SOLUTIONS

EE 520 Midterm Exam, 6 October 2020

Do all parts of all problems. Write your answers on the exam. Note that the point value of each problem is marked. This exam is open book/open notes. You may refer to any source that you like, but you **cannot consult with other people or collaborate on this exam**. If you use scratch paper, you may hand it in with your exam for consideration of partial credit, but it is not required. Your completed exam must be uploaded as a single PDF file through the Blackboard site before **9 am on Wednesday 7 October 2020**. You can take as much time as you want on this exam, so long as it is handed in on time, but it should not require more than about two hours to complete.

Part I

CIRCLE the *best* answer for each of the following questions. There is only one best answer for each question. No partial credit. (3 points each.)

1. The Hadamard matrix H is Hermitian, and therefore is an *observable*. What is its expectation value $\langle H\rangle$ in the qubit state $|1\rangle$?

   (a) $1/\sqrt{2}$ (b) 0 (c) 1 (d) $-1/\sqrt{2}$

2. What is a *Universal Turing Machine*?

   (a) A Turing Machine that can emulate any other Turing Machine.
   (b) A Turing Machine that can compute any function.
   (c) A Turing Machine with an oracle for the halting problem.
   (d) A Turing Machine that calculates any computable function efficiently.

3. What observable represents spin up or down along an axis 45° between the X and Y axes?

   (a) $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (b) $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (c) $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix}$ (d) $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}$

4. Which of the following formulas represents the XOR of two bits a and b, and is in disjunctive normal form?

   (a) $\neg(\neg a \& \neg b)$.
   (b) $(a \vee b)\&(\neg a \vee \neg b)$.
   (c) $(\neg a \& b) \vee (a \& \neg b)$.
   (d) $(a \& b) \vee (\neg a \& \neg b)$.

5. Consider a generalized measurement with $M_0 = (1/\sqrt{2})U_1$ and $M_1 = (1/\sqrt{2})U_2$ as the measurement operators, where U_1 and U_2 are both unitary. What is the Shannon entropy of this measurement?

   (a) 1 bit. (b) 2 bits. (c) 0 bits. (d) It depends on the state of the system.

6. Suppose we have a joint system composed of two subsystems A and B that is *initially* in an entangled state $|\Psi\rangle_{AB}$. Suppose we then measure an observable $O_A \otimes I$ on subsystem A alone. Under what condition is the joint state *after* measurement guaranteed to be a product state, completely unentangled?

   (a) The two subsystems A and B are spatially separated.
   (b) $|\Psi\rangle_{AB}$ is maximally entangled.
   (c) O_A is nondegenerate (i.e., a complete observable).
   (d) None of the above.
   (e) Both (a) and (c).

7. Which of the following quantum gates is NOT its own inverse?

   (a) The Toffoli gate.
   (b) The T (i.e., $\pi/8$) gate.
   (c) The Z gate.
   (d) The Hadamard gate.
   (e) All these gates are their own inverses.

8. Which of the following states is entangled?

   (a) $|01\rangle$.
   (b) $\alpha\,|00\rangle - \beta\,|11\rangle$.
   (c) $\alpha\,|00\rangle + \beta\,|10\rangle$.
   (d) $(|\Phi_+\rangle + |\Phi_-\rangle)/\sqrt{2}$.
   (e) Both (b) and (c) are entangled.

9. If A and B are *equivalent observables*, which of the following must be true?

   (a) $[A, B] = 0$.
   (b) $B = f(A)$ for some invertible function f.
   (c) The eigenvalues of A and B are the same.
   (d) All of the above.
   (e) Both (a) and (b).

10. Which state violates the CHSH inequality $|\langle X_A X_B - X_A Z_B + Z_A X_B + Z_A Z_B\rangle| \leq 2$?

    (a) $|00\rangle$.
    (b) $|\Phi_+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$.
    (c) $(1/\sqrt{3})(|00\rangle + |01\rangle + |11\rangle)$.
    (d) None of the above.

Part II

11. (20 points.) The polarization of a photon, like the spin-1/2, is a natural qubit. A photon can be polarized vertically ($|V\rangle$), horizontally ($|H\rangle$), or at any other angle ϕ ($\cos(\phi)|V\rangle + \sin\phi|H\rangle$). (We are ignoring circular and elliptical polarizations.) A polaroid filter can be oriented at any angle from 0 (vertical, or 0°) to $\pi/2$ (horizontal, or 90°) to π (back to vertical again) and any angle in between. The filter lets through all photons polarized at the same angle as the filter and blocks all photons polarized at right angles to the filter. If a photon is polarized at an angle θ away from the angle of the filter, it will pass through with probability $\cos^2(\theta)$, and be blocked with probability $\sin^2(\theta)$. If the photon passes through the filter, its polarization will be changed afterwards so that its polarization angle is the same as the angle of the filter. (This is equivalent to measuring the polarization of the photon in a basis corresponding to the polaroid filter's angle and then blocking the photon if it is in the orthogonal basis state.)

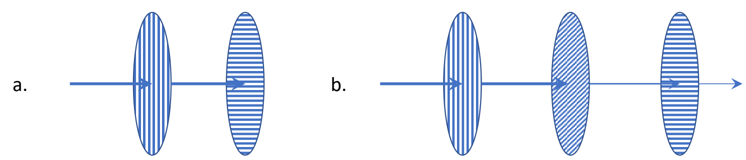


Figure 1: The filter layouts for parts (a) and (b) below.

(a) (5 points.) Suppose a photon polarized at an angle ϕ is incident on a polaroid filter oriented at an angle 0 (vertical) followed by a second filter oriented at an angle $\pi/2$ (horizontal). See Fig. 1a. What is the probability that the photon passes through both filters?

The probability for the photon to pass the first filter is $\cos^2(\phi)$. If it passes, it is polarized vertically. The probability to then pass the second filter is $\cos^2(\pi/2) = 0$. So the probability to pass both filters is 0, regardless of the value of ϕ.

(b) (5 points.) Now suppose that in between those two filters we insert a third filter oriented at an angle $\pi/4$ (45°). See Fig. 1b. What is the probability that the photon passes through all three filters?

The probability to pass the first filter is $\cos^2(\phi)$. The probability to then pass the second filter is $\cos^2(\pi/4) = 1/2$; and the probability to pass the third filter is also $\cos^2(\pi/4) = 1/2$. So the probability to pass all three filters is

$$p_{\text{pass}} = \frac{1}{4}\cos^2(\phi).$$

(c) (5 points.) Now between the vertical and horizontal filters we insert $N-1$ filters, each one rotated by an angle $\pi/(2N)$ from the one before (so the angles from beginning to end are 0, $\pi/(2N)$, $2\pi/(2N)$, $3\pi/(2N), \ldots, \pi/2)$. What is the probability that the photon passes through all $N+1$ filters?

Again, the probability to pass the first filter is $\cos^2(\phi)$. Each subsequent filter is rotated by an angle $\pi/2N$ with respect to the one before. So the probability to pass them all is

$$p_{\text{pass}} = \cos^2(\phi) \times \cos^2(\pi/2N) \times \cdots \times \cos^2(\pi/2N) = \cos^2(\phi)\cos^{2N}(\pi/2N).$$

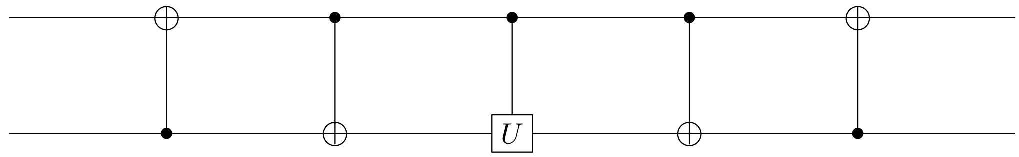
(d) (5 points.) Let the original polarization angle of the photon be $\phi = 0$ (vertical). Show that as N gets larger, the probability from part (c) approaches the function $e^{-\pi^2/(4N)}$.

As $N \to \infty$ we can expand the cosine function and make a chain of approximations:

$$\cos^{2N}(\pi/2N) \approx \left(1 - (\pi/2N)^2/2\right)^{2N} \approx \left(e^{-(\pi/2N)^2/2}\right)^{2N} = e^{-\pi^2/(4N)}.$$

The error scales as $O(1/N^2)$, and hence goes to zero as $N \to \infty$.

12. (15 points.) Write down the states produced by applying the following circuit to each of the compuational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$,



where U is a 2×2 unitary operator $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Let's evolve each basis vector through the five gates in this circuit:

$$|00\rangle \to |00\rangle \to |00\rangle \to |00\rangle \to |00\rangle \to |00\rangle .$$

$$|01\rangle \to |11\rangle \to |10\rangle \to a\,|10\rangle + c\,|11\rangle \to a\,|11\rangle + c\,|10\rangle \to a\,|01\rangle + c\,|10\rangle .$$

$$|10\rangle \to |10\rangle \to |11\rangle \to b\,|10\rangle + d\,|11\rangle \to b\,|11\rangle + d\,|10\rangle \to b\,|01\rangle + d\,|10\rangle .$$

$$|11\rangle \to |01\rangle \to |01\rangle \to |01\rangle \to |01\rangle \to |11\rangle .$$

This is an example of a "two-level unitary." If we write it in matrix form, it is

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

13. (10 points.) The *no-cloning theorem* is only one of a large class of impossibility results in quantum mechanics. Another is the nonexistence of a *universal NOT gate*. A universal NOT gate would be a unitary matrix N such that for every state $|\psi\rangle$, $N|\psi\rangle = |\bar{\psi}\rangle$, where $|\bar{\psi}\rangle$ is a state orthogonal to $|\psi\rangle$: $\langle\psi|\bar{\psi}\rangle = 0$. Prove that no such unitary N exists.

    There are a number of ways of proving this. One fairly quick way: notice that if $N|\psi\rangle = |\bar{\psi}\rangle$ where $\langle\psi|\bar{\psi}\rangle = 0$, then in every state we have

    $$\langle N\rangle = \langle\psi| N |\psi\rangle = \langle\psi|\bar{\psi}\rangle = 0.$$

    If $\langle N\rangle = 0$ in every state, then N must be the zero operator, and hence not a unitary.

    Another easy proof: if N is unitary, then it has eigenvectors $|\phi\rangle$ with eigenvalues $e^{i\theta}$. Clearly in this case, $N|\phi\rangle = e^{i\theta}|\phi\rangle$, which is manifestly not orthogonal to $|\phi\rangle$. So no such operator can exist.

14. (15 points total.) Suppose that our quantum computing scheme relies on a *probabilistic gate*, which performs a desired unitary $R_Z(\theta)$ for a particular angle θ with probability 5/8 and applies the Pauli matrix Z with probability 3/8. We can describe this by a generalized measurement with measurement operators

    $$M_0 = \sqrt{5/8}R_Z(\theta), \quad M_1 = \sqrt{3/8}Z.$$

    (On the homework you will show that such a gate can arise in practice.) We can improve the success probability by undoing the Z gate and repeating the procedure if it fails. Suppose we repeat the procedure up to three times. Then we have the following new generalized measurement:

    $$N_0 = M_0, \quad N_1 = M_0ZM_1, \quad N_2 = M_0ZM_1ZM_1, \quad N_3 = M_1ZM_1ZM_1.$$

    Outcome j (corresponding to measurement operator N_j) represents the case where the procedure failed j times.

    (a) (5 points.) Verify that $\{N_0, N_1, N_2, N_3\}$ forms a valid measurement.

    We just need the POVM elements to add up to the identity. Note that $ZM_1 = M_1^\dagger Z = \sqrt{3/8}I$, $M_0^\dagger M_0 = (5/8)I$, and $M_1^\dagger M_1 = (3/8)I$.

    $$\begin{aligned}\sum_{i=0}^{3} N_i^\dagger N_i &= M_0^\dagger M_0 + M_1^\dagger Z M_0^\dagger M_0 Z M_1 + M_1^\dagger Z M_1^\dagger Z M_0^\dagger M_0 Z M_1 Z M_1 \\ &\quad + M_1^\dagger Z M_1^\dagger Z M_1^\dagger M_1 Z M_1 Z M_1 \\ &= \left((5/8) + (5/8)(3/8) + (5/8)(3/8)^2 + (3/8)^3\right) I = I.\end{aligned}$$

(b) (5 points.) Show that for outcomes 0, 1, and 2, this repeated procedure succeeds in applying the gate $R_Z(\theta)$.

We can just check this in each case:

$$\begin{aligned}
N_0 |\psi\rangle &= M_0 |\psi\rangle = \sqrt{5/8} R_Z(\theta) |\psi\rangle \,. \\
N_1 |\psi\rangle &= M_0 Z M_1 |\psi\rangle = \sqrt{5/8} R_Z(\theta) \times Z \times \sqrt{3/8} Z |\psi\rangle = \sqrt{(5/8)(3/8)} R_Z(\theta) |\psi\rangle \,. \\
N_2 |\psi\rangle &= M_0 Z M_1 |\psi\rangle = \sqrt{5/8} R_Z(\theta) \times Z \times \sqrt{3/8} Z \times Z \times \sqrt{3/8} Z |\psi\rangle \\
&= \sqrt{(5/8)(3/8)^2} R_Z(\theta) |\psi\rangle \,.
\end{aligned}$$

In all three cases, $|\psi\rangle \to R_Z(\theta) |\psi\rangle$ after renormalizing the state.

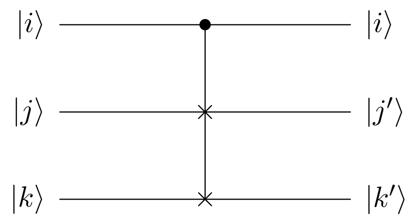
(c) (5 points.) Calculate the probability of failure (outcome 3). (This probability is the same for every state!) Suppose that instead of stopping after 3 repetitions, we repeat the procedure up to k times. What is the probability of failure as a function of k?

The probability of failure is

$$\langle N_3^\dagger N_3 \rangle = \langle M_1^\dagger Z M_1^\dagger Z M_1^\dagger M_1 Z M_1 Z M_1 \rangle = \langle (3/8)^3 I \rangle = (3/8)^3 \approx 0.0527.$$

If we repeat the procedure up to k times, the failure probability will be $(3/8)^k$.

15. (10 points total.) The Fredkin gate is a *controlled-SWAP* gate:

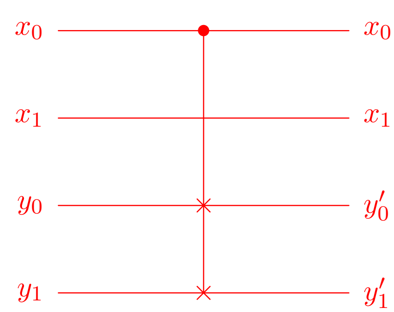


The Fredkin gate takes an input basis vector $|ijk\rangle$ to an output basis vector $|ij'k'\rangle$, where if $i = 0$ then $j' = j$ and $k' = k$, and if $i = 1$ then $j' = k$ and $k' = j$. (This amounts to exchanging $|101\rangle \leftrightarrow |110\rangle$ and leaving all the other basis vectors unchanged.)

Like the Toffoli gate, the Fredkin gate is a classical reversible gate that is *universal*—it can be used to compute any Boolean function. This is not very obvious, because a Fredkin gate keeps the number of 0's and 1's constant, so it seems that it cannot simulate gates that do not (like the CNOT or Toffoli). We can get around this by using an *encoding*: we represent a 0 by *two* bits 01, and we represent a 1 by 10. We will write the encoded bits in boldface: $\mathbf{0} = 01$ and $\mathbf{1} = 10$. (The other combinations 00 and 11 don't mean anything.)

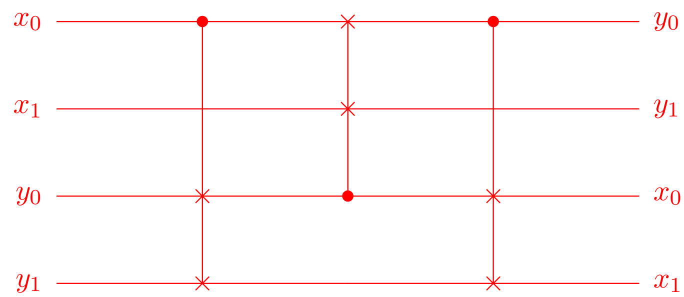
(a) (5 points.) Write a circuit using only Fredkin gates on four input bits for the encoded XOR (or CNOT) gate, that maps $\mathbf{x}, \mathbf{y} \to \mathbf{x}, \mathbf{x} \oplus \mathbf{y}$. That is, $\mathbf{0}, \mathbf{0} \to \mathbf{0}, \mathbf{0}$, $\mathbf{0}, \mathbf{1} \to \mathbf{0}, \mathbf{1}$, $\mathbf{1}, \mathbf{0} \to \mathbf{1}, \mathbf{1}$, and $\mathbf{1}, \mathbf{1} \to \mathbf{1}, \mathbf{0}$. (Hint: only a single Fredkin gate is needed!)

Let's label the four bits x_0, x_1, y_0, y_1, so the codewords are $\mathbf{x} = x_0 x_1$ and $\mathbf{y} = y_0 y_1$. the key to designing this circuit is to realize that a NOT gate in this encoding just corresponds to a SWAP of the two bits; and a CNOT is therefore a controlled SWAP, i.e., a Fredkin gate. The circuit is:



(b) (5 points.) Write a circuit using only Fredkin gates on four input bits that swaps two encoded bits, $\mathbf{x}, \mathbf{y} \rightarrow \mathbf{y}, \mathbf{x}$. (Hint: remember, a swap can be built from three CNOTs.)

Using the result from part (a), we can do a SWAP with three alternating CNOT gates. The circuit is:



If we allow the use of ancillas, there is another straightforward solution: we can use an ancilla in the state 1 as a control, and just use the Fredkin gates as SWAPs: