Quantum Algorithms – Final Exam

Spring 2025-26

This exam must be submitted in pairs and must be typed. Please register you and your partner to a pair in the course's Moodle now (before you start solving). You must answer all questions below (a non-obligatory bonus subquestion is indicated), based only on material covered during the semester. You may use the course materials. Do not use any LLMs, and do not consult anyone other than your partner. If you have questions or need clarification about the exam or any of its questions, feel free to email us (please include both `coheng@gmail.com` and `itaileigh@tauex.tau.ac.il`).

Submission is due on Tuesday at 12:00 (noon). To submit, make sure both partners are registered as the same pair in the "Couples for the Exam" Moodle unit. Then, one of you should submit the exam in the designated submission Moodle unit.

Good luck!
Gil & Itai

Clarifications or fixes added after the first publication will be coloured red.

1. Let $|u\rangle, |v\rangle \in \mathbb{C}^2$ be two fixed qubit states. We are given a state $|\psi\rangle \in \{|u\rangle, |v\rangle\}$ and our task is to determine which one it is.

   (a) Design a zero-error protocol, without using any auxiliary qubits, that maximizes the probability of success in the worst case, i.e. maximizes $\min\{\Pr[A(|u\rangle) \text{ declares "} |u\rangle \text{"}], \Pr[A(|v\rangle) \text{ declares "} |v\rangle \text{"}]\}$ where A is running the protocol (you do not need to prove that your protocol is optimal).

   (b) Give a better protocol using auxiliary qubits.

2. A simple undirected graph G on n vertices is given by the oracle $O|i,j,a\rangle = |i,j,a \oplus A_{ij}\rangle$, where A is the adjacency matrix of G. Give an $O(n^{3/2}\log n)$ query algorithm that calculates the number of connected components of G. The algorithm may fail with a constant probability strictly smaller than $\frac{1}{2}$.

3. Let s, t be two distinct n bit strings known to both Alice and Bob. Alice holds an n-qubit state of the form

$$|\psi\rangle = \alpha\,|s\rangle + \beta\,|t\rangle\,,$$

where $\alpha, \beta \in \mathbb{C}$ are unknown to her. ~~How many EPR pairs must Alice and Bob share, and how many classical bits must Alice communicate to Bob, in order to teleport $|\psi\rangle$ to Bob?~~ Give a protocol for Alice to teleport her state to Bob, using as few shared EPR pairs and communicating as few classical bits as you can (you do not need to prove that your protocol is optimal).

4. In this question we design a quantum-money scheme. To generate a fresh banknote, the bank samples uniformly at random a set of $\frac{n}{2}$ linearly independent vectors in $\mathbb{F}_2^n$, and lets S be their $\mathbb{F}_2$-span. The bank also computes a basis for the dual subspace

$$S^\perp := \{x \in \mathbb{F}_2^n : \forall s \in S,\ \langle x, s\rangle \equiv 0 \pmod 2\}, \qquad \text{where } \langle x, s\rangle := \sum_{i=1}^{n} x_i s_i.$$

The bank assigns the banknote a unique serial number, and stores in its database this serial number together with bases for S and for $S^\perp$. For this serial number, the bank issues the banknote state

$$|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{s\in S} |s\rangle\,.$$

This quantum state is the banknote given to customers.

To verify a purported banknote state $|\psi\rangle$, the bank performs the following two consistency checks:

Membership test: Measure whether the state $|\psi\rangle$ lies in $A := \mathrm{span}_{\mathbb{C}}\{|s\rangle : s \in S\}$ or its orthogonal subspace. Accept if the outcome is A.

Dual test: Apply the Hadamard transform $H^{\otimes n}$. Then measure whether $H^{\otimes n}|\psi\rangle$ lies in $B := \mathrm{span}_{\mathbb{C}}\{|x\rangle : x \in S^\perp\}$ or its orthogonal complement. Accept if the outcome is B.

The state is accepted if it passes both tests.

(a) How can the two tests be implemented efficiently?

(b) With what probability does a legitimate banknote $|S\rangle$ pass verification?

(c) Show how the bank can efficiently prepare the state $|S\rangle$.

(d) **Measurement attack:** Suppose a counterfeiter measures $|S\rangle$ in the computational basis and obtains some $x_0 \in S$. What is the probability that the state $|x_0\rangle$ passes verification?

5. In this question we consider a quantum analogue of a random walk. Consider the discrete-time quantum walk on $\mathbb{Z}$ with a "two-dimensional coin", formally defined as follows.

   The Hilbert space is spanned by orthonormal basis states $|x, c\rangle$, where $x \in \mathbb{Z}$ and $c \in \{0, 1\}$. One step of the walk is given by

   $$U = S\,(I \otimes H),$$

   where H is the Hadamard transform and S is the shift operator defined by

   $$S\,|x, 0\rangle = |x-1, 0\rangle\,, \qquad S\,|x, 1\rangle = |x+1, 1\rangle\,.$$

   The initial state is $|\psi_0\rangle = |0, 0\rangle$. For $t \geq 0$, write

   $$|\psi_t\rangle = \sum_{x\in\mathbb{Z}} (\alpha_t(x)\,|x, 0\rangle + \beta_t(x)\,|x, 1\rangle).$$

   (a) Compute $|\psi_t\rangle$ explicitly for $t = 1, 2, 3$. Group terms by position x.

   (b) Derive recurrence relations expressing $\alpha_{t+1}(x)$ and $\beta_{t+1}(x)$ in terms of the amplitudes at time t.

   (c) Prove that $\alpha_t(x) = \beta_t(x) = 0$ whenever $x \not\equiv t \pmod 2$.

   (d) Compute $\Pr[X_4 = 0]$, where X_t denotes the measured position at time t.

Bonus: By explicitly computing $\Pr[X_t = 0]$ for several small values of t, look for a pattern and make an educated guess for the general behavior of $\Pr[X_t = 0]$ as a function of t. In particular, does it appear to decrease to 0? If so, how fast compared to the classical unbiased random walk on $\mathbb{Z}$?

6. Let C_n be the undirected cycle on n vertices. In the nth odd-cycle game (for odd n), the players Alice and Bob are each given a vertex of the cycle, $x, y \in C_n$, and must respond with bits $a, b \in \{0, 1\}$.

   If they receive the same vertex ($x = y$), they win iff their answers match ($a = b$). If they receive different vertices ($x \neq y$), they win iff their answers differ ($a \neq b$).

   The referee chooses (x, y) as follows:

   - With probability $\frac{1}{2}$, set $x = y$, where x is chosen uniformly at random from C_n.
   - With probability $\frac{1}{2}$, choose x and y to be a uniformly random pair of adjacent vertices in C_n.

   (a) What is the maximum classical winning probability?

   (b) Show that there is a quantum strategy that wins this game with probability $1 - O\big(\frac{1}{n^2}\big)$.