CMPT 476/981: Introduction to Quantum Algorithms
Assignment 2 Solutions

Due **February 1st, 2024 at 11:59pm on coursys**
Complete individually and submit in PDF format.

Question 1 [3 points]: Optimal angles for the Zeno effect

In class we saw that we can *drag* a state from the $|0\rangle$ state to the $|1\rangle$ state by performing measurements in rotated bases. Given a basis $\mathcal{B} = \{|A\rangle, |B\rangle\}$ define the basis $\mathcal{B}$ *rotated* by an angle θ to be $\{\cos(\theta)|A\rangle + \sin(\theta)|B\rangle, -\sin(\theta)|A\rangle + \cos(\theta)|B\rangle\}$. Observe that this basis is in fact orthonormal via the identity $\cos^2(\theta) + \sin^2(\theta) = 1$.

1. Show that rotating the basis twice by θ is the same as rotating once by an angle of 2θ
2. Calculate the angle θ and number of measurements needed to reach the $|1\rangle$ state with success probability **at least** p for some positive real number p close to 1.

   Note: Assume that $\sin^2(x) = x^2$ when x is close to 0. **You will likely need to use the union bound, i.e. Boole's inequality**

   $$pr(A \vee B \vee C \vee \cdots) \leq pr(A) + pr(B) + pr(C) + \cdots$$

Solution.

1. Rotating the basis $\{|A\rangle, |B\rangle\}$ once by θ results in the basis $\{|A'\rangle, |B'\rangle\}$, where

   $$\begin{aligned} |A'\rangle &= \cos\theta|A\rangle + \sin\theta|B\rangle, \\ |B'\rangle &= -\sin\theta|A\rangle + \cos\theta|B\rangle. \end{aligned}$$

   Rotating this basis by θ results in the basis $\{|A''\rangle, |B''\rangle\}$, where

   $$\begin{aligned} |A''\rangle &= \cos\theta|A'\rangle + \sin\theta|B'\rangle \\ &= \cos^2\theta|A\rangle + \cos\theta\sin\theta|B\rangle - \sin^2\theta|A\rangle + \sin\theta\cos\theta|B\rangle \\ &= (\cos^2\theta - \sin^2\theta)|A\rangle + 2\sin\theta\cos\theta|B\rangle \\ &= \cos 2\theta|A\rangle + \sin 2\theta|B\rangle, \end{aligned}$$

and

$$\begin{aligned}|B''\rangle &= -\sin\theta|A'\rangle + \cos\theta|B'\rangle \\ &= -\sin\theta\cos\theta|A\rangle - \sin^2\theta|B\rangle - \cos\theta\sin\theta|A\rangle + \cos^2\theta|B\rangle \\ &= -\sin 2\theta|A\rangle + \cos 2\theta|B\rangle.\end{aligned}$$

This is precisely the basis obtained if the original basis $\{|A\rangle, |B\rangle\}$ is rotated by 2θ.

2. We start with the state $|0\rangle$. Given θ, we attempt to rotate $|0\rangle$ by θ by measuring in the basis $\{|A\rangle, |B\rangle\} = \{\cos\theta|0\rangle + \sin\theta|1\rangle, -\sin\theta|0\rangle + \cos\theta|1\rangle\}$. We get the state $|A\rangle$ with probability $|\langle A|0\rangle|^2 = \cos^2\theta$ and we get $|B\rangle$ with probability $\sin^2\theta$. We then attempt to rotate by θ again by measuring in the basis $\{\cos(\theta)|A\rangle + \sin(\theta)|B\rangle, -\sin(\theta)|A\rangle + \cos(\theta)|B\rangle\}$, and so on. If θ is small, with high probability we will get the 'A' basis vector after each measurement, so that after n measurements we are very likely to have the state $\cos n\theta|0\rangle + \cos n\theta|1\rangle$. After approximately $\pi/(2\theta)$ measurements we get, with high probability (the success probability), the state $|1\rangle$.

   Now we need to find an (approximate) expression for θ in terms of the success probability p. A way to get a nice approximate expression is to find an upper bound for $p_f = 1 - p$, the probability of failure. Using $B_i A_{i-1} \cdots A_1$ to mean the random event where the first $i-1$ measurement results are 'A' and the ith measurement result is 'B', we have

$$\begin{aligned}p_f &= pr(\text{we get a 'B' state after some number of measurements}) \\ &\leq pr\left(\bigvee_i B_i A_{i-1} \cdots A_1\right) \\ &\leq \sum_i pr(B_i | A_{i-1} \cdots A_1) pr(A_{i-1} \cdots A_1) \\ &\leq \sum_i pr(B_i | A_{i-1} \cdots A_1) \\ &= \frac{\pi \sin^2\theta}{2\theta} \\ &\approx \frac{\pi\theta^2}{2\theta} = \frac{\pi\theta}{2}.\end{aligned}$$

   Therefore, we have $\pi\theta/2 = 1 - p$, so $\theta = (2 - 2p)/\pi$. The number of measurements is approx. $\pi^2/(4 - 4p)$.

Question 2 [2 points]: State discrimination

Using computational basis measurement, H gates, and *phase gates*

$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

where θ can be any real number, give a protocol to distinguish with 100% accuracy between the states

$$|\psi\rangle = \frac{1}{\sqrt{2}}(e^{i\pi/4}|0\rangle + |1\rangle), \qquad |\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i3\pi/4}|1\rangle)$$

Solution. If we apply $T = P(\pi/4)$ to each state, we get

$$T|\psi\rangle = \frac{1}{\sqrt{2}}(e^{i\pi/4}|0\rangle + e^{i\pi/4}|1\rangle), \quad T|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

so that if we next apply H, we get

$$HT|\psi\rangle = e^{i\pi/4}|0\rangle, \quad HT|\phi\rangle = |1\rangle.$$

Finally, we measure in the computational basis. If we get an outcome of 0, then we know with certainty that our state was $|\psi\rangle$, and if we get an outcome of 1, then we know with certainty that our state was $|\phi\rangle$.

Question 3 [4 points]: Pauli operators

Recall the definition of the I, X, Z, and Y gates:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

These are known as the *Pauli matrices* or gates.

1. Compute the matrices $X \otimes Z$ and $Z \otimes X$
2. Show that the non-identity Pauli matrices anti-commute: that is, $UV = -VU$ for every pair of X, Y, and Z matrices where $U \neq V$
3. Show that the Pauli matrices I, X, Z, Y are linearly independent
4. Show that the Pauli matrices form a basis for the space of 2×2 complex-valued matrices.

Solution.

1. $X \otimes Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad Z \otimes X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$

2. It's easy to check that $X^2 = Y^2 = Z^2 = I$. Now, we find $ZX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iY$ and $XZ = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -iY$. Thus, X and Z anti-commute. Furthermore, we can now also deduce that

$$XY = X(iXZ) = iX^2Z = iZ \quad \text{and} \quad YX = (-iZX)X = -iZX^2 = -iZ;$$
$$YZ = (iXZ)Z = iXZ^2 = iX \quad \text{and} \quad ZY = Z(-iZX) = -iZ^2X = -iX$$

as required.

3. Let $\alpha, \beta, \gamma, \delta$ be scalars such that $\alpha I + \beta Z + \gamma X + \delta Y = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Thus we have

$$\begin{aligned} \alpha + \beta &= 0, \\ \gamma - i\delta &= 0, \\ \gamma + i\delta &= 0, \\ \alpha - \beta &= 0, \end{aligned}$$

and solving these equations simultaneously gives $\alpha = \beta = \gamma = \delta = 0$. Hence the Pauli matrices are linearly independent.

4. From the previous part, we know that the four Pauli matrices are linearly independent. The vector space of 2×2 complex-valued matrices is isomorphic to $\mathbb{C}^4$ and hence has dimension 4. Thus the Pauli matrices form a minimal spanning set and are therefore a basis.

Question 4 [2 points]: Entanglement

Prove that the *controlled-Z* gate

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

is entangling. Do so by giving an explicit two-qubit (unentangled) state $|\psi\rangle \otimes |\phi\rangle$ and showing that $CZ(|\psi\rangle \otimes |\phi\rangle)$ is entangled.

Solution. One example is $|\psi\rangle \otimes |\phi\rangle = |+\rangle \otimes |-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$. Applying CZ we get $|\chi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$. We claim that $|\chi\rangle$ is entangled. Suppose it isn't, so that there exist a, b, c, d such that $|\chi\rangle = \frac{1}{2}(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$. Expanding and comparing coefficients, we get

$$\begin{aligned} ac &= 1, \\ ad &= -1, \\ bc &= 1, \\ bd &= 1. \end{aligned}$$

Clearly none of a, b, c, d can be 0. From the first two equations we get $c/d = -1$, but from the second two equations we get $c/d = 1$, which is a contradiction.

Question 5 [2 points]: Partial measurement

Let

$$|\psi\rangle = \frac{i\sqrt{2}}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}\sqrt{2}}|01\rangle + \frac{\sqrt{2}}{2\sqrt{3}}|10\rangle.$$

Calculate the probabilities of measuring 0 or 1 in the first qubit, and the resulting normalized state vector in either case.

Solution. The probability of measuring 0 in the first qubit is $||(\langle 0| \otimes I \otimes I)|\psi\rangle||^2 = ||\frac{i\sqrt{2}}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}\sqrt{2}}|01\rangle||^2 = 5/6$. The resulting normalized state is (up to a global phase) $\frac{\sqrt{4}}{\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle$. The probability of measuring 1 in the first qubit is thus $1/6$, and the resulting normalized state is $|10\rangle$.

Question 6 [9 points]: Non-local games

In this question, we're going to examine another non-local game involving 3-parties, or 3 qubits. First let $|\psi\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$

1. Give a 3-qubit circuit U consisting of X, H, and $CNOT$ gates such that
$$U\left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{\sqrt{2}}|111\rangle\right) = |\psi\rangle.$$
2. Show that a partial measurement of any qubit in the $|\psi\rangle$ state leaves an entangled state in the remaining 2 qubits.
3. Compute the parity $a \oplus b \oplus c = a + b + c \mod 2$ of the measurement results if
   (a) All qubits are measured in the $\{0, 1\}$ basis.
   (b) Qubits 0 and 1 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 2 in the $\{0, 1\}$ basis.
   (c) Qubits 0 and 2 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 1 in the $\{0, 1\}$ basis.
   (d) Qubits 1 and 2 are measured in the $\{|+\rangle, |-\rangle\}$ basis and qubit 0 in the $\{0, 1\}$ basis.

   Note: in the $\{|+\rangle, |-\rangle\}$ basis, we consider the result of measuring "+" to be 0 and the result of measuring "-" to be 1
4. Denote the measurement result of qubit i in the $\{0, 1\}$ basis by a_i, and in the $\{|+\rangle, |-\rangle\}$ basis by b_i. Is it possible that each a_i and b_i has a **pre-determined value** independent of which basis the other qubits are measured in? Give a convincing argument for your answer.
5. Give a quantum strategy (i.e. a strategy where involving a shared pre-entangled state) for a 3-player game where Alice, Bob, and Charlie are each given one bit x, y, and z respectively, and have to return a single bit a, b, c respectively. They win if $a \oplus b \oplus c = x \vee y \vee z$. **Jan 29th update: you should assume that $x \oplus y \oplus z = 0$ and your strategy should win the game with 100% probability.**
   Hint: use the state $|\psi\rangle$ from the first part of this question as the initial shared state

Solution.

1. Working backwards, we have $|\psi\rangle = \frac{1}{2}\big(|0\rangle(|00\rangle - |11\rangle) - |1\rangle(|10\rangle + |01\rangle)\big)$. Applying $CNOT_{12}$ (i.e. control on qubit 1 and target on qubit 2) we get
$$\begin{aligned}\tfrac{1}{2}\big(|0\rangle(|00\rangle - |10\rangle) - |1\rangle(|11\rangle + |01\rangle)\big) &= \tfrac{1}{2}\big(|0\rangle(|0\rangle - |1\rangle)|0\rangle - |1\rangle(|1\rangle + |0\rangle)|1\rangle\big)\\ &= \tfrac{1}{\sqrt{2}}(|0\rangle|-\rangle|0\rangle - |1\rangle|+\rangle|1\rangle),\end{aligned}$$

so we can now reach our initial state by applying H_1 followed by X_1. Thus by reversing this circuit we get that

$$\begin{aligned} U &= (X_1 H_1 CNOT_{12})^\dagger \\ &= CNOT_{12} H_1 X_1 \quad \text{(all these gates are hermitian).} \end{aligned}$$

2. Suppose we measure qubit 0. If we obtain an outcome of 0, the resulting state is $\frac{1}{\sqrt{2}}(|000\rangle - |011\rangle)$. If the outcome is 1, the resulting state is (proportional to) $\frac{1}{\sqrt{2}}(|110\rangle + |101\rangle)$. By inspecting qubits 1 and 2, it's easy to check that both of these states are entangled.

   If instead we measure qubit 1 or 2, we note that $|\psi\rangle$ is symmetric under permuting qubits. We can rewrite the state by swapping the qubit we're measuring with qubit 0 and proceed exactly as before.

3. (a) We can either use part 2 as a starting point, or alternatively we can consider measuring the entire system in the 3-qubit computational basis $\{|000\rangle, |001\rangle, \ldots, |111\rangle\}$. In either case, we find that the possible measurement outcomes are $abc =$ 000, 110, 011 or 101. Each of these outcomes has parity $a \oplus b \oplus c = 0$.

   (b) Note that $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. Thus we have

$$\begin{aligned} |000\rangle &= \tfrac{1}{2}(|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle + |{-}{-}\rangle)|0\rangle, \\ |110\rangle &= \tfrac{1}{2}(|{+}{+}\rangle - |{+}{-}\rangle - |{-}{+}\rangle + |{-}{-}\rangle)|0\rangle, \\ |011\rangle &= \tfrac{1}{2}(|{+}{+}\rangle - |{+}{-}\rangle + |{-}{+}\rangle - |{-}{-}\rangle)|1\rangle, \\ |101\rangle &= \tfrac{1}{2}(|{+}{+}\rangle + |{+}{-}\rangle - |{-}{+}\rangle - |{-}{-}\rangle)|1\rangle, \end{aligned}$$

   so $|\psi\rangle = \frac{1}{2}(-|{+}{+}1\rangle + |{+}{-}0\rangle + |{-}{+}0\rangle + |{-}{-}1\rangle)$.
   Measuring in the joint basis $\{|{+}{+}0\rangle, |{+}{+}1\rangle, \ldots, |{-}{-}1\rangle\}$, we see that the parity of any measurement result is 1.

   For parts (c) and (d), we can simply use the symmetry of $|\psi\rangle$ to immediately deduce that the parity is 1 in each of these cases.

4. We can show that the values of a_i and b_i can't have predetermined values by way of a parity argument. The previous question showed that for the 4 measurement bases in that question, we get the series of constraints on the values of a_i and b_i:

$$\begin{aligned} a_0 \oplus a_1 \oplus a_2 &= 0 \\ b_0 \oplus b_1 \oplus a_2 &= 1 \\ b_0 \oplus a_1 \oplus b_2 &= 1 \\ a_0 \oplus b_1 \oplus b_2 &= 1 \end{aligned}$$

   Now suppose each a_i and b_i is pre-determined and independent of the measurement performed on the other qubits. Then each a_i and b_i has a definite value and in particular must simultaneously satisfy *all* the above constraints. We can show that the above constraint system is inconsistent and hence can't be simultaneously satisfied by summing up both sides mod 2:

	$a_0 \oplus a_1 \oplus a_2$	0
	$b_0 \oplus b_1 \oplus a_2$	1
	$b_0 \oplus a_1 \oplus b_2$	1
	$a_0 \oplus b_1 \oplus b_2$	1
+	$= 0 \mod 2$	$= 1 \mod 2$

5. Part 3 gives us a clue for a potential strategy. Let Alice, Bob and Charlie share the state $|\psi\rangle$ such that Alice can only perform local operations and measurements on qubit 0, Bob on qubit 1, and Charlie on qubit 2. Each player performs a measurement on their qubit as follows: if the bit they are given is 0, they measure in the computational basis; if the bit is 1, they measure in the $\{|+\rangle, |-\rangle\}$ basis. They each return a bit corresponding to their measurement outcome.

   By symmetry, and after imposing the additional constraint that $x \oplus y \oplus z = 0$, we only need to check what happens in two cases: x, y, z are all 0; two of x, y, z are 1. In the case where x, y, z are all 0, part 3(a) tells us that the returned bits satisfy $a \oplus b \oplus c = 0$, which is equal to $x \vee y \vee z$. Similarly, in the case where two of x, y, z are 1, parts 3(b)–(d) tell us that the returned bits satisfy $a \oplus b \oplus c = 1$, which is equal to $x \vee y \vee z$. Hence this strategy succeeds with 100% probability.