X_1 \otimes g \cdot \bar{U}, X_1 \bar{U} = g \cdot \bar{U}Z_1$$
$$\bar{U}X_1 = Z_1 \otimes g' \cdot \bar{U}, Z_1 \bar{U} = g' \cdot \bar{U}X_1$$

We use these to come up with a few alternate definitions of U':

$$\begin{aligned} U'|\psi\rangle = \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle) = \\ \sqrt{2}\langle 0|g' \cdot U(|1\rangle \otimes |\psi\rangle) = \\ \sqrt{2}\langle 1|g \cdot U(|0\rangle \otimes |\psi\rangle) = \\ -\sqrt{2}\langle 1|g \cdot g' \cdot U(|1\rangle \otimes |\psi\rangle) \end{aligned}$$

First,

$$\begin{aligned} \langle 0|\bar{U}(|0\rangle \otimes |\psi\rangle) &= \langle 0|\frac{1}{\sqrt{2}}(|0\rangle \otimes U'|\psi\rangle + |1\rangle \otimes gU'|\psi\rangle) \\ &= \frac{1}{\sqrt{2}}U'|\psi\rangle = \langle 0|U(|0\rangle \otimes |\psi\rangle) \end{aligned}$$

likewise,

$$\begin{aligned} \langle 0|\bar{U}(|1\rangle \otimes |\psi\rangle) &= \langle 0|\frac{1}{\sqrt{2}}(|0\rangle \otimes g' \cdot U'|\psi\rangle - |1\rangle \otimes g \cdot g'U'|\psi\rangle) \\ &= \frac{1}{\sqrt{2}}g'U'|\psi\rangle = \langle 0|g'g'U(|1\rangle \otimes |\psi\rangle) = \langle 0|U(|1\rangle \otimes |\psi\rangle) \end{aligned}$$

likewise,

$$\langle 1|\,\bar{U}\,(|0\rangle\otimes|\psi\rangle) = \langle 1|\,\frac{1}{\sqrt{2}}\,(|0\rangle\otimes U'\,|\psi\rangle + |1\rangle\otimes gU'\,|\psi\rangle) =$$

$$\frac{1}{\sqrt{2}}\,(gU'\,|\psi\rangle) = \langle 1|\,ggU\,(|0\rangle\otimes|\psi\rangle) = \langle 1|\,U\,(|0\rangle\otimes|\psi\rangle)$$

and lastly,

$$\langle 1|\,\bar{U}\,(|1\rangle\otimes|\psi\rangle) = \langle 1|\,\frac{1}{\sqrt{2}}\,(|0\rangle\otimes g'\cdot U'\,|\psi\rangle - |1\rangle\otimes g'\cdot gU'\,|\psi\rangle) =$$

$$-\frac{1}{\sqrt{2}}\,(g'\cdot gU'\,|\psi\rangle) = \langle 1|\,gg'g'gU\,(|1\rangle\otimes|\psi\rangle) = \langle 1|\,\bar{U}\,(|1\rangle\otimes|\psi\rangle)\,.$$

Since $\langle\sigma|\,\bar{U}\,|\gamma\rangle\otimes|\psi\rangle = \langle\sigma|\,U\,|\gamma\rangle\otimes|\psi\rangle\,\forall\sigma,\gamma,|\psi\rangle$, $\bar{U}=U$, and we have therefore performed the desired unitary.

We write $U = V\cdot U'$ where V, the unitary described by all of the circuit except for U':

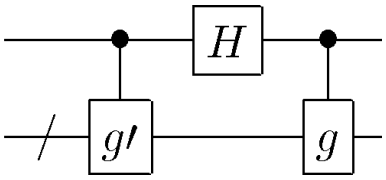


FIG. 3. Circuit which describes the unitary V

is in the normalizer subgroup. Therefore, $U' = V^\dagger\cdot U$ is an n-qubit gate in the normalizer subgroup. We can see from the circuit that constructing a gate in $N(G_{n+1})$ requires the construction of a gate in $N(G_n)$, followed by $O(n)$ gates. Therefore, inductively it takes $\sum_{i=1}^{n} O(i) = O(n^2)$ gates to construct U.

(c) The above procedure only works when $UZ_1U^\dagger = X_1\otimes g$, $UX_1U^\dagger = Z_1\otimes g'$, so we must show how to extend the procedure to work on arbitrary elements of the normalizer group. Given an arbitrary normalizer U, we write $UZ_1U^\dagger = G$, $UX_1U^\dagger = G'$, where G, G' are $n+1$-qubit elements of the Pauli group. G, G' must anticommute, so looking at the entries of G, G', there must be some qubit j where the entries of G, G' are different Pauli matrices σ,σ'. Therefore, applying the swap gate(which is in the normalizer subgroup) between qubits 1,j:

$$\mathbf{SWAP}_{1j}\cdot U\cdot Z_1\,(\mathbf{SWAP}_{1j}\cdot U)^\dagger = \mathbf{SWAP}_{1j}^\dagger\cdot G\cdot\mathbf{SWAP}_{1j}^\dagger = \sigma_1\otimes g$$

$$\mathbf{SWAP}_{1j}\cdot U\cdot X_1\,(\mathbf{SWAP}_{1j}\cdot U)^\dagger = \mathbf{SWAP}_{1j}^\dagger\cdot G'\cdot\mathbf{SWAP}_{1j}^\dagger = \sigma_1'\otimes g'$$

Lemma: Given any two different Pauli matrices $\sigma\neq\sigma'$, there is some product of Hadamards and phase gates N s.t. $N\sigma N^\dagger = X, N\sigma, N^\dagger = Z$. Therefore,

$$N\cdot\mathbf{SWAP}_{1j}\cdot U\cdot Z_1\,(N\cdot\mathbf{SWAP}_{1j}\cdot U)^\dagger = X_1\otimes g,$$
$$N\cdot\mathbf{SWAP}_{1j}\cdot U\cdot X_1\,(N\cdot\mathbf{SWAP}_{1j}\cdot U)^\dagger = Z_1\otimes g',$$

and to apply any unitary U in the normalizer group, we first apply $N \cdot \mathbf{SWAP}_{1j} \cdot U$ through the procedure in part b), and then apply $(N \cdot \mathbf{SWAP}_{1j})^\dagger$. Doing this procedure takes $\sum_{i=1}^{n} O(i) = O(n^2)$ gates.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT 2.111/8.411/6.898/18.435
Quantum Information Science I

October 21, 2010

Problem Set #6
(due in class, 28-Oct-10)

1. **Building controlled-U from U.**

   Suppose you are given a box which performs a unitary gate U on a one-qubit input state. In addition, you are given $|u\rangle$, and eigenstate of U with eigenvalue one.

   (a) Provide a quantum circuit using quantum Fredkin (ie controlled-swap) gates, which peforms a controlled-U gate, using this box, and $|u\rangle$.

   (b) Can you use the same approach if $|u\rangle$ has some known eigenvalue $e^{i\phi}$?

   (c) What if ϕ is unknown?

2. **The Gottesman-Knill Theorem**. An important result in quantum computation is that H, CNOT, and the Pauli gates are not universal for quantum computation, and in fact any quantum circuit composed from those gates (together with standard input states and measurements in the computational basis) can be simulated efficiently by a classical computer! This result is known as the *Gottesman-Knill* theorem, and in this problem we prove the essential result behind the theorem.

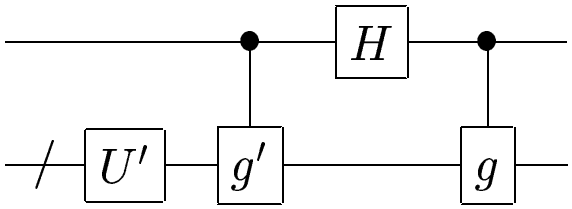
   Let G_n denote the Pauli group on n qubits, that is, matrix multiplication acting on the set of n-fold tensor products of Pauli matrices (including multiplicative factors $\pm 1, \pm i$). By definition, we say the set of U such that $UG_nU^\dagger = G_n$ is the *normalizer* of G_n, and denote it by $N(G_n)$. The following theorem about the normalizer of the Pauli group holds:

   > Suppose U is any unitary operator on n qubits with the property that if $g \in G_n$ then $UgU^\dagger \in G_n$. Then up to a global phase U may be composed from $O(n^2)$ Hadamard, phase and controlled-NOT gates.

   We can construct an inductive proof of this theorem as follows:

   (a) Prove that the Hadamard and phase gates (H and S) can be used to perform any normalizer operation on a single qubit.

   (b) Suppose U is an $n+1$ qubit gate in $N(G_{n+1})$ such that $UZ_1U^\dagger = X_1 \otimes g$ and $UX_1U^\dagger = Z_1 \otimes g'$ for some $g, g' \in G_n$. Define U' on n qubits by $U'|\psi\rangle \equiv \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle)$. Use the inductive hypothesis to show that this construction for U:

   may be implemented using $O(n^2)$ Hadamard, phase and controlled-NOT gates.

   (c) Show that any gate $U \in N(G_{n+1})$ may be implemented using $O(n^2)$ Hadamard, phase and controlled-NOT gates.