CPSC 519/619 (Fall 2016)

Final exam questions

A 180 minutes exam held on December 12, 2016

1. Short answers

1. Consider the 3-qubit state

$$|\Psi\rangle = \frac{3}{5}|000\rangle + \frac{\imath}{5}|001\rangle + \frac{2}{5}|010\rangle + \frac{1}{5}|100\rangle + \frac{3}{5}|101\rangle - \frac{1}{5}|111\rangle.$$

   What is the probability that a measurement of the least significant bit of $|\Psi\rangle$ (i.e. the third qubit) yields the outcome 1? Show your calculations.

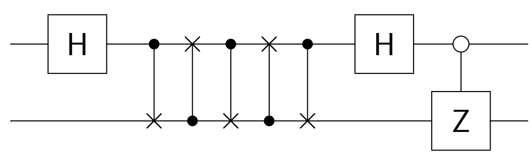
2. Explain why

$$\mathsf{U} = |\circlearrowright\rangle\langle +| + \imath|\circlearrowleft\rangle\langle -|$$

   is unitary. Give an explanation that is as simple as possible. (The circular vectors are defined by $|\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \imath|1\rangle)$ and $|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \imath|1\rangle)$.)

3. Give a circuit that acts on two qubits, takes as input the state $|00\rangle$, and outputs the state $\frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle)$, using only single-qubit gates and controlled-not gates. Explain.

4. Consider the following circuit acting on two qubits. The second gate is a controlled-not gate that maps $|a\rangle|b\rangle$ to $|a\rangle|(a+b) \bmod 2\rangle$. The third gate is an application of the controlled-not gate in the opposite direction. The last gate applies the Z gate to the second qubit conditioned on that the first qubit is $|0\rangle$.



   Simplify the above circuit as much as possible. Show your calculations.

5. Let $N \geq 2$ and $0 \leq i < N$. Consider $\mathcal{C}^N$. Show that $\mathsf{F}_N^2|i\rangle = |(-i) \bmod N\rangle$.

6. Consider the following four product states over $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$,

$$\begin{array}{rcccccc} |{-}01\rangle & = & |-\rangle & \otimes & |0\rangle & \otimes & |1\rangle \\ |1{-}0\rangle & = & |1\rangle & \otimes & |-\rangle & \otimes & |0\rangle \\ |01{-}\rangle & = & |0\rangle & \otimes & |1\rangle & \otimes & |-\rangle \\ |{+}{+}{+}\rangle & = & |+\rangle & \otimes & |+\rangle & \otimes & |+\rangle. \end{array}$$

   They are mutually orthogonal by construction. Show that there does **not** exist a fifth product state $|\Psi\rangle = |a\rangle \otimes |b\rangle \otimes |c\rangle$ that is simultaneously orthogonal to all of the four states above. (Remark: These four states have many interesting properties and are well-studied in quantum information processing.)

2. A four-qubit code

Shor's 9-qubit code encodes a single qubit into 9 qubits and is based on the classical repetition code $b \mapsto bbb$. It can *detect* and *correct* an arbitrary single qubit error. We now consider the following code $\mathcal{C}$ that encodes *two* qubits into just *four* qubits.

$$
\begin{aligned}
|0\rangle_L &= \frac{1}{\sqrt{2}}\Big(|0001\rangle + |1110\rangle\Big)\\
|1\rangle_L &= \frac{1}{\sqrt{2}}\Big(|0010\rangle + |1101\rangle\Big)\\
|2\rangle_L &= \frac{1}{\sqrt{2}}\Big(|0100\rangle + |1011\rangle\Big)\\
|3\rangle_L &= \frac{1}{\sqrt{2}}\Big(|1000\rangle + |0111\rangle\Big).
\end{aligned}
$$

Let S denote the four-dimensional subspace spanned by $|0\rangle_L$, $|1\rangle_L$, $|2\rangle_L$, and $|3\rangle_L$, and let $S^\perp$ denote the 12-dimensional complementary subspace (that is, $S^\perp$ is the subspace of states that are orthogonal to every vector in S).

1. Show that $\mathsf{I} \otimes \mathsf{I} \otimes \mathsf{I} \otimes \mathsf{X}|\Psi\rangle \in S^\perp$, for any state $|\Psi\rangle \in S$ in the code space S.
2. Show that $\mathsf{I} \otimes \mathsf{I} \otimes \mathsf{I} \otimes \mathsf{Z}|\Psi\rangle \in S^\perp$, for any state $|\Psi\rangle \in S$ in the code space S.
3. Show that $\mathsf{I} \otimes \mathsf{I} \otimes \mathsf{I} \otimes \mathsf{Y}|\Psi\rangle \in S^\perp$, for any state $|\Psi\rangle \in S$ in the code space S.

The above implies that the code $\mathcal{C}$ can *detect* an arbitrary single-qubit error (you are *not* asked to show this).

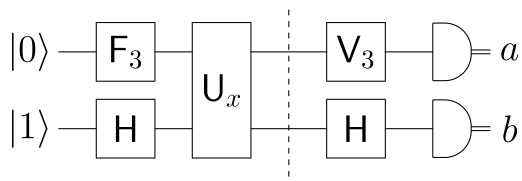
3. Not-All-Equal

Consider the boolean function $\mathsf{NAE} : \{0,1\}^3 \rightarrow \{0,1\}$ on three bits defined by

$$\mathsf{NAE}(x_0, x_1, x_2) = \begin{cases} 1 & \text{if } 1 \leq x_0 + x_1 + x_2 \leq 2 \\ 0 & \text{if } x_0 = x_1 = x_2. \end{cases}$$

The function takes the value 0 if and only if all three bits are equal.

We consider the following quantum circuit over $\mathcal{C}^3 \otimes \mathcal{C}^2$ for computing the function NAE.



The circuit takes as input $|0\rangle \otimes |1\rangle$. Here U_x is defined by $\mathsf{U}_x|i\rangle|b\rangle = |i\rangle|(b + x_i) \bmod 2\rangle$, for $0 \leq i \leq 2$. The operator F_3 is the Fourier transform over $\{0,1,2\}$. The final measurement produces an outcome (a, b) where $a \in \{0,1,2\}$ and $b \in \{0,1\}$. We want to output a bit. So given the measurement outcome (a, b), we output a bit $z = g(a, b)$. The algorithm succeeds if $z = \mathsf{NAE}(x_0, x_1, x_2)$.

1. Give the unique multilinear polynomial representing NAE.
2. Compute a simple expression for the superposition $|\Psi\rangle$ at the dashed line in the circuit.
3. Give a unitary operator V_3 and a boolean function $g : \{0,1,2\} \times \{0,1\} \rightarrow \{0,1\}$ such that the output $g(a, b)$ equals $\mathsf{NAE}(x_0, x_1, x_2)$ with probability as high as possible. Explain and analyze your algorithm. What is the success probability of your algorithm?

4. *W*-states

Consider the following scenario of five parties, spatially separated. Initially, Alice, Bob and Charlie share the 3-qubit state

$$|W_3\rangle = \frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big),$$

and Charlie, David, and Eve also share a $|W_3\rangle$ state. Thus, Alice, Bob, David, and Eve each hold one qubit, while Charlie holds two qubits. We illustrate the shared states as follows.

They can communicate an arbitrary amount of classical bits, but no quantum bits (qubits). Their goal is for Alice, Bob, David, and Eve to share the state

$$|W_4\rangle = \frac{1}{\sqrt{4}}\big(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\big).$$

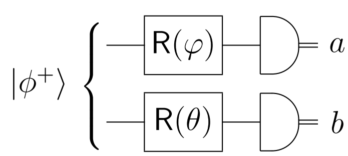
It is impossible for the five parties to create $|W_4\rangle$ with certainty.

1. Give a protocol that creates $|W_4\rangle$ with success probability (at least) 4/9. Analyze your protocol and argue that your protocol works as claimed.

2. What is the resulting state $|\Psi\rangle$ of your protocol when it fails in producing $|W_4\rangle$? Analyze $|\Psi\rangle$ and argue what $|\Psi\rangle$ may be used for.

5. EPR-pairs (619 only)

For any angle $-\pi < \vartheta \leq \pi$, let $\mathsf{R}(\vartheta) = \begin{pmatrix} \cos(\vartheta) & -\sin(\vartheta) \\ \sin(\vartheta) & \cos(\vartheta) \end{pmatrix}$ denote a rotation by angle ϑ. Let $-\pi < \varphi, \theta \leq \pi$ be given angles, and let $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ denote an EPR-pair. The following circuit produces two classical bits $a, b \in \{0, 1\}$ as output.



1. Show that the probability that $a \oplus b = 0$ equals $\cos^2(\theta - \varphi)$. (Here $\oplus$ denotes addition modulo 2.)

2. Given two bits $x, y \in \{0, 1\}$, set

$$\varphi = \begin{cases} 0 & \text{if } x = 0 \\ \frac{\pi}{4} & \text{if } x = 1 \end{cases} \qquad \text{and} \qquad \theta = \begin{cases} \frac{\pi}{8} & \text{if } y = 0 \\ -\frac{\pi}{8} & \text{if } y = 1. \end{cases}$$

   Show that, for all $x, y \in \{0, 1\}$, the probability that $a \oplus b = xy$ is exactly $\cos^2(\pi/8)$. (Note that $xy = 1$ if and only if both x and y are 1.)