Quantum algorithms (CO 781/CS 867/QIC 823) Winter 2013

ASSIGNMENT 1 due Tuesday 5 February (in class)

Problem 1 (*Solovay-Kitaev*).

In this problem you will fill in some details in the proof of the Solovay-Kitaev Theorem.

a. Prove the following basic facts about SU(2):

   (i) $\|I - e^{i\vec{a}\cdot\vec{\sigma}}\| = 2\sin\frac{\|\vec{a}\|}{2} = \|\vec{a}\| + O(\|\vec{a}\|^3)$

   (ii) $\|e^{i\vec{b}\cdot\vec{\sigma}} - e^{i\vec{c}\cdot\vec{\sigma}}\| \le \|\vec{b} - \vec{c}\|$

   (iii) $[\vec{b}\cdot\vec{\sigma}, \vec{c}\cdot\vec{\sigma}] = 2i(\vec{b}\times\vec{c})\cdot\vec{\sigma}$

   (iv) $\|\llbracket e^{i\vec{b}\cdot\vec{\sigma}}, e^{i\vec{c}\cdot\vec{\sigma}}\rrbracket - e^{-[\vec{b}\cdot\vec{\sigma},\vec{c}\cdot\vec{\sigma}]}\| = O(\|\vec{b}\|\|\vec{c}\|(\|\vec{b}\| + \|\vec{c}\|))$

   Here $\vec{a},\vec{b},\vec{c}\in\mathbb{R}^3$, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, and the big-$O$ notation is with respect to $\|\vec{a}\|\to 0$ in (i) and with respect to $\|\vec{b}\|, \|\vec{c}\|\to 0$ in (iv).

b. Read and understand the proof (in the notes for lecture 1) that if Γ is an ϵ^2-net for S_ϵ, then $\llbracket\Gamma,\Gamma\rrbracket$ is an $O(\epsilon^3)$-net for S_{ϵ^2}.

c. Describe an explicit recursive procedure that constructs an approximation to a given gate $U \in \mathrm{SU}(2)$ with precision ϵ. What is the asymptotic running time of your procedure? (It should be $O((\log\frac{1}{\epsilon})^k)$ for some explicit value of k.)

Problem 2 (*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 you 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

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

   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 (for any particular constant k) by a circuit of logarithmic depth. (Hint: $k = 3$ is possible, but the construction is somewhat involved.)

Problem 3 (*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 why D_x can be implemented efficiently by 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 4 (*Properties of the solutions to Pell's equation*).
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.)

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

b. Write down the mixed quantum state obtained by querying $f_{\alpha,\beta}$ on a uniform superposition over $\mathbb{F}_p \times \mathbb{F}_p$ and then discarding the function value.

c. Show that this state is invariant under additive translations of one of the two registers, and hence will be block diagonalized by the Fourier transform over $\mathbb{Z}_p$ on that register. Compute the resulting Fourier transformed state.

d. Suppose the register on which the Fourier transform was performed is measured, and consider the resulting post-measurement state. Show that this density matrix is rank one, and write down the corresponding pure quantum state.

e. Write down the state obtained when the process described in parts b–d is performed twice. Collect the terms in the phase of this state proportional to the unknown parameters α, β, and show that these coefficients can be computed in ancilla registers.

f. For any fixed value of the two ancilla registers, compute the state of the other two registers. In particular, show that it is (proportional to) the uniform superposition over the set of solutions to a pair of quadratic equations in two variables.

g. Find the solutions of this system of quadratic equations. (If you like, you can use a computer algebra program to do the calculation.)

h. Explain how to efficiently erase the values in the registers containing the solution to the quadratic system.

i. Having implemented the erasure, perform the inverse Fourier transform over $\mathbb{Z}_p \times \mathbb{Z}_p$ on the ancilla registers, and show that a measurement of the resulting state gives the outcome α, β with probability $\Omega(1)$.