CS 593/MA 595 - Introduction to Quantum Computing

Quantum Computation and Quantum Information by *Isaac Chuang, Michael Nielsen*
Student: **Ralph Razzouk**

Homework 5

Problem 4.50
Let $H = \sum_k^L H_k$, and define

$$U_{\Delta t} = \left[e^{-iH_1\Delta t}e^{-iH_2\Delta t}\cdots e^{-iH_L\Delta t}\right]\left[e^{-iH_L\Delta t}e^{-iH_{L-1}\Delta t}\cdots e^{-iH_1\Delta t}\right].$$

(a) Prove that $U_{\Delta t} = e^{-2iH\Delta t} + O(\Delta t^3)$.

(b) Use the results in Box 4.1 to prove that, for a positive integer m,

$$E\left(U_{\Delta t}^m, e^{-2miH\Delta t}\right) \leq m\alpha\Delta t^3,$$

for some constant α.

Proof. (a) We have $H = \sum_k^L H_k$. The Baker-Campbell-Hausdorf formula states that

$$\mathrm{e}^{(A+B)\Delta t} = \mathrm{e}^{A\Delta t}\mathrm{e}^{B\Delta t}\mathrm{e}^{-\frac{1}{2}[A,B]\Delta t^2} + O(\Delta t^3).$$

By repeated application of the Baker-Campbell-Hausdorf formula, knowing that $[H_i, H_i] = 0$, we have

$$\begin{aligned}
U_{\Delta t} &= \left[e^{-iH_1\Delta t}\cdots e^{-iH_L\Delta t}\right]\left[e^{-iH_L\Delta t}\cdots e^{-iH_1\Delta t}\right]\\
&= \left[e^{-iH_1\Delta t}\cdots e^{-iH_{L-1}\Delta t}\right]e^{-2iH_L\Delta t}\left[e^{-iH_{L-1}\Delta t}\cdots e^{-iH_1\Delta t}\right] + O(\Delta t^3)\\
&= \left[e^{-iH_1\Delta t}\cdots e^{-iH_{L-2}\Delta t}\right]e^{-2i(H_L+H_{L-1})\Delta t}\left[e^{-iH_{L-2}\Delta t}\cdots e^{-iH_1\Delta t}\right] + O(\Delta t^3)\\
&= e^{-2iH\Delta t} + O(\Delta t^3).
\end{aligned}$$

(b) We have

$$\begin{aligned}
E\left(U_{\Delta t}^m, e^{-2miH\Delta t}\right) &\leq mE\left(U_{\Delta t}, e^{-2iH\Delta t}\right)\\
&= m||\left(U_{\Delta t} - e^{-2iH\Delta t}\right)|\psi\rangle||\\
&= m||O(\Delta t^3)|\psi\rangle||\\
&= m\alpha\Delta t^3.
\end{aligned}$$

■

Problem 4.1
(Computable phase shifts) Let m and n be positive integers. Suppose $f : \{0,\ldots,2m-1\} \to \{0,\ldots,2n-1\}$ is a classical function from m to n bits which may be computed reversibly using T Toffoli gates, as described in Section 3.2.5. That is, the function $(x,y) \to (x, y\oplus f(x))$ may be implemented using T Toffoli gates. Give a quantum circuit using $2T+n$ (or fewer) one, two, and three qubit gates to implement the unitary operation defined by

$$|x\rangle \to \exp\left(\frac{-2\mathrm{i}\pi f(x)}{2^n}\right)|x\rangle.$$

Proof. We first need to compute $\hat{P}\left|x,y\right\rangle \equiv \left|x, y\oplus f(x)\right\rangle$ using T Toffoli gates. Then we expand $q = \sum_{j=0}^{n-1} q_j 2^j$ with q_j being the digits of a binary representation of $0 \leq q \leq 2^{n-1}$. Observe that

$$\begin{aligned}\hat{O}\left|x,q\right\rangle &\equiv \mathrm{e}^{\frac{2\pi \mathrm{i} yn}{2^n}} \prod_{j=0}^{n-1} \mathrm{e}^{-\pi \mathrm{i} q_j 2^{j-n+1}} \left|x,q\right\rangle \\ &= \mathrm{e}^{-\frac{2\pi\mathrm{i}}{2^n}\left(\sum_{j=0}^{n-1} q_j 2^j - y\right)} \left|x,q\right\rangle \\ &= \mathrm{e}^{-\frac{2\pi\mathrm{i}}{2^n}(q-y)} \left|x,q\right\rangle .\end{aligned}$$

For $q = y \oplus f(x)$, we obtain

$$\hat{O}\left|x, y\oplus f(x)\right\rangle = \mathrm{e}^{-\frac{2\pi\mathrm{i}}{2^n} f(x)} \left|x, y\oplus f(x)\right\rangle .$$

The operation $\prod_{j=0}^{n-1} \mathrm{e}^{-\pi\mathrm{i} q_j 2^{j-n+1}}$ can be implemented using n single-qubit phase gates $\hat{U}_{n-1}\cdots\hat{U}_0$, each acting as

$$\hat{U}_j = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{-\pi\mathrm{i}2^{j-n+1}} \end{pmatrix},$$

while the y-dependent phase can be neglected.
Finally, we uncompute $P^\dagger \left|x, y\oplus f(x)\right\rangle = \left|x,y\right\rangle$ using T Toffoli gates.
The total cost of the operation $\hat{P}^\dagger \hat{O} \hat{P}$, and therefore requires $2T + n$ gates, as required. ■

Problem 3
Show that if A is a finite abelian group, then the dual group $\widehat{A} \cong A$. [Hint: do it in two steps. First, use the fact that every finite abelian group A is a direct sum of cyclic groups to reduce to the case that $A = \mathbb{Z}/N\mathbb{Z}$. Then argue however you want that $\widehat{\mathbb{Z}/N\mathbb{Z}}$ is a cyclic group of order N.]

Before I start my proof of this, I will state the definition of a **character** (since it wasn't done in class).

Definition 1. Let V be a finite-dimensional vector space over a field F and let $\rho : G \to \mathrm{GL}(V)$ be a representation of a group G on V. The **character** of ρ is the function $\chi_\rho : G \to F$ given by

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)),$$

where Tr is the trace.

Proof. This proposition is known as the self-duality of finite Abelian groups. The weak fundamental theorem of group theory states that, if G is a finite Abelian group, then either G is cyclic or $G \cong H \times K$ for non-trivial groups H and K. These two possibilities are not mutually exclusive, since, for example, $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. Since G is a finite Abelian group, then $|G| < \infty$, on which we perform induction.

- For $|G| = 1$, this is trivially true.
- For $|G| > 1$, since G is a finite Abelian group, then either G is cyclic or $G \cong H \times K$ for non-trivial groups H and K
  - If G is a cyclic group, we need to prove that $G \cong \widehat{G}$. We can assume without loss of generality that $G = \mathbb{Z}/N\mathbb{Z}$. A character $\chi \in \widehat{G}$ is determined by what it does to the generator $1 \in \mathbb{Z}/N\mathbb{Z}$. Furthermore, since $\chi(N) = \chi(1)^N$ and $N = 0$ in $\mathbb{Z}/N\mathbb{Z}$, then $\chi(1)^N = 1$. In fact, choose a Nth root of unity and assign it to $\chi(1)$. Define $\mathrm{e}(t) = \mathrm{e}^{2\pi\mathrm{i}t}$, then the Nth roots of unity are of the form $\mathrm{e}\left(\frac{a}{N}\right)$, with $a \in \mathbb{Z}/N\mathbb{Z}$. Define χ_a by

    $$\chi_a(x) = \mathrm{e}\left(\frac{ax}{N}\right).$$

    We can verify that χ_a is a character on $\mathbb{Z}/N\mathbb{Z}$, and that $\chi_a(1) = \mathrm{e}\left(\frac{a}{N}\right)$. Hence, the set $\{\chi_a : a \in \mathbb{Z}/N\mathbb{Z}\}$ is all of $\widehat{G}$. Finally, we can also verify that the map $a \mapsto \chi_a$ is a bijective homomorphism. Therefore, $G \cong \widehat{G}$

- If $G = H \times K$, then let $\chi \in \widehat{G}$ and define $\nu \in H$ and $\eta \in K$ by $\nu(h) = \chi(h, 1)$ and $\eta(k) = \chi(1, k)$. Let $\nu \in H$ and $\eta \in K$. Define $\chi \in G$ by $\chi(h, k) = \nu(h)\eta(k)$. Then the maps $\chi \mapsto (\nu, \eta)$ and $(\nu, \eta) \mapsto \chi$ described are inverses of each other and are both homomorphisms. Thus, $G \cong H \times K \implies \widehat{G} \cong \widehat{H} \times \widehat{K}$. Since G is finite, then we have that $1 < |H|, |K| < |G|$, and by strong induction, we have $H \cong \widehat{H}$ and $K \cong \widehat{K}$. Thus $H \times K \cong \widehat{H} \times \widehat{K}$. Therefore, $G \cong \widehat{G}$.

■

Problem 5.6
(Approximate quantum Fourier transform) The quantum circuit construction of the quantum Fourier transform apparently requires gates of exponential precision in the number of qubits used. However, such precision is never required in any quantum circuit of polynomial size. For example, let U be the ideal quantum Fourier transform on n qubits, and V be the transform which results if the controlled-R_k gates are performed to a precision $\Delta = 1/p(n)$ for some polynomial $p(n)$. Show that the error $E(U, V) \equiv \max_{|\psi\rangle} ||(U - V)|\psi\rangle||$ scales as $\Theta(n^2/p(n))$, and thus polynomial precision in each gate is sufficient to guarantee polynomial accuracy in the output state.

Proof. In the quantum Fourier transform circuit of n qubits, we have $m = \frac{n(n+1)}{2} = \Theta(n^2)$ controlled-R_k gates. We are given that each approximation of the ideal transform is performed to a precision of $\Delta = \frac{1}{p(n)}$. Thus, $E(U, V) \leq m\Delta = \Theta\left(\frac{n^2}{p(n)}\right)$. ■

Problem 5.8
Suppose the phase estimation algorithm takes the state $|0\rangle|u\rangle$ to the state $|\widetilde{\varphi_u}\rangle|u\rangle$, so that given the input $|0\rangle\left(\sum_u c_u|u\rangle\right)$, the algorithm outputs $\sum_u c_u|\widetilde{\varphi_u}\rangle|u\rangle$. Show that if t is chosen according to (5.35), then the probability for measuring φ_u accurate to n bits at the conclusion of the phase estimation algorithm is at least $|c_u|^2(1 - \epsilon)$.

Proof. We measure φ of the state $|u\rangle$ with a probability of $|c_u|^2$. If t is of the form of (5.35), then each $\widehat{\varphi}$ is accurate to φ up to n bits with probability $1 - \epsilon$. Thus, the total probability of measuring φ up to n bits is $|c_u|^2(1 - \epsilon)$. ■