Due: Fri, Nov 18 @ 11:59pm
[Gradescope Link]

CSE 599Q: Homework #4

Quantum algorithms

1. Bernstein-Vazirani with a noisy oracle [16 points]

Recall that in the Bernstein-Vazirani problem, there is a hidden string $s \in \{0,1\}^n$ and we have access to a function $f : \{0,1\}^n \to \{0,1\}$ such that

$$f(x) = s \cdot x \bmod 2 = (s_1 x_1 + s_2 x_2 + \cdots + s_n x_n) \bmod 2.$$

The goal is to recover the secret s, and the Bernstein-Vazirani algorithm allows us to do this with only a *single quantum query* to f.

Suppose now that the function f is noisy, in the sense that, for some noise parameter $\varepsilon > 0$, we only have the guarantee

$$\frac{\#\{x \in \{0,1\}^n : f(x) = s \cdot x \bmod 2\}}{2^n} \geq 1 - \varepsilon.$$

A. [10 pts] Calculate a lower bound on the probability that a single run of the Bernstein-Vazirani algorithm nevertheless succeeds in recovering s and make sure to justify your calculation.

B. [6 pts] What happens when $\varepsilon = 1/2$? Explain why there is no hope for an algorithm to recover s in this case.

2. Group theory for Shor [16 points]

A. [0 pts] We write $\mathbb{Z}_n$ for the additive group of integers modulo n, whose elements can be represented by the numbers $\{0, 1, 2, \ldots, n-1\}$, and we use $\mathbb{Z}_n^*$ to denote the multiplicative group of integers modulo n, whose elements can be represented by the numbers $\{1 \leq a < n : \gcd(a,n) = 1\}$.

Show that for p prime, there is some generator $g \in \mathbb{Z}_p^*$ such that $\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$.

You may assume that $\mathbb{Z}_p^*$ has a generator for the rest of the problem.

B. [4 pts] Use this to show that the groups $\mathbb{Z}_{p-1}$ and $\mathbb{Z}_p^*$ are [isomorphic].

C. [4 pts] Show that $g^{(p-1)/2} \equiv -1 \pmod{p}$ must hold, where g is your generator of $\mathbb{Z}_p^*$.

D. [4 pts] Suppose that p, q are two distinct prime numbers. Show that $\mathbb{Z}_{pq}^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ are isomorphic.

You may use the Chinese Remainder Theorem: If m, n are two numbers with $\gcd(m, n) = 1$ then the system of equations $\{x \equiv a \pmod{m}, x \equiv b \pmod{n}\}$ has a solution and any two solutions x, x' satisfy $x \equiv x' \pmod{mn}$.

What is the imag[illegible]morphism?

E. [4 pts] Suppose y[illegible]se isomorphisms to map $\mathbb{Z}_{pq}^* \to \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$. What is the imag[illegible]

3. More group theory for Shor [16 points]

A. [4 pts] If $(G, +)$ is a group with identity element 0, then the *order of an element* $g \in G$ is the smallest k such that $g + g + \cdots + g = 0$ (the sum of k copies of g). We write $\mathrm{ord}_G(g)$ for the order of g.

Suppose $m = 2^k b$ is an even integer ($k \geq 1$) and b is odd. Show that if $u \in \mathbb{Z}_m$ is odd, then 2^k divides $\mathrm{ord}_{\mathbb{Z}_m}(u)$. Show that if $u \in \mathbb{Z}_m$ is even, then 2^k does **not** divide $\mathrm{ord}(u)$.

B. [4 pts] Suppose m, n are even integers and we pick $u \in \mathbb{Z}_m$ and $v \in \mathbb{Z}_n$ uniformly at random. Show that with probability at least $1/2$, the largest power of 2 that divides $\mathrm{ord}_{\mathbb{Z}_m}(u)$ is different from the largest power of 2 that divides $\mathrm{ord}_{\mathbb{Z}_n}(v)$.

C. [4 pts] Show that if $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then

$$\mathrm{ord}_{\mathbb{Z}_m \times \mathbb{Z}_n}(u, v) = \mathrm{LCM}\left(\mathrm{ord}_{\mathbb{Z}_m}(u), \mathrm{ord}_{\mathbb{Z}_n}(v)\right).$$

D. [4 pts] Suppose now that p, q are distinct odd prime numbers and we pick $u \in \mathbb{Z}_{p-1}$ and $v \in \mathbb{Z}_{q-1}$ uniformly at random, and define $L := \mathrm{ord}_{\mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}}(u, v)$. Use Problem 1 and parts (A)-(C) to show that with probability at least $1/2$, both of the following hold:

- L is even
- $(u, v) + (u, v) + \cdots + (u, v)$ (summed $L/2$ times) is not equal to $(\frac{p-1}{2}, \frac{q-1}{2})$.

4. Non-trivial square roots [12 points]

Use Problems 1 and 2 to show the following: Suppose that $B = pq$ is a product of two distinct odd primes p and q. Choose an element $A \in \mathbb{Z}_B^*$ uniformly at random and define $L := \mathrm{ord}_{\mathbb{Z}_B^*}(A)$.

Show that with probability at least $1/2$, it holds that L is even and $A^{L/2}$ is a non-trivial square root of 1 modulo B, i.e., $\left(A^{L/2}\right)^2 \equiv 1 \pmod{B}$, and $A^{L/2} \not\equiv \pm 1 \pmod{B}$.

5. Order finding reduces to factoring [12 points]

In class, we showed that if $B = pq$ is a product of two primes and we can find the order of an element A in $\mathbb{Z}_B^*$, we can produce the factors p and q.

Suppose now that you have a subroutine that takes a number B as input and outputs its prime factorization. Show that you can use this to find the order of any given element $A \in \mathbb{Z}_B^*$. Your a[illegible] polynomial time in the size of the input, i.e., in time $(\log_2 B)^{O(1)}$.

Extra credit: [illegible]ue [20 points]

One measure of progress in building quantum computers might be the size of numbers they can factor via Shor's algorithm. The state of the art is still $15 = 3 \cdot 5$. But is this impressive? Is $77 = 7 \cdot 11$ more impressive?

A. Read the paper Pretending to factor large numbers on a quantum computer. Write a paragraph summarizing their main critique of prior experiments.

B. Read the paper Realization of a scalable Shor algorithm. Do you think it adequately addresses the criticisms of the first article? Why (or why not)? Explain your thinking.