CSE 534 Autumn 2024: Set 4

Instructor: Chinmay Nirkhe
Due date: November 20th, 2024 10:00pm

Instructions: Solutions should be legibly handwritten or typset. Mathematically rigorous solutions are expected for all problems unless explicitly stated.

You are encouraged to collaborate on problems in small teams but everyone must individually submit solutions. Solutions for the problems may be found online or in textbooks – but do not use them.

For grading purposes, start each problem on a new page.

Problem 1 (Runtime of Shor's factoring algorithm)**.** **(6 points)** To the best of your ability, give an expected runtime of Shor's algorithm discussed in class in terms of $\log(N)$. It would be good, but not necessary for credit, to separate out the runtime in terms of quantum and classical subroutines.

This problem is meant to be be graded liberally, so state whatever assumptions you are making about parallelism, gate set, etc. as these may drastically change the runtime of the algorithm.

Problem 2 (Breaking Diffie-Helman)**.** Shor's factoring algorithm solves factoring which is the basis of security for the RSA cryptosystem. The Diffie-Helman key-exchange is a cryptographic primitive with which two parties Alice and Bob agree on a key K over a public channel. Once they have a shared key that no evesdropper Eve knows, they can encode and send each other messages with information-theoretic security.

Diffie-Helman protocol:

1. Alice and Bob publicly announce a prime p and a generator $g \in \mathbb{Z}_p^\times$.
2. Privately, Alice picks a random element $a \in \mathbb{Z}_p^\times$ and computes $A = g^a$. She announces A publicly.
3. Privately, Bob picks a random element $b \in \mathbb{Z}_p^\times$ and computes $B = g^b$. He announces B publicly.
4. Privately, Alice computes $K_A = B^a$ and privately, Bob computes $K_B = A^b$.

All computations are done within the group $\mathbb{Z}_p^\times$. If the protocol is executed honestly by Alice and Bob, then $K_A = K_B$ since $(g^a)^b = (g^b)^a$. An evesdropper Eve listening to the public communication would hear p, g, A, and B.

1. **(2 points)** Show that if Eve can compute x such that $h = g^x$ for any $g, h \in \mathbb{Z}_p^\times$, then Eve can calculate the key K of the Diffie-Helman protocol from p, g, A and B. Calculating x given $h, g \in \mathbb{Z}_p^\times$ is the discrete log(arithm) problem.

2. **(8 points)** Give a reduction from the discrete log problem to the ~~order finding problem~~ Abelian hidden subgroup problem and argue that a quantum computer can efficiently break the Diffie-Helman protocol.

Hint: Consider the function $f(x, z) = g^x h^z$.

Problem 3 (Clifford Circuits)**.** ~~In class, we saw how to simulate a n-qubit Clifford computation with m gates in classical deterministic time poly(n, m). In this problem, we will explore other properties of Clifford circuits.~~

1. ~~In fact, the computational power of Clifford computation is very weak – they are not capable of expressing even classical computation. We will end up showing that deciding if a Clifford computation accepts or not is complete for the class ⊕L.~~

   ~~The language Clifford is the set of Clifford circuit descriptions $\langle C \rangle$ such that measuring the first qubit of $C|0^m\rangle$ accepts with probability 1.~~

   ~~**(2 points)** Argue that measuring the first qubit of $C|0^m\rangle$ either accepts with probability 1, $\frac{1}{2}$ or 1 for every Clifford circuit C.~~

2. ~~**(4 points)** The language $\mathsf{LINEQ}_{\mathbb{Z}_2}$ is the set of matrices $(A, b) \in \mathbb{Z}_2^{m \times n} \times \mathbb{Z}_2^{m \times 1}$ such that $Ax = b$ has a solution. This language happens to be complete for ⊕L. Construct a reduction from $\mathsf{LINEQ}_{\mathbb{Z}_2}$ to Clifford (i.e. construct a Clifford circuit that is satisfiable iff $Ax = b$ has a solution).~~

3. ~~**(6 points)** Construct a reduction from Clifford to $\mathsf{LINEQ}_{\mathbb{Z}_2}$. Hint: every Pauli matrix $P \in \mathcal{P}_n$ can be expressed using $2n + 2$ bits.~~

   ~~(In general, both reductions should be log-space for proving completeness for the class ⊕L, but this is not required for full credit on this homework problem.)~~

Problem 4 (BQP is low)**.** In complexity theory, a complexity class C is called *low* if $\mathsf{C}^{\mathsf{C}} = \mathsf{C}$. We will show that BQP is low meaning $\mathsf{BQP}^{\mathsf{BQP}} = \mathsf{BQP}$ – or equivalently, a BQP computation using BQP computations as subroutines – even in superposition - can be rewritten as a single BQP computation. We will break this down into steps.

1. **(4 points)** First show that if a measurement is nearly deterministic, then it is not too perturbative. I.e. Consider a generic POVM on register A of a state ρ_{AB} with the probability of outcome 0 is $1 - \epsilon$. Let ρ' be the post-measurement state. What is $\|\rho - \rho'\|_1$?

2. **(4 points)** Show that the class BQP has error-amplification; meaning the $2/3$ vs $1/3$ definition can be replaced with $1 - 2^{-\Omega(n)}$ and $2^{-\Omega(n)}$ as the bounds with only a polynomial increase in the size of the circuit.

3. **(8 points)** Consider a generic BQP quantum circuit imbibed with $\mathrm{poly}(n)$ many "oracle" gates to other BQP problems. Recall an oracle gate for a computation f is one that computes $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$. In the case of an oracle gate to a BQP problem $(\mathcal{L}_{\mathsf{yes}}, \mathcal{L}_{\mathsf{no}})$, we mean that a function family of functions $f_n : \{0,1\}^n \to \{0,1\}$ such that $f_n(x) = 1$ if $x \in \mathcal{L}_{\mathsf{yes}}$, $f_n(x) = 0$ if $x \in \mathcal{L}_{\mathsf{no}}$, and $f_n(x)$ can take on either value of $x \notin \mathcal{L}_{\mathsf{yes}} \cup \mathcal{L}_{\mathsf{no}}$.

   Using parts 1 and 2, that we can replace each oracle gate with a quantum circuit such that the output success probability only changed negligibly with this replacement.

4. **(Optional)** Write a conclusion proving that BQP is low.