# Ph 219b/CS 219b

**Exercises**
**Due: Wednesday 11 February 2009**

### 5.1 The peak in the Fourier transform

In the period finding algorithm we prepared the "periodic state"

$$\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle \ , \tag{1}$$

where $A$ is the least integer greater than $N/r$; then we performed the quantum Fourier transform with base $N$ and measured. The probability distribution governing the measurement outcome $y$ is

$$\text{Prob}(y)=\frac{1}{NA}\left(\frac{\sin^2\pi Ayr/N}{\sin^2\pi yr/N}\right) \ . \tag{2}$$

Letting $\delta$ denote the deviation of the rational number $y/N$ from the nearest integer multiple of $1/r$,

$$\delta=\frac{y}{N}-\frac{k}{r} \ , \tag{3}$$

this probability may be expressed as

$$\text{Prob}(y)=\frac{1}{NA}\left(\frac{\sin^2\pi Ar\delta}{\sin^2\pi r\delta}\right) \ . \tag{4}$$

Note that, since there is a multiple of $1/r$ within distance $1/2r$ from any real number, we may assume that $-1/2r\le\delta\le 1/2r$.

*a*) Show that

$$\text{Prob}(y)\le\frac{1}{4NAr^2\delta^2} \ . \tag{5}$$

*b*) Let us say that the measurement outcome $y$ is "$\delta$-bad" if the distance to the nearest multiple of $1/r$ is larger than $\delta$. Show that the probability Prob$(>\delta)$ of a $\delta$-bad outcome satisfies

$$\text{Prob}(>\delta)<\frac{1}{N\delta} \ . \tag{6}$$

Thus, for fixed $\delta$, the probability of a $\delta$-bad outcome is small for $N >> 1/\delta$.

### 5.2 Estimating the trace of a unitary matrix

Recall that using an oracle that applies the conditional unitary $\Lambda(U)$,

$$\begin{aligned}\Lambda(U): \qquad & |0\rangle \otimes |\psi\rangle \mapsto |0\rangle \otimes |\psi\rangle \ , \\ & |1\rangle \otimes |\psi\rangle \mapsto |1\rangle \otimes U|\psi\rangle \end{aligned} \tag{7}$$

(where $U$ is a unitary transformation acting on $n$ qubits), we can measure the eigenvalues of $U$. If the state $|\psi\rangle$ is the eigenstate $|\lambda\rangle$ of $U$ with eigenvalue $\lambda = \exp(2\pi i\phi)$, then by querying the oracle $k$ times, we can determine $\phi$ to accuracy $O(1/\sqrt{k})$.

But suppose that we replace the pure state $|\psi\rangle$ in eq. (7) by the maximally mixed state of $n$ qubits, $\rho = I/2^n$.

*a*) Show that, with $k$ queries, we can estimate both the real part and the imaginary part of $\mathrm{tr}\,(U)\,/2^n$, the normalized trace of $U$, to accuracy $O(1/\sqrt{k})$.

*b*) Given a polynomial-size quantum circuit, the problem of estimating to fixed accuracy the normalized trace of the unitary transformation realized by the circuit is believed to be a hard problem classically. Explain how this problem can be solved efficiently with a quantum computer.

The initial state needed for each query consists of one qubit in the pure state $|0\rangle$ and $n$ qubits in the maximally mixed state. Surprisingly, then, the initial state of the computer that we require to run this (apparently) powerful quantum algorithm contains only a constant number of "clean" qubits, and $O(n)$ very noisy qubits.

### 5.3 A generalization of Simon's problem

Simon's problem is a hidden subgroup problem with $G = Z_2^n$ and $H = Z_2 = \{0, a\}$. Consider instead the case where $H = Z_2^k$, with generator set $\{a_i, i = 1, 2, 3, \ldots, k\}$. That is, suppose an oracle evaluates a function

$$f : \{0,1\}^n \to \{0,1\}^{n-k} \ , \tag{8}$$

where we are promised that $f$ is $2^k$-to-1 such that

$$f(x) = f(x \oplus a_i) \tag{9}$$

for $i = 1, 2, 3, \ldots, k$ (here $\oplus$ denotes bitwise addition modulo 2). Since the number of cosets of $H$ in $G$ is smaller, we can expect that the hidden subgroup is easier to find for this problem than in Simon's ($k = 1$) case.

Find an algorithm using $n - k$ quantum queries that identifies the $k$ generators of $H$, and show that the success probability of the algorithm is greater than 1/4.

### 5.4 Query complexity of non-abelian hidden subgroup problems

We have seen that there is an efficient quantum algorithm that solves the hidden subgroup problem for any finitely generated abelian group. What about non-abelian groups? The purpose of this exercise is to show that for any finite group $G$, the hidden subgroup problem can be solved with polylog($|G|$) queries to the oracle, an exponential improvement over the best classical algorithm.

The oracle evaluates a function

$$f : G \to X \ , \tag{10}$$

from the group $G$ to a set $X$, that is constant and distinct on the cosets of a subgroup $H \le G$. The problem is to identify $H$. The input register contains at least $\log |G|$ qubits ($|G|$ denotes the order of $G$, the number of elements that it contains), and there are basis states $\{|g\rangle, g \in G\}$ that can be identified with group elements, such that $\langle g'|g\rangle = 0$ for $g \ne g'$. We can query the oracle with a uniform superposition of all group elements, and so prepare the state

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \ . \tag{11}$$

By measuring the output register, we prepare the input register in a randomly selected "coset state" $|gH\rangle$, a uniform superposition of the elements of the coset:

$$|gH\rangle \equiv \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle \ . \tag{12}$$

Distinct cosets of $H$ are disjoint, so the coset states corresponding to two distinct cosets are orthogonal.

*a*) Note that if $H$ and $H'$ are two subgroups of $G$, then their intersection $H \cap H'$ is also a subgroup of $G$. Show that if the intersection of cosets $g'H' \cap gH$ is not empty, then it contains $|H \cap H'|$ elements of $G$.

*b*) Recall that if $H' \leq H$, then $|H'|$ divides $|H|$. Let $P_H$ denote the orthogonal projection onto the linear span of the coset states $\{|gH\rangle, g \in G\}$. Show that

$$\|P_{H'}|gH\rangle\|^2 = \frac{|H \cap H'|}{|H'|} \ . \tag{13}$$

Conclude that $P_{H'}|gH\rangle = |gH\rangle$ for $H' \leq H$, and that for $H' \not\leq H$,

$$\|P_{H'}|gH\rangle\| \leq \frac{1}{\sqrt{2}} \ . \tag{14}$$

With $k$ queries we can prepare a tensor product of randomly selected coset states

$$|\psi\rangle = |g_1H\rangle \otimes |g_2H\rangle \otimes \cdots \otimes |g_kH\rangle \ . \tag{15}$$

Let $P_H^{(k)} \equiv P_H^{\otimes k}$ denote the orthogonal projector onto the linear span $V_H^{(k)}$ of all such product states. Note that for $H' \not\leq H$,

$$\|P_{H'}^{(k)}|\psi\rangle\| \leq \frac{1}{2^{k/2}} \ . \tag{16}$$

Thus if the actual hidden subgroup is $H$, and we make an orthogonal measurement $M_{H'}^{(k)}$ that projects onto either $V_{H'}^{(k)}$ (the positive outcome) or its orthogonal complement $V_{H'}^{(k)\perp}$ (the negative outcome), then we obtain the positive outcome with probability one for $H' \leq H$, and we obtain the positive outcome with probability no greater than $2^{-k}$ for $H' \not\leq H$.

We can make a list $H_1, H_2 \ldots, H_R$ of the candidate hidden subgroups starting with the largest subgroups, such that no $H_r$ on the list is a subgroup of another $H_s$ for $s > r$; then we perform a series of tests to identify the hidden subgroup by first performing the measurement $M_{H_1}^{(k)}$, then $M_{H_2}^{(k)}$, continuing until a positive outcome is obtained for the first time. The first $H'$ for which the measurement yields a positive outcome is identified as the hidden subgroup.

To check that this algorithm really works, we need to verify that the measurements that yield negative outcomes do not disturb the state

$|\psi\rangle$ very much. If the actually hidden subgroup is $H_r$ (the $r$th one listed), then the probability that the algorithm successfully identifies $H_r$ is

$$P_{\text{success}} = \|P_{H_r}\left(I - P_{H_{r-1}}\right)\left(I - P_{H_{r-2}}\right)\cdots\left(I - P_{H_1}\right)|\psi\rangle\|^2 \qquad (17)$$

$c$) Note that

$$\|A|\varphi\rangle - A(I-B)|\varphi\rangle\| = \|AB|\varphi\rangle\| \le \|B|\varphi\rangle\| \qquad (18)$$

for $\|A\|_{\text{sup}} \le 1$; applying eq. (18) repeatedly $r-1$ times, conclude that

$$P_{\text{success}} \ge \left(1 - \frac{r-1}{2^{k/2}}\right)^2 . \qquad (19)$$

We see that the algorithm has constant success probability for $k = O(\log R)$, where $R$ is the number of candidates for the hidden subgroup. In fact, since any subgroup of $G$ can be generated by a set of at most $n = \log_2|G|$ elements of $G$ (you are not asked to prove this), and there are fewer than $|G|^n$ ways to choose $n$ elements of $|G|$, the number of subgroups of $G$ (and hence $R$) is less than $2^{n^2}$. Therefore $O(\log^2|G|)$ queries suffice to solve the hidden subgroup problem.

However . . . in contrast to the solution to the abelian hidden subgroup problem, our algorithm runs in exponential time, because we may have to perform $R$ measurements after the queries are completed. So far, polynomial time (in $\log|G|$) algorithms that solve the hidden subgroup problem for non-abelian $G$ are known in only a few special cases.