Midterm Exam 2026
Solution
Quantum Computation

Exercise 1 *The U-Test.*

1.

$$|\psi_1\rangle = (H \otimes I)CU((H|0\rangle) \otimes |\psi\rangle) = \frac{1}{\sqrt{2}}(H \otimes I)CU(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle) \tag{1}$$

$$= \frac{1}{\sqrt{2}}(H \otimes I)(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U|\psi\rangle) \tag{2}$$

$$= \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes U|\psi\rangle \tag{3}$$

$$= \frac{1}{2}|0\rangle \otimes (|\psi\rangle + U|\psi\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi\rangle - U|\psi\rangle) \tag{4}$$

So:

$$p_0 = \langle\psi_1| \left(|0\rangle\langle 0| \otimes I\right) |\psi_1\rangle \tag{6}$$

$$= \frac{1}{4}\left(\langle\psi| + \langle\psi|U^\dagger\right)\left(|\psi\rangle + U|\psi\rangle\right) \tag{7}$$

$$= \frac{1}{4}\left(\langle\psi \mid \psi\rangle + \langle\psi|U|\psi\rangle + \langle\psi|U^\dagger|\psi\rangle + \langle\psi|U^\dagger U|\psi\rangle\right) \tag{8}$$

$$= \frac{1}{2}(1 + \mathrm{Re}(\langle\psi|U|\psi\rangle)) \tag{9}$$

2. For the SWAP operator:
   (a) $U|u\rangle \otimes |v\rangle = |v\rangle \otimes |u\rangle$ and $\langle v|u\rangle = \overline{\langle u|v\rangle}$, so:
   $$p_0 = \frac{1}{2}\left(1 + |\langle u \mid v\rangle|^2\right)$$
   (b) for the Bell state, $U|\psi\rangle = |\psi\rangle$ so $p_0 = 1$.
3. for the double Hadamard gate:
   (a) if $|\psi\rangle = |u\rangle \otimes |v\rangle$ for $u, v \in \{0, 1\}$, then $(H \otimes H)|\psi\rangle = \frac{1}{2}\left(|0\rangle + (-1)^u|1\rangle\right) \otimes (|0\rangle + (-1)^v|1\rangle)$ so:
   $$p_0 = \begin{cases} 3/4 \text{ if } u = v \\ 1/4 \text{ if } u \neq v \end{cases}$$

(b) for the Bell state, we find:

$$(H \otimes H)|\psi\rangle = \frac{1}{2\sqrt{2}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) + (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)]$$
$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\psi\rangle$$

So we find again $p_0 = 1$.

4. (a) Choose $\alpha = \frac{1+b}{2}$, $\beta = \frac{1-b}{2}$, $A = I$ and $B = Z$.

   (b) The state of the circuit before the ancilla is measured is

$$|0\rangle \left(\sin^2\left(\tfrac{\theta}{2}\right) A + \cos^2\left(\tfrac{\theta}{2}\right) B\right) |\psi\rangle + |1\rangle \sin\left(\tfrac{\theta}{2}\right) \cos\left(\tfrac{\theta}{2}\right) (A - B) |\psi\rangle$$

   The post-measurement states (up to normalisation) are:

$$|\psi_0\rangle = \left(\sin^2\left(\tfrac{\theta}{2}\right) A + \cos^2\left(\tfrac{\theta}{2}\right) B\right) |\psi\rangle$$
$$|\psi_1\rangle = \sin\left(\tfrac{\theta}{2}\right) \cos\left(\tfrac{\theta}{2}\right) (A - B) |\psi\rangle$$

   (c) Post-selecting on $c = 0$ and setting $\theta = 2 \arcsin(\sqrt{\alpha})$ yields the desired mapping.

Exercise 2 *A quantum algorithm for the discrete logarithm problem.*

Solution. Throughout the solution, all additions in the exponents are understood modulo N. Since g is a generator of $\mathbb{Z}_M^*$ and $N = |\mathbb{Z}_M^*|$, the order of g is N. Therefore

$$g^r \equiv g^s \pmod{M} \qquad \Longleftrightarrow \qquad r \equiv s \pmod{N}.$$

Moreover, since $a = g^\ell$, we will repeatedly use

$$f(x, y) = a^x g^y \equiv g^{\ell x + y} \pmod{M}.$$

1. For $M = 7$, $N = 6$, $g = 3$ and $a = 2$, the powers of g modulo 7 are

$$3^0, 3^1, 3^2, 3^3, 3^4, 3^5 \equiv 1, 3, 2, 6, 4, 5 \pmod{7}.$$

   Thus $3^2 \equiv 2 \pmod{7}$, so

$$\ell = 2 \in \mathbb{Z}_6.$$

   The values of $f(x, y) = 2^x 3^y \pmod{7}$ are as follows:

$x \backslash y$	0	1	2	3	4	5
0	1	3	2	6	4	5
1	2	6	4	5	1	3
2	4	5	1	3	2	6
3	1	3	2	6	4	5
4	2	6	4	5	1	3
5	4	5	1	3	2	6

2. We show that
$$H = \{(t, -\ell t) : t \in \mathbb{Z}_N\}$$
is a subgroup of $\mathbb{Z}_N \times \mathbb{Z}_N$. First, H is nonempty because taking $t = 0$ gives $(0, 0) \in H$. If $(t, -\ell t), (s, -\ell s) \in H$, then
$$(t, -\ell t) + (s, -\ell s) = (t + s, -\ell(t + s)) \in H,$$
so H is closed under addition. Finally, the inverse of $(t, -\ell t)$ is
$$(-t, \ell t) = (-t, -\ell(-t)) \in H.$$
Thus H is a subgroup.

3. Let $(u, v) \in (x, y) + H$. Then there exists $t \in \mathbb{Z}_N$ such that
$$(u, v) = (x + t, y - \ell t).$$
Therefore
$$\begin{aligned} f(u, v) &= f(x + t, y - \ell t) \\ &= a^{x+t} g^{y-\ell t} \\ &= a^x g^y \, a^t g^{-\ell t} \\ &= a^x g^y \, g^{\ell t} g^{-\ell t} \\ &= a^x g^y \\ &= f(x, y). \end{aligned}$$
Hence f is constant on each coset $(x, y) + H$. In particular, if (u, v) and (u', v') are both in the same coset, then
$$f(u, v) = f(x, y) = f(u', v').$$

4. We prove the contrapositive. Suppose
$$f(u, v) = f(u', v').$$
Using $f(x, y) = g^{\ell x + y}$, this means
$$g^{\ell u + v} \equiv g^{\ell u' + v'} \pmod{M}.$$
Since g has order N, we get
$$\ell u + v \equiv \ell u' + v' \pmod{N}.$$
Equivalently,
$$v' - v \equiv -\ell(u' - u) \pmod{N}.$$
Let $t = u' - u$. Then
$$(u', v') = (u + t, v - \ell t) \in (u, v) + H.$$
Thus $(u', v') + H = (u, v) + H$. Therefore, if two cosets are distinct, the function values on them must be distinct.

5. The initial state is

$$|\psi_a\rangle = |0\rangle\,|0\rangle\,|0^m\rangle\,.$$

After applying F_N to the first two registers, we get

$$|\psi_b\rangle = \frac{1}{N}\sum_{x,y\in\mathbb{Z}_N} |x\rangle\,|y\rangle\,|0^m\rangle = \frac{1}{N}\sum_{x,y\in\mathbb{Z}_N} |x,y\rangle\,|0^m\rangle\,.$$

Applying the oracle O_f gives

$$|\psi_c\rangle = \frac{1}{N}\sum_{x,y\in\mathbb{Z}_N} |x,y\rangle\,|f(x,y)\rangle\,,$$

where $|f(x,y)\rangle$ denotes the binary encoding of $f(x,y)$ in the third register.

Finally, applying F_N again to the first two registers gives

$$\begin{aligned}|\psi_d\rangle &= \frac{1}{N}\sum_{x,y\in\mathbb{Z}_N}\left(\frac{1}{\sqrt{N}}\sum_{\alpha\in\mathbb{Z}_N}\omega_N^{-\alpha x}\,|\alpha\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{\beta\in\mathbb{Z}_N}\omega_N^{-\beta y}\,|\beta\rangle\right)|f(x,y)\rangle\\ &= \frac{1}{N^2}\sum_{\alpha,\beta,x,y\in\mathbb{Z}_N}\omega_N^{-(\alpha x+\beta y)}\,|\alpha,\beta\rangle\,|f(x,y)\rangle\,.\end{aligned}$$

6. From the expression above,

$$|\psi_d\rangle = \sum_{(\alpha,\beta)\in\mathbb{Z}_N\times\mathbb{Z}_N} |\alpha,\beta\rangle\,\big|\varphi_{(\alpha,\beta)}\big\rangle\,,$$

where

$$\big|\varphi_{(\alpha,\beta)}\big\rangle = \frac{1}{N^2}\sum_{x,y\in\mathbb{Z}_N}\omega_N^{-(\alpha x+\beta y)}\,|f(x,y)\rangle\,.$$

We can make this expression more explicit by grouping the sum over cosets of H. Let R be any set of representatives for the cosets of H in $\mathbb{Z}_N\times\mathbb{Z}_N$. Since $|\mathbb{Z}_N\times\mathbb{Z}_N| = N^2$ and $|H| = N$, there are exactly N cosets, so $|R| = N$. For a representative $(x_0,y_0)\in R$, the corresponding coset is

$$(x_0,y_0)+H = \{(x_0+t,\,y_0-\ell t) : t\in\mathbb{Z}_N\}.$$

Using the fact that f is constant on this coset, we obtain

$$\begin{aligned}\big|\varphi_{(\alpha,\beta)}\big\rangle &= \frac{1}{N^2}\sum_{(x_0,y_0)\in R}\sum_{t\in\mathbb{Z}_N}\omega_N^{-(\alpha(x_0+t)+\beta(y_0-\ell t))}\,|f(x_0,y_0)\rangle\\ &= \frac{1}{N^2}\sum_{(x_0,y_0)\in R}\omega_N^{-(\alpha x_0+\beta y_0)}\left(\sum_{t\in\mathbb{Z}_N}\omega_N^{-t(\alpha-\ell\beta)}\right)|f(x_0,y_0)\rangle\,.\end{aligned}$$

The inner geometric sum is

$$\sum_{t\in\mathbb{Z}_N}\omega_N^{-t(\alpha-\ell\beta)} = \begin{cases}N, & \text{if } \alpha\equiv\ell\beta \pmod N,\\ 0, & \text{otherwise.}\end{cases}$$

Therefore

$$\left|\varphi_{(\alpha,\beta)}\right\rangle = \begin{cases} \dfrac{1}{N} \displaystyle\sum_{(x_0,y_0)\in R} \omega_N^{-(\alpha x_0+\beta y_0)} \left|f(x_0,y_0)\right\rangle, & \text{if } \alpha \equiv \ell\beta \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$

7. The probability of observing a given pair (α, β) in the first two registers is

$$\Pr(\alpha,\beta) = \left\| \left|\varphi_{(\alpha,\beta)}\right\rangle \right\|^2.$$

From the previous question, this probability is 0 unless

$$\alpha \equiv \ell\beta \pmod{N}.$$

Now suppose $\alpha \equiv \ell\beta \pmod{N}$. We showed that

$$\left|\varphi_{(\alpha,\beta)}\right\rangle = \frac{1}{N} \sum_{(x_0,y_0)\in R} \omega_N^{-(\alpha x_0+\beta y_0)} \left|f(x_0,y_0)\right\rangle.$$

By Question 4, distinct cosets give distinct function values. Therefore the states

$$\left|f(x_0,y_0)\right\rangle, \qquad (x_0,y_0) \in R,$$

are distinct computational basis states and hence orthonormal. Thus

$$\Pr(\alpha,\beta) = \frac{1}{N^2} \sum_{(x_0,y_0)\in R} 1 = \frac{|R|}{N^2} = \frac{N}{N^2} = \frac{1}{N}.$$

Hence the measurement outcome is uniform over the pairs satisfying

$$\alpha \equiv \ell\beta \pmod{N}.$$

There are exactly N such pairs, one for each choice of $\beta \in \mathbb{Z}_N$, namely

$$(\alpha,\beta) = (\ell\beta,\beta).$$

8. From the measurement we obtain a pair satisfying

$$\alpha \equiv \ell\beta \pmod{N}.$$

To recover ℓ uniquely from this congruence, β must be invertible in $\mathbb{Z}_N$, i.e.

$$\gcd(\beta, N) = 1.$$

In that case,

$$\ell \equiv \alpha\beta^{-1} \pmod{N}.$$

If β is not invertible, then multiplication by β is not injective modulo N, and the congruence $\alpha \equiv \ell\beta \pmod{N}$ does not determine ℓ uniquely in general.

Since the distribution from Question 7 is uniform over the N pairs

$$(\ell\beta, \beta), \qquad \beta \in \mathbb{Z}_N,$$

the fraction of outcomes that allow recovery of ℓ is exactly the fraction of invertible elements $\beta \in \mathbb{Z}_N$. Hence this fraction is

$$\frac{\varphi(N)}{N}.$$

This is the exact success probability for one run of the algorithm. Using the estimate provided in the question, in the worst case this ratio can be as small as order $1/\log\log N$. Thus the one-run success probability is at worst inverse-loglogarithmic in N; repeating the procedure $O(\log\log N)$ times gives an invertible β with constant probability.

Exercise 3 *2- and 3-qubit gate decompositions*

1. A controlled- U gate acts as:

$$CU\ |\psi\rangle \otimes |\phi\rangle = c_0\,|0\rangle \otimes |\phi\rangle + c_1\,|1\rangle \otimes U\,|\phi\rangle\,,$$

where $|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle$.

2. The circuit corresponds to the unitary:

$$(A \otimes D)\,\mathrm{CNOT}\,(I \otimes C)\,\mathrm{CNOT}\,(I \otimes B).$$

Its action on $|\psi\rangle \otimes |\phi\rangle$ is:

$$c_0 A\,|0\rangle \otimes (DCB)\,|\phi\rangle + c_1 A\,|1\rangle \otimes (DXCXB)\,|\phi\rangle\,.$$

3. To implement a controlled-U gate:

$$A = \mathrm{diag}(1, e^{i\alpha}).$$

The remaining gates must satisfy:

$$\begin{aligned} DCB &= I, \\ DXCXB &= R_z(2\beta)R_y(2\gamma)R_z(2\delta). \end{aligned}$$

Note: It may be tempting to set $A = I$. If one tries that, the system of equations becomes:

$$DCB = I, \tag{1}$$

$$DXCXB = e^{i\alpha}R_z(2\beta)R_y(2\gamma)R_z(2\delta)\ . \tag{2}$$

You can see this method fails by taking the determinants in both sides of these equations, and then using the multiplicative property of the determinant. The first equation implies:

$$|D|\,|C|\,|B| = 1 \tag{3}$$

And the second

$$|D|\,|C|\,|B| = e^{2i\alpha}\,, \tag{4}$$

a contradiction whenever α is arbitrary.

4. Given:

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

we verify:

First condition:

$$\begin{aligned} DCB &= R_z(2\beta)R_y(\gamma)R_y(-\gamma)R_z(-\delta - \beta)R_z(\delta - \beta) \\ &= I. \end{aligned}$$

Second condition: Using $XR_y(\theta)X = R_y(-\theta)$ and $XR_z(\phi)X = R_z(-\phi)$:

$$\begin{aligned} DXCXB &= R_z(2\beta)R_y(\gamma)XR_y(-\gamma)R_z(-\delta - \beta)XR_z(\delta - \beta) \\ &= R_z(2\beta)R_y(\gamma)R_y(\gamma)R_z(\delta + \beta)R_z(\delta - \beta) \\ &= R_z(2\beta)R_y(2\gamma)R_z(2\delta). \end{aligned}$$

5. Evaluating the circuit on computational basis states:

$$\begin{aligned} |000\rangle &\to |000\rangle\,, \\ |001\rangle &\to |001\rangle\,, \\ |010\rangle &\to |010\rangle\,, \\ |011\rangle &\to |011\rangle\,, \\ |100\rangle &\to |100\rangle\,, \\ |101\rangle &\to |101\rangle\,, \\ |110\rangle &\to |11\rangle \otimes V^2\,|0\rangle\,, \\ |111\rangle &\to |11\rangle \otimes V^2\,|1\rangle\,. \end{aligned}$$

Thus, the circuit implements a controlled-controlled-U gate with:

$$U = V^2.$$

6. Given:

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

we recognize $V = \sqrt{X}$, hence:

$$U = V^2 = X.$$

Therefore, the circuit implements a **Toffoli gate**.