Ph219/CS219: Quantum Computation

Winter 2006

Solutions to Problem Set 7

Problem 7.1

a) Let us choose $c\sqrt{N}$ distinct inputs x_i at random, where c is a constant. For each of these inputs, we can compute $f(x_i)$ and store the $c\sqrt{N}$ pairs $(x_i, f(x_i))$ in memory. This requires space $O(\sqrt{N})$ and can be accomplished with $O(\sqrt{N})$ oracle queries. We will now compute the probability that we will fail to find a single collision among these $c\sqrt{N}$ randomly chosen inputs.

We first pick the input x_1. Let A_2 denote the event that the second input x_2 does not collide with x_1 (i.e., $f(x_1) \neq f(x_2)$). Its probability is

$$P(A_2) = \sum_{x_1} P(x_1)P(A_2|x_1) = N\frac{1}{N}\frac{N-1}{N} = \frac{N-1}{N} \; . \tag{1}$$

Similarly, let A_3 be the event that there is no collision among x_1, x_2 and our third input x_3. Then

$$P(A_3) = P(A_3|A_2)P(A_2) = \frac{N-2}{N}\frac{N-1}{N} \; . \tag{2}$$

After choosing k distinct inputs x_i, the probability that we will fail to find a single collision is

$$\begin{aligned} P(A_k) &= P(A_k|A_{k-1})P(A_{k-1}|A_{k-2})\cdots P(A_3|A_2)P(A_2) \\ &= \left(1-\tfrac{k-1}{N}\right)\left(1-\tfrac{k-2}{N}\right)\cdots\left(1-\tfrac{2}{N}\right)\left(1-\tfrac{1}{N}\right) \\ &\leq exp\left(-\tfrac{1}{N}\textstyle\sum_{i=1}^{k-1} i\right) \\ &= exp\left(-\tfrac{k(k-1)}{2N}\right) \; . \end{aligned} \tag{3}$$

where we used that $1+x \leq e^x$.

Substituting $k = c\sqrt{N}$ and since $N >> 1$, Eq. (3) gives for the probability of failure to find a collision after $c\sqrt{N}$ queries, $P(A_k) \leq e^{-c^2/2}$. Thus we can upper bound the failure probability by any constant $0 < \delta \leq 1$ by choosing c to be sufficiently large.

b) We now choose $cN^{1/3}$ distinct inputs x_i at random for some constant c. We compute again $f(x_i)$ for all of them and store the $cN^{1/3}$ pairs $(x_i, f(x_i))$ as before.

This requires space $O(N^{1/3})$ and also $O(N^{1/3})$ oracle queries. Let $X = \bigcup_i \{x_i\}$. We can check whether there is a collision within X and declare success if we find one. If we are unsuccessful, we know that every $x_i \in X$ collides with a unique $y \in S \setminus X$, where $S = \{0,1\}^n$ is the total input space.

We define a new function $g : S \setminus X \to \{0,1\}$ such that $g(y) = 1$ if $f(y) = f(x)$ for some $x \in X$ and $g(y) = 0$ otherwise. Thus g takes the value 1 at exactly $|X| = cN^{1/3}$ inputs and our goal is to find one such input. This can be done in $O(N^{2/3})$ queries since g is defined in $|S \setminus X| < N$ inputs and has $O(N^{1/3})$ marked inputs (i.e., inputs for which g takes the value 1). In more detail, the probability that after k trials $y_i \in S \setminus X$ we will fail to find a single collision is

$$P_{\text{fail}} = \left(\frac{|S \setminus X| - |X|}{|S \setminus X|} \right)^k \leq exp\left(\frac{-k|X|}{|S \setminus X|} \right) . \tag{4}$$

Since $|S \setminus X| = N - cN^{1/3}$ and taking $N >> 1$, the failure probability can be made smaller than any constant $0 < \delta \leq 1$ by making $k = c' N^{2/3}$ for some constant c' large enough.

Overall, we succeed with high probability using $k + cN^{1/3} = O(N^{2/3})$ oracle queries and space $O(N^{1/3})$.

c) We first pick a random input $x_0 \in S$. Then we can consider the new function $h : S \setminus \{x_0\} \to \{0,1\}$ such that $h(y) = 1$ if $f(y) = f(x_0)$ and $h(y) = 0$ otherwise. Using Grover's algorithm for the function h, we can find a collision (i.e., the unique y such that $f(y) = f(x_0)$) in $O(\sqrt{N})$ oracle queries using space $O(1)$ since we just need to store the pair $(x_0, f(x_0))$.

d) We now choose M distinct inputs x_i at random and compute the M pairs $(x_i, f(x_i))$ as before. This requires space $O(M)$ and also $O(M)$ oracle queries. Using the function g of part (b), we can perform Grover's algorithm to find one of the M marked inputs of g in $O(\sqrt{N/M})$ oracle queries with high probability. We then query the oracle one additional time to learn the value of f for this input and compare with the M pairs $(x_i, f(x_i))$ to find the x_i with which it collides. Overall, choosing $M = N^{1/3}$, we can find a collision using space $O(N^{1/3})$ and oracle queries $O(N^{1/3} + \sqrt{N/N^{1/3}}) = O(N^{1/3})$.

Problem 7.2

a) After k queries, the probability of success is

$$P_{\text{success}} \leq \left(\frac{1}{2} \right)^{N-k} , \tag{5}$$

since we have only 1/2 probability to guess the value of the function at the remaining $N-k$ inputs correctly. Thus, the success probability is greater than 2/3 only for $k=N$.

b) We note that

$$H^{\otimes N}|X\rangle = \frac{1}{\sqrt{2^N}} \sum_{Y\in\{0,1\}^N} (-1)^{X\cdot Y}|Y\rangle = |\Psi_{X,N}\rangle \ . \tag{6}$$

Thus, $H^{\otimes N}|\Psi_{X,N}\rangle = |X\rangle$, which implies that we can find X by applying N transversal Hadamard gates on $|\Psi_{X,N}\rangle$ and then measure each qubit in the computation basis.

c) First, recall that we can use the oracle to perform the operation $|i\rangle \to (-1)^{f(i)}|i\rangle$ where $i \in \{0,1\}^n$. Indeed, this is possible if we use the input state $|i\rangle \otimes |-\rangle$ on the standard oracle $\Lambda(f) : |i\rangle \otimes |y\rangle \to |i\rangle \otimes |y \oplus f(i)\rangle$ where $i \in \{0,1\}^n$and $y \in \{0,1\}$.

Now, consider the N-bit input $Y = Y_{N-1}Y_{N-2}\cdots Y_0$. We can control from each bit Y_k the oracle acting on the corresponding n-bit input that is encoded by k, i.e. the n-bit input $x_{n-1}x_{n-2}\cdots x_0$ such that $\sum_{a=0}^{n-1} x_a 2^a = k$. This will multiply $|Y\rangle$ with the phase $\Pi_{i=0}^{N-1}(-1)^{f(i)\cdot Y_i} = (-1)^{X\cdot Y}$. The oracle is thus queried only $|Y|$ times, and since the computation is reversible we can also use it with inputs in superposition.

d) We can write $|\Psi_{X,K}\rangle = \alpha|\Psi_{X,N}\rangle + \beta|E\rangle$ where $\langle E|\Psi_{X,N}\rangle = 0$. From part (b), applying $H^{\otimes N}$ on $|\Psi_{X,N}\rangle$ and measuring in the computation basis will give the correct answer for X. Therefore, if we apply $H^{\otimes N}$ on $|\Psi_{X,K}\rangle$ and measure, we will obtain X with success probability

$$P_{\text{success}} = |\langle\Psi_{X,N}|\Psi_{X,K}\rangle|^2 = \frac{1}{2^N M_K}\left(\sum_{Y:|Y|\le K} 1\right)^2 = \frac{M_K^2}{2^N M_K} = \frac{M_K}{2^N} \ . \tag{7}$$

e) We calculate

$$1 - P_{\text{success}} = 1 - \frac{M_K}{2^N} = 1 - \frac{1}{2^N}\sum_{j=0}^{K}\binom{N}{j} = P(j > K) \ , \tag{8}$$

where the last equality follows if we consider the binomially distributed random variable j with mean $p = 1/2$ such that $P(j) = \binom{N}{j}\left(\frac{1}{2}\right)^j\left(\frac{1}{2}\right)^{N-j} = \frac{1}{2^N}\binom{N}{j}$.

For large N, $P(j)$ is well approximated by a Gaussian with mean $N/2$ and standard deviation $\sigma = \sqrt{N}/2$. Therefore

$$1 - P_{\text{success}} = P(j > K) \approx \int_K^\infty P(j)dj = \frac{1}{\sqrt{\pi}}\int_{\frac{K-N/2}{\sqrt{N/2}}}^\infty e^{-j^2} dj \ . \tag{9}$$

Taking $K = N/2 + c\sqrt{N}$ we obtain

$$1 - P_{\text{success}} \approx \frac{1}{\sqrt{\pi}} \int_{\sqrt{2}c}^{\infty} e^{-j^2} dj = \frac{1 - erf(\sqrt{2}c)}{2} = O(e^{-2c^2}) \ . \tag{10}$$

Problem 7.3

a) This construction is similar to that in Problem 5.3(b). The only difference is that the oracle implements here a n-qubit unitary U. Therefore we need to attach n ancilla qubits and use n transversal $\Lambda(\text{SWAP})$ gates to swap each qubit of the target with the corresponding ancilla qubit.

b) We can use a m-bit register for t such that $t = \sum_{k=0}^{m-1} t_k 2^k$. Now we control from the k-th bit the unitary $(U_{\text{Grover}})^{2^k}$. Overall, we use $2^0 + 2^1 + 2^2 + \cdots + 2^{m-1} = 2^m - 1 = T - 1$ oracle queries.

c) We start with a uniform superposition over all counter values and all input values,

$$|\Psi_{\text{initial}}\rangle = \frac{1}{\sqrt{T}} \sum_{t=0}^{T-1} |t\rangle \otimes \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \ . \tag{11}$$

We then apply V to obtain the state

$$V|\Psi_{\text{initial}}\rangle = \frac{1}{\sqrt{T}} \sum_{t=0}^{T-1} |t\rangle \otimes \Big(cos((2t+1)\theta)|\Psi_X^{\perp}\rangle + sin((2t+1)\theta)|\Psi_X\rangle \Big) \ , \tag{12}$$

since the initial state $|s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle = cos(\theta)|\Psi_X^{\perp}\rangle + sin(\theta)|\Psi_X\rangle$ and each Grover iteration rotates $|s\rangle$ closer to $|\Psi_X\rangle$ by an angle 2θ.

Finally, we want to apply the QFT on the counter register and then measure in the computation basis. Applying the QFT on $V|\Psi_{\text{initial}}\rangle$ produces

$$\begin{aligned} |\Psi_{\text{QFT}}\rangle &= \tfrac{1}{T} \sum_{t=0}^{T-1} \sum_{l=0}^{T-1} e^{i2\pi lt/T} |l\rangle \otimes \big(cos((2t+1)\theta)|\Psi_X^{\perp}\rangle + sin((2t+1)\theta)|\Psi_X\rangle \big) \\ &= \tfrac{1}{T} \sum_{l=0}^{T-1} |l\rangle \otimes \big(\tfrac{a+b}{2} |\Psi_X^{\perp}\rangle + \tfrac{a-b}{2i} |\Psi_X\rangle \big) \ , \end{aligned} \tag{13}$$

where $a = \sum_{t=0}^{T-1} e^{i2\pi(l + \frac{T\theta}{\pi})t/T + i\theta}$, $b = \sum_{t=0}^{T-1} e^{i2\pi(l - \frac{T\theta}{\pi})t/T - i\theta}$.

Therefore, the probability of measuring the outcome l is given by

$$P(l) = \frac{1}{4T^2} \left(|a+b|^2 + |a-b|^2 \right) = \frac{1}{2T^2} \left(|a|^2 + |b|^2 \right) \ . \tag{14}$$

Consider first the case when $T\theta/\pi \in \mathbb{Z}$. Then, the only values of l that survive in Eq. (13) are $l = \pm T\theta/\pi$ since $a = T\delta_{l,-T\theta/\pi}$ and $b = T\delta_{l,T\theta/\pi}$. Measuring the counter in the computation basis will therefore yield the integers $T\theta/\pi$ or $T - T\theta/\pi$ with equal probability 1/2, from which we can learn θ with accuracy $O(1/T)$.

However, in general $T\theta/\pi \notin \mathbb{Z}$. Consider first the case $0 < T\theta/\pi < 1$. Then, for $0 < T\theta/\pi \leq 1/2$, success means measuring $l = 0$ which is the closest integer to $T\theta/\pi$ and we have

$$P(l=0) = \frac{1}{2T^2}\left(|a_{\,l=0}|^2 + |b_{\,l=0}|^2\right) \geq \frac{1}{2T^2}\left(\left(T\frac{2}{\pi}\right)^2 + \left(T\frac{2}{\pi}\right)^2\right) = \frac{4}{\pi^2}\ , \qquad (15)$$

since[1] $|a_{\,l=0}| = \left|\frac{e^{i2T\theta}-1}{e^{2\theta}-1}\right| \geq \frac{2\frac{2T\theta}{\pi}}{2\theta} = T\frac{2}{\pi}$, and $|b_{\,l=0}| = \left|\frac{e^{-i2T\theta}-1}{e^{-2\theta}-1}\right| = |a_{\,l=0}|$. When $1/2 < T\theta/\pi < 1$, success means measuring $l = \pm 1$ (i.e., $l = 1$ or $l = T-1 = -1\ (\mathrm{mod}T)$) since 1 is now the closest integer to $T\theta/\pi$. We calculate

$$\begin{aligned} P(l=1) &= \tfrac{1}{2T^2}\left(|a_{\,l=1}|^2 + |b_{\,l=1}|^2\right) \geq \tfrac{|b_{\,l=1}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \\ P(l=T-1) &= \tfrac{1}{2T^2}\left(|a_{\,l=T-1}|^2 + |b_{\,l=T-1}|^2\right) \geq \tfrac{|a_{\,l=T-1}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \end{aligned} \qquad (16)$$

since $|b_{\,l=1}| = \left|\frac{e^{-i2T\theta}-1}{e^{i(-2\theta+2\pi/T)}-1}\right| \geq \frac{2\frac{2\pi-2T\theta}{\pi}}{2\pi/T-2\theta} = T\frac{2}{\pi}$, and $|a_{\,l=T-1}| = \left|\frac{e^{i2T\theta}-1}{e^{i(2\theta-2\pi/T)}-1}\right| = |b_{\,l=1}|$. Therefore, the success probability is again lower bounded by $4/\pi^2$.

The second case is when $1 < T\theta/\pi < \frac{T}{2} - 1$. Let $f^- = \left\lfloor\frac{T\theta}{\pi}\right\rfloor$ and $f^+ = \left\lceil\frac{T\theta}{\pi}\right\rceil$. Then, if $\frac{T\theta}{\pi} - f^- \leq \frac{1}{2}$, success means measuring $l = \pm f^-$ (i.e., $l = f^-$ or $l = T - f^-$), and we can calculate

$$\begin{aligned} P(l=f^-) &= \tfrac{1}{2T^2}\left(|a_{\,l=f^-}|^2 + |b_{\,l=f^-}|^2\right) \geq \tfrac{|b_{\,l=f^-}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \\ P(l=T-f^-) &= \tfrac{1}{2T^2}\left(|a_{\,l=T-f^-}|^2 + |b_{\,l=T-f^-}|^2\right) \geq \tfrac{|a_{\,l=T-f^-}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \end{aligned} \qquad (17)$$

since, defining $\phi = \frac{T\theta}{\pi} - f^-$, $|b_{\,l=f^-}| = \left|\frac{e^{-i2\pi\phi}-1}{e^{-i2\pi\phi/T}-1}\right| \geq \frac{2\frac{2\pi\phi}{\pi}}{2\pi\phi/T} = T\frac{2}{\pi}$, and $|a_{\,l=T-f^-}| = \left|\frac{e^{i2\pi\phi}-1}{e^{i2\pi\phi/T}-1}\right| = |b_{\,l=f^-}|$. When $f^+ - \frac{T\theta}{\pi} < \frac{1}{2}$, success means measuring $l = \pm f^+$ (i.e., $l = f^+$ or $l = T - f^+$), and we have

$$\begin{aligned} P(l=f^+) &= \tfrac{1}{2T^2}\left(|a_{\,l=f^+}|^2 + |b_{\,l=f^+}|^2\right) \geq \tfrac{|b_{\,l=f^+}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \\ P(l=T-f^+) &= \tfrac{1}{2T^2}\left(|a_{\,l=T-f^+}|^2 + |b_{\,l=T-f^+}|^2\right) \geq \tfrac{|a_{\,l=T-f^+}|^2}{2T^2} \geq \tfrac{2}{\pi^2}\ , \end{aligned} \qquad (18)$$

since, defining now $\phi' = f^+ - \frac{T\theta}{\pi}$, $|b_{\,l=f^+}| = \left|\frac{e^{i2\pi\phi'}-1}{e^{i2\pi\phi'/T}-1}\right| \geq T\frac{2}{\pi}$ and $|a_{\,l=T-f^+}| = \left|\frac{e^{-i2\pi\phi'}-1}{e^{-i2\pi\phi'/T}-1}\right| = |b_{\,l=f^+}|$. The success probability is again lower bounded by $4/\pi^2$.

[1]In what follows we make repetitive use of the bounds (a) $|e^{\phi} - 1| \leq |\phi|$ for $|\phi| << 1$, and (b) $|e^{i\phi} - 1| \geq 2\frac{\phi}{\pi}$ for $|\phi| \leq \pi$.

The final case is when $\frac{T}{2}-1 < T\theta/\pi < \frac{T}{2}$. First, for $T\theta/\pi - \left(\frac{T}{2}-1\right) \le \frac{1}{2}$, success means measuring $l = \pm\frac{T}{2}-1$ (i.e., $l = \frac{T}{2}-1$ or $l = \frac{T}{2}+1$). Setting $f^- = \frac{T}{2}-1$, it follows from Eq. (17) that the success probability is at least $4/\pi^2$. For $\frac{T}{2} - T\theta/\pi < \frac{1}{2}$, success means measuring $l = \frac{T}{2}$. We can calculate

$$P(l = T/2) = \frac{1}{2T^2}\left(|a_{l=\frac{T}{2}}|^2 + |b_{l=\frac{T}{2}}|^2\right) \ge \frac{1}{2T^2}\left(\left(T\frac{2}{\pi}\right)^2 + \left(T\frac{2}{\pi}\right)^2\right) = \frac{4}{\pi^2}\ , \quad (19)$$

since, defining $\phi''' = \frac{T}{2} - \frac{T\theta}{\pi}$, $|a_{l=\frac{T}{2}}| = \left|\frac{e^{-2i\pi\phi'''}-1}{e^{-2\pi\phi'''/T}-1}\right| \ge T\frac{2}{\pi}$, and $|b_{l=\frac{T}{2}}| = \left|\frac{e^{2i\pi\phi'''}-1}{e^{2\pi\phi'''/T}-1}\right| = |a_{l=\frac{T}{2}}|$.

Therefore, for all cases above, measuring the counter in the computation basis reveals the closest integer to $\frac{T\theta}{\pi}$ with *constant* probability of success at least $4/\pi^2$ so that θ can be determined to $O(1/T)$ accuracy.

We also have $\theta \approx \sqrt{r/N}$, or $r \approx N\theta^2$. Hence, $\delta r \approx 2\sqrt{rN}\delta\theta$. Since $\delta\theta = O(1/T)$ and setting $\delta r \approx 1$ it follows that $T = O(\sqrt{rN})$. Classically, the query complexity is $O(rN)$ since we would need to determine the values of rN inputs for which $X_i = 1$.