# CSE 534 Autumn 2025: Set 4

Instructor: Chinmay Nirkhe
Due date: November 20th, 2025 11:59pm

**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; however, each team member must write and submit their own individual solution. Read the AI tools policy on the course webpage. Furthermore, 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 or abelian hidden subgroup problems 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** (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 $\rho_{AB}$ with the probability of outcome 0 is $1 - \epsilon$. Let $\rho'$ 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 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 a 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.

**Problem 4** (Magic States and the Cost of Non-Clifford Gates)**.** Universal quantum computation requires supplementing the Clifford group with a non-Clifford resource such as the $T$ gate or its associated *magic*

*state*. In this problem, you will analyze both the operational use of the magic state and its implications for computational complexity.

**Important:** The implementation of the $T$ gate from a magic state is described in the Nielsen–Chuang textbook (Sec. 10.6). Please *do not read that section* until after you have completed part (a) of this problem.

1. **(2 points)** Implementing a $T$ gate using the magic state.

   Let

   $$|T\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle + e^{i\pi/4}|1\rangle\big), \qquad T = \mathrm{diag}(1, e^{i\pi/4}).$$

   Show that if one can prepare copies of $|T\rangle$ and perform only Clifford gates and measurements in the computational basis, then a single-qubit $T$ gate can be realized using a single copy of $|T\rangle$ together with one measurement and a classically-controlled Clifford correction determined by the measurement outcome. Construct an explicit circuit implementing this procedure, and verify that the data qubit undergoes $T$ up to a known Pauli correction.

2. **(4 points)** Bounding the runtime via stabilizer decompositions.

   Suppose a quantum circuit $C$ acts on $n$ qubits, consists of Clifford operations, and contains $t$ applications of the $T$ gate. Assume that the joint magic-state resource can be written as

   $$|T\rangle^{\otimes t} = \sum_{j=1}^{J} c_j\,|\phi_j\rangle,$$

   where each $|\phi_j\rangle$ is a stabilizer state and the $c_j$ are complex coefficients. Prove that the total runtime of simulating $C$ (or equivalently, executing it on a stabilizer-based architecture) is upper-bounded by

   $$O\big(J \cdot \mathrm{poly}(n, t)\big).$$

   That is, argue that each stabilizer component contributes one stabilizer-circuit evaluation, and the amplitudes combine linearly with the coefficients $c_j$.

3. **(2 points)** When does magic-state decomposition make quantum computing easy?

   Let the *stabilizer rank* $\chi(t)$ denote the minimal $J$ for which the above decomposition exists. Determine what asymptotic scaling of $\chi(t)$ with respect to $t$ would imply that every $\mathsf{BQP}$ computation could be efficiently simulated classically (that is, $\mathsf{P} = \mathsf{BQP}$). Briefly justify your answer.