Quantum algorithms (CO 781) Winter 2008

ASSIGNMENT 1 due Monday 4 February (in class)

Problem 1 (*Parallelizing the QFT*).

Consider the Fourier transform over $\mathbb{Z}_{2^n}$,

$$F_{\mathbb{Z}_{2^n}} := \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{Z}_{2^n}} \omega_{2^n}^{xy} |y\rangle\langle x|.$$

Here we will show that $F_{\mathbb{Z}_{2^n}}$ can be implemented with a circuit of only logarithmic depth, meaning that it can be implemented very quickly if gates can be performed in parallel.

a. What is the depth of the standard quantum circuit for $F_{\mathbb{Z}_{2^n}}$ (both the exact version of size $O(n^2)$ and the approximate version of size $O(n \log n)$)?

b. Let $|\tilde{x}\rangle := F_{\mathbb{Z}_{2^n}} |x\rangle$ denote a Fourier basis state. Define three operators A, B, C by

$$\begin{aligned} A|x, 0\rangle &= |x, \tilde{x}\rangle \\ B|\tilde{x}, 0\rangle &= |\tilde{x}, \tilde{x}\rangle \\ C|\tilde{x}\rangle^{\otimes k}|0\rangle &= |\tilde{x}\rangle^{\otimes k}|x\rangle \end{aligned}$$

where $k \in \mathbb{N}$ is some constant. Show how to produce a quantum circuit for $F_{\mathbb{Z}_{2^n}}$ using quantum circuits for A, B, and C.

c. Modify the standard quantum circuit for $F_{\mathbb{Z}_{2^n}}$ to give a quantum circuit for A. Show that an approximate version of this circuit has depth $O(\log n)$.

d. Show that $D|\tilde{x}, \tilde{y}\rangle = |\tilde{x}, \widetilde{x+y}\rangle$, where the operator D is defined by $D|x, y\rangle = |x - y, y\rangle$. Explain how this observation can be used to give a quantum circuit for B of depth $O(\log n)$. (Note that addition of n-bit integers can be performed by a classical circuit of depth $O(\log n)$.)

e. *Challenge problem:* Give an implementation of C by a circuit of logarithmic depth. (Hint: $k = 3$ is possible, but the construction is somewhat involved.)

Problem 2 (*Discrete log with χ states*).

Let $G = \langle g \rangle$ be a cyclic group of order N. For each $\alpha \in \mathbb{Z}_N$, define the state

$$|\chi^\alpha\rangle := \frac{1}{\sqrt{N}} \sum_{\beta \in \mathbb{Z}_N} \omega_N^{\alpha\beta} |g^\beta\rangle.$$

These states turn out to give an alternative method for computing discrete logarithms over G.

a. For any $x \in G$, let D_x denote the "division operator" defined by $D_x|\alpha, y\rangle = |\alpha, y/x^\alpha\rangle$ where $\alpha \in \mathbb{Z}_N$ and $y \in G$. Explain how to implement D_x efficiently on a quantum computer.

b. Show that $|\alpha, \chi^\beta\rangle$ is an eigenvector of D_x, and compute its eigenvalue.

c. Show that $(F_{\mathbb{Z}_N}^\dagger \otimes I) D_x (F_{\mathbb{Z}_N} \otimes I)|0, \chi^1\rangle = |\log_g x, \chi^1\rangle$, where

$$F_{\mathbb{Z}_N} := \frac{1}{\sqrt{N}} \sum_{\alpha,\beta \in \mathbb{Z}_N} \omega_n^{\alpha\beta} |\beta\rangle\langle\alpha|$$

denotes the Fourier transform over the additive group $\mathbb{Z}_N$.

This shows how to compute $\log_g x$, provided we are given a copy of the state $|\chi^1\rangle$.

Note that $|\chi^\alpha\rangle$ is simply the Fourier transform of $|g^\alpha\rangle$ over G. However, even though we know how to implement $F_{\mathbb{Z}_N}$ (the Fourier transform over the *additive* group $\mathbb{Z}_N$), this does not let us implement the Fourier transform over the *multiplicative* group G, unless we can compute discrete logarithms. Nevertheless, it is possible to create $|\chi^1\rangle$ using only simple operations.

d. Show that $(F_{\mathbb{Z}_N} \otimes I) D_{g^{-1}} (F_{\mathbb{Z}_N} \otimes I) |0, g^0\rangle = \frac{1}{\sqrt{N}} \sum_{\alpha \in \mathbb{Z}_N} |\alpha, \chi^\alpha\rangle$.

e. For any $\alpha \in \mathbb{Z}_N$, let D^α denote another "division operator," this one defined by $D^\alpha |x, y\rangle = |x, y/x^\alpha\rangle$ where $x, y \in G$. Show that $D^\alpha |\chi^\beta, \chi^\gamma\rangle = |\chi^{\beta+\alpha\gamma}, \chi^\gamma\rangle$.

f. Suppose we measure the first register of the state from part d and obtain a value α, leaving the second register in the state $|\chi^\alpha\rangle$. Furthermore, suppose that $\gcd(\alpha, N) = 1$, so that α^{-1} is well-defined modulo N. (Note that this happens with probability $\phi(N)/N = \Omega(1/\log\log N)$, so we don't have to repeat the procedure from part d many times before obtaining such an α.) Show how to use the state $|\chi^\alpha\rangle$ to prepare $|\chi^1\rangle$. (Hint: Use part e.)

g. Explain why part e also shows that $|\chi^1\rangle$ can be easily copied.

Problem 3 (*Relative difficulty of breaking RSA and elliptic curve cryptography*).

The best known classical algorithm for factoring a number N, the number field sieve, takes time $\exp(O((\log N)^{1/3}(\log\log N)^{2/3}))$. In contrast, the best known algorithms for computing the discrete logarithm over an elliptic curve of order N take time $O(\sqrt{N})$. Thus, it is widely accepted that elliptic curve cryptography (ECC) provides greater security than RSA for a given key size. For example, Certicom (the company that provides the ECC software used on BlackBerry devices) claims that ECC with a key size of 512 bits provides comparable security to RSA with a key size of 15360 bits.

a. Estimate the number of qubits and number of elementary gates that Shor's algorithm would need to break RSA with a key size of 15360 bits and ECC with a key size of 512 bits, respectively. A rough estimate is fine, but you should justify whatever assumptions you make.

b. Briefly comment on the implications of your estimate.

Problem 4 (*Properties of the solutions to Pell's equation and of algebraic integers*).

Consider Pell's equation, $x^2 - dy^2 = 1$, where $d \in \mathbb{Z}$ is squarefree. Associate the solution $x, y \in \mathbb{Z}$ with the real number $\xi = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, whose conjugate is defined as $\bar{\xi} := x - y\sqrt{d}$.

a. Show that the set of solutions to Pell's equation forms a group, where the group operation corresponds to multiplication of the associated elements of $\mathbb{Z}[\sqrt{d}]$, and inversion corresponds to conjugation.

b. A solution (x, y) of Pell's equation is called *positive* if $x > 0$ and $y > 0$. Let (x_1, y_1) be the positive solution of Pell's equation for which $x_1 + y_1\sqrt{d}$ is smallest. Show that the set of all positive solutions is $\{(x_1 + y_1\sqrt{d})^n : n \in \mathbb{N}\}$. (Hint: Suppose there is some solution lying strictly between $(x_1 + y_1\sqrt{d})^j$ and $(x_1 + y_1\sqrt{d})^{j+1}$ for some $j \in \mathbb{N}$, and derive a contradiction.)

c. Recall that $\xi = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ is called an *algebraic integer* if it is the root of a monic polynomial with integer coefficients. Prove that ξ is an algebraic integer if and only if $2x$ and $x^2 - dy^2$ are integers. (Hint: Consider the quantities $\xi + \bar{\xi}$ and $\xi\bar{\xi}$, where $\bar{\xi}$ is defined the same way for arbitrary elements of $\mathbb{Q}[\sqrt{d}]$ as it is for elements of $\mathbb{Z}[\sqrt{d}]$.)

Problem 5 (*The hidden parabola problem*).
Suppose we are given a black box function $f_{\alpha,\beta} : \mathbb{F}_p^2 \to S$, where p is a prime and S is a finite set, satisfying the promise that

$$f_{\alpha,\beta}(x,y) = f_{\alpha,\beta}(x',y') \quad \text{if and only if} \quad \alpha x^2 + \beta x - y = \alpha x'^2 + \beta x' - y'$$

for some unknown $\alpha \in \mathbb{F}_p^\times$ and $\beta \in \mathbb{F}_p$. In other words, $f_{\alpha,\beta}$ is constant on the parabola

$$P_{\alpha,\beta,\gamma} := \{(x,y) \in \mathbb{F}_p^2 : y = \alpha x^2 + \beta x + \gamma\}$$

for any fixed $\gamma \in \mathbb{F}_p$, and distinct on parabolas corresponding to different values of γ. Given the ability to query $f_{\alpha,\beta}$, the *hidden parabola problem* asks us to determine the values of α and β.

a. Explain why a classical computer must query $f_{\alpha,\beta}$ exponentially many times (in $\log p$) to solve the hidden parabola problem.

b. Show that the quantum query complexity of determining α and β is $\text{poly}(\log p)$.

Problem 6 (*Weak Fourier sampling fails for the symmetric group*).
Consider the hidden subgroup problem in an arbitrary finite group G.

a. Compute the distributions over $\hat{G}$ that are observed when we perform weak Fourier sampling in two cases: the hidden subgroup is trivial, or the hidden subgroup is $\{1, \pi\}$ where π is an involution. Your answer should be expressed in terms of the characters of G.

b. Show that the total variation distance between these two distributions is upper bounded by $\sqrt{\frac{1}{|G|} \sum_{\sigma \in \hat{G}} |\chi_\sigma(\pi)|^2}$.

c. Prove that $\sum_{\sigma \in \hat{G}} |\chi_\sigma(\pi)|^2 = |G|/|\text{conj}(\pi)|$, where $\text{conj}(\pi)$ denotes the conjugacy class of G to which π belongs. (Hint: Use the orthogonality relations for the character table of G.)

d. Let $G = S_n$, the symmetric group on n items, and find a choice of π for which the total variation distance is exponentially small in n. This shows that weak Fourier sampling fails to solve the hidden subgroup problem in S_n.

Problem 7 (*Nonabelian Fourier sampling for the dihedral group*).
In lecture, we attacked the hidden subgroup problem over the dihedral group of order $2N$,

$$D_N := \langle r, s | r^2 = s^N = rsrs = 1 \rangle,$$

using the Fourier transform over the cyclic group $\mathbb{Z}_N$. In this problem you will show that this is essentially the same as performing the nonabelian Fourier transform over D_N. You will also give a representation-theoretic interpretation of Kuperberg's algorithm.

For reference, the irreducible representations of D_N are as follows: there are two one-dimensional irreps, σ_{triv} and σ_{sign}, with

$$\sigma_{\text{triv}}(r) := 1 \qquad \sigma_{\text{triv}}(s) := 1$$
$$\sigma_{\text{sign}}(r) := -1 \qquad \sigma_{\text{sign}}(s) := 1;$$

and $\lceil N/2 \rceil - 1$ two-dimensional irreps, σ_j for $j = 1, 2, \ldots, \lceil N/2 \rceil - 1$, with

$$\sigma_j(r) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_j(s) := \begin{pmatrix} \omega_N^j & 0 \\ 0 & \omega_N^{-j} \end{pmatrix}.$$

(If N is even then there are two additional one-dimensional irreps, but let us assume for simplicity that N is odd.)

a. Consider the HSP in D_N with the hidden subgroup $\{1, rs^\alpha\}$. Write down the state obtained by Fourier sampling over D_N, assuming you measure a two-dimensional irrep σ_j. Compare to the possible states obtained by Fourier sampling over $\mathbb{Z}_N$, obtaining some measurement outcome $k \in \mathbb{Z}_N$ with $k \neq 0$, and describe a correspondence between the two procedures. (Hint: There are more possible values of k than values of j, so each value of j must correspond to multiple values of k.)

b. Describe a similar correspondence between the one-dimensional irreps of D_N and the state obtained when Fourier sampling over $\mathbb{Z}_N$ yields the measurement outcome 0.

c. Decompose the representation $\sigma_j \otimes \sigma_k$ as a direct sum of irreducible representations of D_N.

d. In view of the correspondence established in parts a and b, interpret the combination operation used in Kuperberg's algorithm in the light of representation theory.

e. *Challenge problem:* Give a quantum circuit for F_{D_N} that uses $F_{\mathbb{Z}_N}$ as a subroutine.