Ph 219/CS 219

Exercises
Due: Wednesday 4 March 2009

6.1 Finding a collision

Suppose that a black box evaluates a function

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

We are promised that the function is 2-to-1, and we are to find a "collision" – values x and y such that $f(x) = f(y)$. This problem is harder than Simon's problem, because we are not promised that the function is periodic. Let $N = 2^n$.

a) Describe a randomized classical algorithm that requires SPACE $= O(\sqrt{N})$ and that succeeds in finding a collision with high probability in $O(\sqrt{N})$ queries of the black box.

b) Now suppose that only SPACE $= O(N^{1/3})$ is available. Describe a randomized classical algorithm that finds a collision with high probability in $O(N^{2/3})$ queries.

c) Show that Grover's exhaustive search algorithm can be used to find a collision in $O(\sqrt{N})$ quantum queries, using SPACE $= O(1)$.

d) Describe a quantum algorithm that uses SPACE $= O(M)$ and finds a collision in $O(M) + O(\sqrt{N/M})$ quantum queries. [**Hint**: First query the box M times to learn the value of $f(x)$ for M arguments $\{x_1, x_2, \ldots, x_M\}$, then search for y such that $f(y) = f(x_i)$ for some x_i.] Thus, if M is chosen to optimize the number of queries, the quantum algorithm uses SPACE $= O(N^{1/3})$ and $O(N^{1/3})$ quantum queries.

6.2 All the information for half the price

A black box computes a function

$$f : \{0,1\}^n \to \{0,1\} . \tag{2}$$

This function can be represented by a binary string

$$X = X_{N-1}X_{N-2}\cdots X_1X_0 , \tag{3}$$

where $X_i = f(i)$ and $N = 2^n$. Our goal is to obtain, with high probability of success, *complete* information about the box; that is, to find the value of X. The only resource we care about is the number of queries of the box — TIME and SPACE are otherwise unlimited.

a) How many classical queries are needed to find X with success probability at least $2/3$?

b) Suppose that the state

$$|\Psi_{X,N}\rangle = \frac{1}{\sqrt{2^N}} \sum_{Y\in\{0,1\}^N} (-1)^{X\cdot Y}|Y\rangle \tag{4}$$

has been prepared, where the sum is over all N-bit strings, and $X \cdot Y$ denotes the mod 2 bitwise inner product

$$\begin{aligned} X \cdot Y \quad &= \quad (X_{N-1} \cdot Y_{N-1}) \oplus (X_{N-2} \cdot Y_{N-2}) \\ &\qquad \cdots \oplus (X_1 \cdot Y_1) \oplus (X_0 \cdot Y_0) \ . \end{aligned} \tag{5}$$

Describe a way, by applying a simple unitary and then a measurement, to find the value of X with certainty.

c) Explain how the unitary transformation

$$U : |Y\rangle \to (-1)^{X\cdot Y}|Y\rangle \tag{6}$$

can be implemented with $|Y|$ queries of the box, where $|Y|$ denotes the *Hamming weight* of Y, the number of 1's in the string.

d) Suppose we prepare the state

$$|\Phi_K\rangle = \frac{1}{\sqrt{M_K}} \sum_{Y:|Y|\le K} |Y\rangle \ , \tag{7}$$

where

$$M_K = \sum_{j=0}^{K} \binom{N}{j} \ , \tag{8}$$

and then apply U (requiring at most K queries) to obtain

$$|\Psi_{X,K}\rangle = \frac{1}{\sqrt{M_K}} \sum_{Y:|Y|\le K} (-1)^{X\cdot Y}|Y\rangle \ , \tag{9}$$

Show that, by applying the procedure that you described in your answer to (*b*), we can determine the value of X with a probability of success

$$P_{\rm succ}(N, K) = |\langle\Psi_{X,K}|\Psi_{X,N}\rangle|^2 \ , \tag{10}$$

and compute the value of $P_{\rm succ}(N, K)$.

e) Suppose that

$$K = N/2 + c\sqrt{N} \ , \tag{11}$$

where c is a constant. Show that

$$1 - P_{\rm succ}(N,K) = O(e^{-2c^2}) \ . \tag{12}$$

Thus we can extract all the information from the box in a number of queries $(N/2)\cdot[1 + O(1/\sqrt{N})]$.

6.3 Quantum counting

A black box computes a function

$$f : \{0,1\}^n \to \{0,1\} \ , \tag{13}$$

which can be represented by a binary string

$$X = X_{N-1}X_{N-2}\cdots X_1 X_0 \ , \tag{14}$$

where $X_i = f(i)$ and $N = 2^n$. Our goal is to count the number r of states "marked" by the box; that is, to determine the Hamming weight $r = |X|$ of X. We can devise a quantum algorithm that counts the marked states by combining Grover's exhaustive search with the quantum Fourier transform.

a) Suppose we can consult a quantum oracle that executes the unitary transformation U. We'd like to perform $\Lambda(U)$, the unitary U conditioned on the value of a control qubit. Devise a quantum circuit with one oracle query that executes $\Lambda(U)$, using ancilla qubits and $\Lambda({\rm SWAP})$ gates, where

$${\rm SWAP} : |x\rangle|y\rangle \to |y\rangle|x\rangle \ . \tag{15}$$

b) Let

$$|\Psi_X\rangle = \frac{1}{\sqrt{r}} \sum_{j:X_j=1} |j\rangle \tag{16}$$

denote the uniform superposition of the marked states, and let $U_{\rm Grover}$ denote the "Grover iteration," which performs a rotation by the angle 2θ in the plane spanned by $|\Psi_X\rangle$ and

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N} |j\rangle \ , \tag{17}$$

where

$$\sin\theta = \langle s|\Psi_X\rangle = \sqrt{\frac{r}{N}}\ . \tag{18}$$

Consider a unitary transformation

$$V : |t\rangle \otimes |\Phi\rangle \to |t\rangle \otimes U^t_{\text{Grover}}|\Phi\rangle \tag{19}$$

that reads a counter register taking values $t \in \{0, 1, 2, \ldots, T-1\}$ (where $T = 2^m$), and then applies U_{Grover} t times. Explain how V can be implemented, calling the oracle $T-1$ times. [**Hint:** Use the binary expansion $t = \sum_{k=0}^{m-1} t_k 2^k$ and the conditional oracle call from (a).]

c) Suppose that $r \ll N$. Show that, by applying V, performing the quantum Fourier transform on the counter register, and then measuring the counter register, we can determine θ to accuracy $O(1/T)$, and hence we can find r with high success probability in $T = O(\sqrt{rN})$ queries. Compare to the best classical protocol.

6.4 Simulating the Schrödinger equation

A quantum computer can simulate the continuous time evolution of a quantum system governed by a "geometrically local" Hamiltonian. Usually such simulations are done by approximating continuous time evolution with a series of discrete time steps, introducing an error that should be small if the step size is small enough.

For example, by expanding the exponential in a power series, you can verify that

$$e^{A+B} - e^A e^B = -\frac{1}{2}[A, B] + \cdots\ ; \tag{20}$$

here $[A, B] = AB - BA$ is the commutator of operators A and B and the ellipsis indicates terms that are higher order in A and B. Suppose the (time-independent) Hamiltonian H can be expressed as a sum of terms $H = \sum_a H_a$. Then we may approximate the time evolution operator $e^{-i\Delta H}$ for time interval Δ using

$$\begin{aligned} & e^{-i\Delta(H_1+H_2+\cdots H_n)} - \left(e^{-i\Delta H_1} e^{-i\Delta H_2} \cdots e^{-i\Delta H_n}\right) \\ = \ & \frac{1}{2}\Delta^2 \sum_{a<b} [H_a, H_b] + \cdots\ . \end{aligned} \tag{21}$$

If the Hamiltonian H is geometrically local, then $e^{-i\Delta H_a}$ acts on a constant number of qubits, and let us therefore assume it can be simulated accurately with a constant number of gates (ignoring a possible

"Solovay-Kitaev slowdown"). Furthermore, for an n-qubit system, the total number of terms $\{H_a\}$ is $O(n)$, and the number of terms in $\{H_a\}$ that fail to commute with any fixed term H_b is a constant. Therefore, if all the terms have a bounded operator norm, $\|H_a\| \leq E$, then the error on the right-hand side of eq. (21) has operator norm no larger than $C\Delta^2 E^2 n$, where C is a constant. To simulate the evolution for time T, we need T/Δ time steps, and the accumulated error is bounded above by $CT\Delta E^2 n$. Therefore our simulation has constant accuracy if we choose $\Delta = O(1/nT)$ (assuming E is a constant), and circuit size $O(nT/\Delta) = O[(nT)^2]$. In effect, then, the circuit size scales quadratically with the volume of the simulated spacetime.

The object of this exercise is to show that the cost of the simulation can be reduced to a lower power of nT, namely the 3/2 power.

a) Show that

$$e^{2(A+B)} - e^A e^B e^B e^A = \frac{1}{3}[A,[A,B]] - \frac{2}{3}[B,[B,A]] + \cdots \; , \quad (22)$$

where now the ellipsis indicates terms of quartic or higher order.

b) Show that

$$\begin{aligned} & e^{-i\Delta(H_1+H_2+\cdots H_n)} \\ & - \left(e^{-i\Delta H_1/2} e^{-i\Delta H_2/2} \cdots e^{-i\Delta H_n/2}\right) \\ & \times \left(e^{-i\Delta H_n/2} \cdots e^{-i\Delta H_2/2} e^{-i\Delta H_1/2}\right) \\ = \; & \Delta^3 \left(\sum_{a<b<c} \mathcal{O}_{abc} + \sum_{a<b} \mathcal{O}_{ab} + \cdots \right), \end{aligned} \quad (23)$$

where the ellipsis indicates terms of quartic order and above. Find explicit expressions for $\mathcal{O}_{abc}$ and $\mathcal{O}_{ab}$ in terms of third-order commutators of the terms in $\{H_a\}$.

c) Assuming as above that $e^{-i\Delta H_a/2}$ can be simulated using a constant number of gates, show that for a geometrically local n-qubit Hamiltonian $H = \sum_a H_a$, where $\|H_a\| \leq$ constant, the time evolution operator e^{-iHT} can be simulated to constant accuracy using $O[(nT)^{3/2}]$ gates.

The power of nT can be reduced further using more elaborate constructions.