Midterm Exam 2026
Quantum Computation

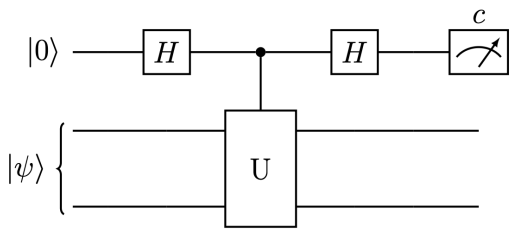
Instructions: Please start each problem on a new page. Write your SCIPER number and the problem number at the top of each page.

There are three exercises, for a total of 43 points. 2 points will be given for good presentation, so the midterm will be graded on a total of 45 points. In addition, the last question of the last problem gives 3 bonus points. (This means that the points will count towards this midterm, unless your total already reaches the max of 45.)

Please pay attention to the presentation of your answers! (2 points)

Exercise 1 *The U-Test (12 points).*

1. (2 pts) Consider the "controlled-U test" for some unitary operator $U : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$:



   Given the initial state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ and a measurement stored in a classical bit c, show that we have the following probability:

$$p_0 = \Pr(c = 0) = \frac{1}{2}\big(1 + \mathrm{Re}(\langle\psi|U|\psi\rangle)\big) \ . \tag{1}$$

2. (2 pts) *SWAP Test.* Say U is the swap operator such that for any $|u\rangle,\ |v\rangle \in \mathbb{C}^2 \times \mathbb{C}^2$, we have $U(|u\rangle \otimes |v\rangle) = |v\rangle \otimes |u\rangle$.

   (a) What is p_0 for $|\psi\rangle = |u\rangle \otimes |v\rangle$? (Give the solution in terms of $\langle u \mid v\rangle$.)

   (b) What is p_0 for $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$? (Give the numerical value of p_0.)

3. (2 pts) Now suppose that $U = H \otimes H$.

   (a) Suppose further that $|u\rangle, |v\rangle \in \{|0\rangle, |1\rangle\}$. In that case, what is p_0 for $|\psi\rangle = |u\rangle \otimes |v\rangle$? (Give the numerical value of p_0, and distinguish cases if you need to.)

(b) What is p_0 for $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$? (Give the numerical value of p_0.)

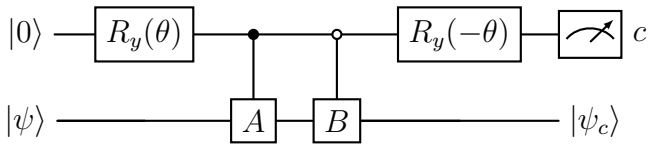
4. (6 pts) *Linear Combination of Unitaries.* As you have learned in class, quantum gates are unitary operations. However, some applications of quantum computation require applying a non-unitary map to a quantum state. This can be achieved using ancilla qubits together with *post-selection*, where we keep the state only when specific measurement outcomes are obtained on the ancilla. In this exercise, you will show how post-selection can be used to implement maps of the form $\alpha \cdot A + \beta \cdot B$ for generic unitaries A, B and $\alpha, \beta \in \mathbb{R}_{\geq 0}$ such that $\alpha + \beta = 1$.

(a) (This question is not subsequently used.) Let's work out an example of such decomposition. Consider the following linear operation:

$$M = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \text{ with } |b| \leq 1$$

To implement M, how should you choose α, β, A, B? (There may be more than one possibility; it is enough to give one.)

Now let's see how such operations could be implemented. Consider the following circuit:



Here, the open control symbol ($\circ$) denotes a control conditioned on the control qubit being in the state $|0\rangle$. That is, gate B is applied if and only if the control qubit is in state $|0\rangle$, and does nothing otherwise. Furthermore, the gate $R_y(\theta)$ is defined by

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} .$$

(b) Compute the quantum state of this circuit just before the ancilla measurement as a function of θ. Write this state in the form

$$|\psi_{final}\rangle = \sum_{c \in \{0,1\}} |c\rangle\,|\psi_c\rangle \ ,$$

where $|\psi_0\rangle$ and $|\psi_1\rangle$ are (not necessarily normalized) states that you will specify explicitly, as a function of θ, A and B.

The measurement rule stipulates that, if we measure an outcome c, then the state in the second qubit becomes equal to $|\psi_c\rangle$ (renormalized).

(c) Suppose that we would like to compute $(\alpha \cdot A + \beta \cdot B)\,|\psi\rangle$, where $\alpha, \beta \in \mathbb{R}_{\geq 0}$ are given parameters such that $\alpha + \beta = 1$. Based on your answer to the previous question, Which measurement outcome c will allow us to achieve this, and what is the correct choice of θ?

Exercise 2 *A quantum algorithm for the discrete logarithm problem (20 points).*

Let $M \geq 2$ be an integer. As usual, we denote by $\mathbb{Z}_M$ the set $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$, together with addition modulo M. Furthermore, let $\mathbb{Z}_M^*$ denote the group of invertible integers modulo M (i.e., those $a \in \mathbb{Z}_M$ with $\gcd(a, M) = 1$). In the discrete logarithm problem, we are given:

- an integer $M \geq 1$,
- a generator $g \in \mathbb{Z}_M^*$, i.e.,

$$\{g^0, g^1, \ldots, g^{N-1}\} = \mathbb{Z}_M^* \ , \quad \text{where } N = |\mathbb{Z}_M^*| \ ,$$

- an element $a \in \mathbb{Z}_M^*$.

We assume that N is also known. The goal is to find the discrete logarithm of a, i.e. the element $\ell \in \mathbb{Z}_N$ such that

$$g^\ell \equiv a \pmod{M}. \tag{2}$$

It is possible to find ℓ by computing $g \pmod{M}, g^2 \pmod{M}, \ldots$, but that risks taking around $O(M)$ multiplications in the worst case. Our goal in this problem is to design and analyze a much faster quantum algorithm.

Consider the function $f : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_M^*$ defind by

$$f(x, y) = a^x g^y \pmod{M}. \tag{3}$$

As a warm-up, let us first investigate a numeric example.

1. (2 pts) Take $M = 7$, $N = 6$, $g = 3$, $a = 2$. Plot the values taken by the function f as a 6×6 table of integers $\pmod{M}$, with rows indexed by $x \in \{0, \ldots, 5\}$ and columns indexed by $y \in \{0, \ldots, 5\}$. Do you see any pattern? Find the value of ℓ such that $g^\ell \equiv a \pmod{M}$ in this case. (For your solution, you only need to fill in the table and return the value of ℓ. You do not need to say what you see on the table. But it will help you understand the next questions.)

We now investigate the periodic nature of f.

2. (2 pts) Define

$$H = \{(t, -\ell t) : t \in \mathbb{Z}_N\}.$$

Show that H is a subgroup of $\mathbb{Z}_N \times \mathbb{Z}_N$. (Recall that a set X together with an addition law $+$ is a subgroup if for all $x, y \in X$, $x + y \in X$ and there is $x' \in X$ such that $x + x' = 0 \in X$. Here, X is formed of pairs of elements from $\mathbb{Z}_N$ and addition is componentwise.)

3. (2 pts) For any $(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N$ we define the "shifted set", also known as a *coset*, of H:
$$(x, y) + H = \{(x + t, y - \ell t) : t \in \mathbb{Z}_N\}.$$
Show that the function f is constant on cosets, i.e. for any (x, y), $f(a, b) = f(a', b')$ whenever $(a, b), (a', b') \in (x, y) + H$.

4. (2 pts) Show that f takes distinct values on distinct cosets: if $(x, y) + H \neq (x', y') + H$ then $f(a, b) \neq f(a', b')$ for any $(a, b) \in (x, y) + H$ and $(a', b') \in (x', y') + H$.

Given that the function f is a product of two exponentiations, it is reasonable to assume that we can come up with a simple circuit that implements the unitary map
$$O_f : |x\rangle|y\rangle|z\rangle \mapsto |x\rangle|y\rangle|z \oplus f(x, y)\rangle,$$
where $x, y \in \mathbb{Z}_N$ and $z \in \{0, 1\}^m$, with $m = \lceil \log_2(M) \rceil$, so that the third register can be used to encode elements of $\mathbb{Z}_M^*$ as binary strings. (You are not asked to come up with such a circuit.)

Using this, we design the following circuit.

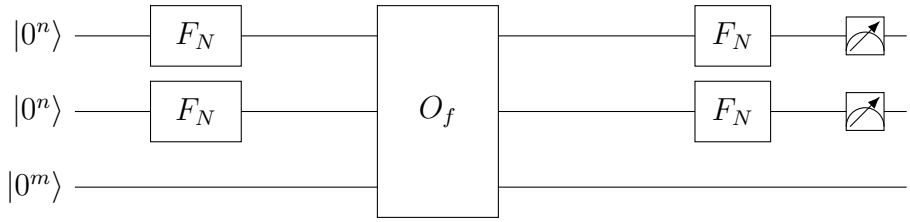


Figure 1: Quantum circuit for the discrete logarithm.

Here, the first two wires are each a register of $n = \lceil \log_2(N) \rceil$ qubits. We write a basis of each such register as $|0\rangle$ (written $|0^n\rangle$ on the circuit to emphasize the number of qubits), $|1\rangle, \ldots, |N-1\rangle$.[1] The third wire has dimension 2^m. Furthermore, F_N denotes the unitary that implements the Fourier transform over $\mathbb{Z}_N$,
$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{\gamma \in \mathbb{Z}_N} \omega_N^{-\gamma x} |\gamma\rangle \ ,$$
where $\omega_N = e^{2\pi i/N}$. Finally, the oracle O_f is described above and the last gates on the right hand side are measurement gates.

5. (4 pts) Write down the full quantum states $|\psi_a\rangle, |\psi_b\rangle, |\psi_c\rangle, |\psi_d\rangle$ of the circuit, at the initialization (a), after F_N is applied to the first two registers (b), after application of O_f (c), and at the last step (before measurement) (d).

6. (4 pts) Rewrite $|\psi_d\rangle$ as a state of the form
$$|\psi_d\rangle = \sum_{(\alpha,\beta) \in \mathbb{Z}_N \times \mathbb{Z}_N} |\alpha, \beta\rangle \left|\varphi_{(\alpha,\beta)}\right\rangle \ , \tag{4}$$

[1] If $2^n > N$ is not a power of two, not all the space is used, but we do not worry about that.

where for each pair (α, β), $\left|\varphi_{(\alpha,\beta)}\right\rangle$ is a vector that you will describe explicitly (and may not be normalized).

7. (2 pts) Suppose that the first two registers $|\alpha, \beta\rangle$ are measured. Show that the outcome distribution obtained is uniform over all pairs (α, β) such that $\alpha = \ell\beta \pmod N$. How many such pairs are there? *Hint:* Use questions 3. and 4.

Recall that an element $z \in \mathbb{Z}_N$ is invertible if and only if $\gcd(z, N) = 1$. For example, 2 has an inverse in $\mathbb{Z}_{15}$, because $2 \cdot 8 = 1 \pmod{15}$, but 3 does not. The Euler totient function $\varphi(N)$ counts the number of elements of $\mathbb{Z}_N$ that are invertible, and it satisfies $\varphi(N) = O(N/\log\log N)$ as $N \to \infty$.

8. (2 pts) What is the condition on (α, β) for it to be possible to recover ℓ from them? What fraction of the N pairs (α, β) sampled from the distribution in question 7 allows recovery of ℓ, as a function of N? What happens to this fraction as $N \to \infty$?

Exercise 3 *2- and 3-qubit gate decompositions (11 points + 3 bonus points).*

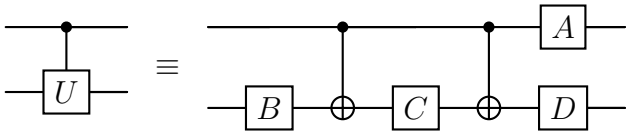
In this problem, we will use the fact that any single-qubit unitary U can be decomposed into the form

$$U = e^{i\alpha} R_z(2\beta) R_y(2\gamma) R_z(2\delta) \,, \tag{5}$$

for $\alpha \in [0, 2\pi), \beta, \gamma, \delta \in [0, \pi)$ and the rotation gates

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \,, \qquad R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \,.$$

Now, let us investigate arbitrary two- and three-qubit gate constructions: Assuming that we have at our disposal only CNOT gates, we claim that we can realize an arbitrary controlled gate U with two CNOTs and four single qubit rotations using the following quantum circuit:



1. (2 pts) What is the definition of a controlled-U gate? Write it down in terms of its action on a product state:

$$|\psi\rangle|\phi\rangle = (c_0|0\rangle + c_1|1\rangle)|\phi\rangle \,.$$

2. (2 pts) What is the action of the equivalent quantum circuit (in terms of single-qubit gates A, B, C, D) on the same state?

3. (2 pts) Give the two conditions that the gates B, C and D should satisfy, for the two actions, in question 1 and 2, to match. Deduce a formula for gate A.

   Hint: Make use of the explicit form of the unitary U given in Eq. (5).

4. (3 pts) Let us define the gates B, C and D as follows:

$$B = R_z(\delta - \beta), \qquad C = R_y(-\gamma)R_z(-\delta - \beta), \qquad D = R_z(2\beta)R_y(\gamma).$$

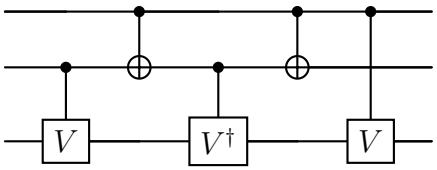
   Verify that they satisfy the two conditions from question 3.

   Hint: To simplify your calculations, you may use that

$$R_x(\theta) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X$$
$$R_y(\theta) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y$$
$$R_z(\theta) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Z \ ,$$

   and use (without proof) the identities $XR_y(\theta)X = R_y(-\theta)$, $XR_z(\theta)X = R_z(-\theta)$.

Now consider the following quantum circuit for some unitary V:



5. (2 pts) Evaluate the action of this circuit on all 8 computational basis states. If you were to give a name to the gate that the circuit implements, what would you call it?

6. (Bonus 3 pts) Now suppose that

$$V = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

   In this case, recognize a circuit implementation for a certain gate seen in class.