QIC 710 / CO 681 / AMATH 871 / CS 768 / PHYS 767 Fall 2018

Homework 4 Solutions

1. **Grover search (10%)**

Given a function $f\colon \{0,1\}^n \to \{0,1\}$, let $A = |f^{-1}(1)|$ be the set of satisfying assignments, and let $B = |f^{-1}(0)|$ be the set of non-satisfying assignments. As in class, let $a = |A|$ be the number of satisfying assignment, let $b = |B|$ and let $N = a + b = 2^n$. Define the states

$$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, \quad \text{and} \quad |B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$$

and recall that Grover's algorithm works by starting with the state,

$$|\theta\rangle := H|0\cdots 0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

then applying an alternating sequence of the reflections U_f and $-HU_0H$, each of which acts on the span of $|A\rangle$ and $|B\rangle$ as

$$U_f = 2|B\rangle\langle B| - I_2, \;\; -HU_0H = 2|\theta\rangle\langle\theta| - I_2,$$

where $I_2 = |A\rangle\langle A| + |B\rangle\langle B|$. Note that we are *not* assuming there is only $n = 1$ qubit. Rather, Grover's algorithm only focuses on this two dimensional subspace spanned by $|A\rangle$ and $|B\rangle$. In class, we saw geometrically how the product of these two reflections is a rotation by 2θ.

Show via explicit calculation that

$$-HU_0HU_f = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}.$$

Solution. We are writing the states in the $|A\rangle$,$|B\rangle$ basis, where $|A\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|B\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $|\theta\rangle = \begin{pmatrix} \sin(\theta) \\ \cos(\theta) \end{pmatrix}$. We first compute

$$\begin{aligned} U_f &= 2|B\rangle\langle B| - I_2 = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ -HU_0H &= 2|\theta\rangle\langle\theta| - I_2 = \begin{pmatrix} 2\sin^2(\theta) - 1 & 2\cos(\theta)\sin(\theta) \\ 2\cos(\theta)\sin(\theta) & 2\cos^2(\theta) - 1 \end{pmatrix} = \begin{pmatrix} -\cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}. \end{aligned}$$

Therefore,

$$-HU_0HU_f = \begin{pmatrix} -\cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ -\sin(2\theta) & \cos(2\theta) \end{pmatrix}.$$

2. **Qubit Clifford group (40%)**

For each integer $k \geq 1$, the k-qubit Pauli group $\mathcal{P}_k \subset \mathrm{U}(2^k)$ is the group of unitary matrices generated by the Pauli matrices acting on each of k qubits. Each element of $\mathcal{P}_k$ has the form $i^a P_1 \otimes P_2 \cdots \otimes P_k$, where $a \in \{0,1,2,3\}$ and each $P_i \in \{I, X, Y, Z\}$, with

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli group $\mathcal{P}_k$ plays a central role in the theory of quantum error correction. The k-qubit Clifford group $\mathcal{C}_k$ is defined to be the group of all k-qubit unitaries U for which $U\mathcal{P}_k U^{-1} = \mathcal{P}_k$. Mathematically speaking, $\mathcal{C}_k$ is the normalizer of $\mathcal{P}_k$. The Clifford group $\mathcal{C}_k$ is important because there exist error correcting codes (e.g. k qubits encoded into $7k$ qubits via many instances of the 7-qubit Steane code) for which unitaries from $\mathcal{C}_k$ can be performed reliably without needing to decode.

Note: To prove that $U \in \mathcal{C}_k$, it is enough to show that $U(I_2^{\otimes i-1} \otimes P \otimes I_2^{k-i})U^\dagger \in \mathcal{P}_k$ for every $P \in \{X, Z\}$ and every $1 \leq i \leq k$, as these single-qubit Paulis generate $\mathcal{P}_k$ up to phases. To prove that a given unitary U is not in $\mathcal{C}_k$, it suffices to show that $U(I_2^{\otimes(i-1)} \otimes P \otimes I_2^{\otimes(k-i)})U^\dagger \notin \mathcal{P}_k$ for some i and some $P \in \{X, Z\}$.

(a) Show that the Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is in $\mathcal{C}_1$.

Solution: $HXH^\dagger = Z$ and $HZH^\dagger = X$, so H is in the 1-qubit Clifford group.

(b) Show that the T-gate $T = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_8 \end{pmatrix}$, where $\zeta_8 = e^{2\pi i/8}$, is not in $\mathcal{C}_1$.

Solution: $TXT^\dagger = \begin{pmatrix} 0 & -\zeta_8^{-1} \\ \zeta_8 & 0 \end{pmatrix} = \zeta_8 \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}$. This matrix is not proportional to any Pauli matrix (obviously not Z, and it can't be proportional to X or Y since only one of the two matrix elements fits each of those), so T is not in the 1-qubit Clifford group.

(c) Show that the phase gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ is in $\mathcal{C}_1$.

Solution: $SXS^\dagger = Y$ and $SZS^\dagger = Z$, so S is in the 1-qubit Clifrord group.

(d) Show that the controlled-not gate is in $\mathcal{C}_2$.

Solution: $\mathrm{CNOT}(X \otimes I)\mathrm{CNOT}^\dagger = X \otimes X$, $\mathrm{CNOT}(I \otimes X)\mathrm{CNOT}^\dagger = I \otimes X$, $\mathrm{CNOT}(Z \otimes I)\mathrm{CNOT}^\dagger = Z \otimes I$, $\mathrm{CNOT}(I \otimes Z)\mathrm{CNOT}^\dagger = Z \otimes Z$, so CNOT is in the 2-qubit Clifford group.

(e) Is the Toffoli gate in $\mathcal{C}_3$?

Solution: No. $\text{Toffoli}(X \otimes I \otimes I)\text{Toffoli}^\dagger = X \otimes \text{CNOT}$, but CNOT is not proportional to a tensor product of Paulis (for this, it would have to be of the form $\begin{pmatrix} P & 0 \\ 0 & \pm P \end{pmatrix}$ or $\begin{pmatrix} 0 & \pm P \\ P & 0 \end{pmatrix}$, where P is proportional to a single-qubit Pauli). Hence, the Toffoli gate is not in the 3-qubit Clifford group. Note that (suppressing the tensor product) Toffoli also takes IXI and IIZ to non-Pauli gates, so any one of these could also have been usd to show it is not Clifford, whereas Toffoli commutes with ZII, IZI and IIX, so these cannot be used to show it is not Clifford.

(f) Is the 2-qubit quantum Fourier transform F_4 in $\mathcal{C}_2$?

Solution. No. Although $F_4(X \otimes I)F_4^{-1} = (I \otimes Z)$ and $F_4(I \otimes X)F_4^{-1} = (X \otimes I)$, this gate is not in the Clifford group because neither of the following can be expressed as a tensor product of Paulis:

$$F_4(I \otimes X)F_4^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & -1 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}, \quad F_4(Z \otimes I)F_4^{-1} = \frac{1-i}{2}\begin{pmatrix} 0 & 1 & 0 & i \\ i & 0 & 1 & 0 \\ 0 & i & 0 & 1 \\ 1 & 0 & i & 0 \end{pmatrix}.$$

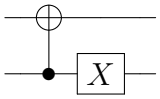
Note that you only needed to find one of these to show F_4 is not Clifford.

(g) Let U_{2^k} be the unitary that adds 1 mod 2^k, acting in the computational basis as $U_{2^k}|x\rangle = |x + 1 \bmod 2^k\rangle$ with respect to the usual binary encoding (e.g. $|0\rangle = |0 \cdots 0\rangle$ and $|2^k - 1\rangle = |1 \cdots 1\rangle$. For example, $U_2 = X$ is the usual Pauli-X, and

$$U_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Is U_4 in $\mathcal{C}_2$?

Solution. Note that

$U_4 =$ 

Since X and CNOT are in $\mathcal{C}_2$, then U_4 is also in $\mathcal{C}_2$ since $\mathcal{C}_2$ is a group.

(h) Is U_8 in $\mathcal{C}_3$?

Solution. No. While direct calculation shows that

$$U_8(X\otimes I\otimes I)U_8^{-1} = X\otimes I\otimes I, U_8(I\otimes Z\otimes I)U_8^{-1} = -I\otimes Z\otimes Z, U_8(I\otimes I\otimes Z)U_8^{-1} = -I\otimes I\otimes Z,$$

U_8 is not Clifford because it takes the remaining Pauli generators to the following matrices, none of which are Pauli by inspection (tensor products of Paulis have a recognizable block structure):

$$U_4(I\otimes X\otimes I)U_4^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$U_4(I\otimes I\otimes X)U_4^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$U_4(Z\otimes I\otimes I)U_4^{-1} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

3. **Coherent information and the complementary channel (50%).** A quantum channel in Kraus form $\mathcal{N}(\rho) = \sum_{j=1}^{e} N_j \rho N_j^\dagger$ can be represented in Stinespring form as $\mathcal{N}(\rho) = \operatorname{Tr}_1 U\rho U^\dagger$, where U is the isometry

$$U = \begin{pmatrix} N_1 \\ \vdots \\ N_e \end{pmatrix}.$$

If we instead do a partial trace over the output system, we get another quantum operation $\mathcal{E}(\rho) = \operatorname{Tr}_2 U\rho U^\dagger$, called a *complementary channel* or *conjugate channel* to the channel $\mathcal{N}$. It models the process that leaks information to the environment about the input. Note that a different Kraus representation of $\mathcal{N}$ gives a different complementary channel $\mathcal{E}$. Because different Stinespring representations are related by isometries between the environments, and because eigenvalues of density matrices are unchanged under isometries, the *coherent information* $I_c(\rho, \mathcal{N}) = S(\mathcal{N}(\rho)) - S(\mathcal{E}(\rho))$ ($S(\rho) = -\operatorname{Tr}\rho\log_2\rho$) is well-defined as a function of ρ and $\mathcal{N}$ for any choice of complementary channel $\mathcal{E}$. Coherent information is important because if $I_c(\rho, \mathcal{N}) > 0$ for some ρ, it can be proved that for any $0 < R < I_c(\rho, \mathcal{N})$, there exists a sequence of codes simulating nR perfect qubit channels using the noisy channels $\mathcal{N}^{\otimes n}$, with vanishing error as $n \to \infty$. Note that better bounds are possible for some channels. Computing the best bound for a general channel is an important open question.

(a) Let $\mathcal{N}_p : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}$ be the qubit p-depolarizing channel $\mathcal{N}_p(\rho) = (1-p)\rho + pI/2$. Show that $\mathcal{N}_p$ has the following Kraus representation

$$\mathcal{N}_p(\rho) = \sum_{e=0}^{3} N_e \rho N_e^\dagger, \quad N_0 = \sqrt{1-q}I, \quad N_1 = \sqrt{\tfrac{q}{3}}X, \quad N_2 = \sqrt{\tfrac{q}{3}}Y, \quad N_3 = \sqrt{\tfrac{q}{3}}Z,$$

where $q = \frac{3p}{4}$.

Solution. Because $I/2 = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z)$, we can write the channel as

$$\mathcal{A}_p(\rho) = (1-q)\rho + q/3 X\rho X + q/3 Y\rho Y + q/3 Z\rho Z,$$

where $q = \frac{3p}{4}$. Therefore we can express the channel with four Kraus operators $\sqrt{1-q}I, \sqrt{q/3}X, \sqrt{q/3}Y, \sqrt{q/3}Z$.

(b) Give an expression for a complementary channel $\mathcal{E}_p : \mathbb{C}^{2\times 2} \to \mathbb{C}^{4\times 4}$ in Kraus form. It is possible to do this with two 4×2 Kraus operators, as the channel $\mathcal{N}_p$ can be realized with four Kraus operators.

Solution. From the Krauf form derived above, we can write a Stinespring extension $U\colon \mathbb{C}^2 \to \mathbb{C}^4 \otimes \mathbb{C}^2$ as

$$U = \begin{pmatrix} \sqrt{1-q}I \\ \sqrt{q/3}X \\ \sqrt{q/3}Y \\ \sqrt{q/3}Z \end{pmatrix} = \begin{pmatrix} \sqrt{1-q} & 0 \\ 0 & \sqrt{1-q} \\ 0 & \sqrt{q/3} \\ \sqrt{q/3} & 0 \\ 0 & -\sqrt{q/3}i \\ \sqrt{q/3}i & 0 \\ \sqrt{q/3} & 0 \\ 0 & -\sqrt{q/3} \end{pmatrix}.$$

Swapping the tensor product to $\mathbb{C}^2 \otimes \mathbb{C}^4$ lets us write the isometry as

$$U = \begin{pmatrix} \sqrt{1-q} & 0 \\ 0 & \sqrt{q/3} \\ 0 & -\sqrt{q/3}i \\ \sqrt{q/3} & 0 \\ 0 & \sqrt{1-q} \\ \sqrt{q/3} & 0 \\ \sqrt{q/3}i & 0 \\ 0 & -\sqrt{q/3} \end{pmatrix} = \begin{pmatrix} E_1 \\ E_2 \end{pmatrix},$$

where

$$E_1 = \begin{pmatrix} \sqrt{1-q} & 0 \\ 0 & \sqrt{q/3} \\ 0 & -\sqrt{q/3}i \\ \sqrt{q/3} & 0 \end{pmatrix} \text{ and } E_2 = \begin{pmatrix} 0 & \sqrt{1-q} \\ \sqrt{q/3} & 0 \\ \sqrt{q/3}i & 0 \\ 0 & -\sqrt{q/3} \end{pmatrix}.$$

(c) Compute the the density matrices induced on the output $\mathcal{N}_p(I/2)$ and environment $\mathcal{E}_p(I/2)$ when the depolarizing channel acts on a maximally mixed state.

Solution. Direct calculation gives $\mathcal{N}_p(I/2) = I/2$ for all p and

$$\mathcal{E}_p(I/2) = \frac{1}{2}E_1E_1^\dagger + \frac{1}{2}E_2E_2^\dagger = \begin{pmatrix} 1-q & 0 & 0 & 0 \\ 0 & q/3 & 0 & 0 \\ 0 & 0 & q/3 & 0 \\ 0 & 0 & 0 & q/3 \end{pmatrix} = \begin{pmatrix} 1-3p/4 & 0 & 0 & 0 \\ 0 & p/4 & 0 & 0 \\ 0 & 0 & p/4 & 0 \\ 0 & 0 & 0 & p/4 \end{pmatrix}.$$

(d) Give expressions for the entropy of the output $S(\mathcal{N}_p(I/2))$ and $S(\mathcal{E}_p(I/2))$ induced in the environment when the input is maximally mixed.

Solution. $S(\mathcal{N}_p(I/2)) = S(I/2) = 1$ and

$$\begin{aligned} S(\mathcal{E}_p(I/2)) &= S(1-q, q/3, q/3, q/3) = -(1-q)\log_2(1-q) - q\log_2(q/3) \\ &= H(q) + q\log_2 3 = H(3p/4) + \frac{3p}{4}\log_2(3), \end{aligned}$$

where $H(q) = -(1-q)\log(1-q) - q\log q$ and $H(p_1, \ldots, p_n) = -\sum_i p_i \log_2 p_i$.

(e) Numerically compute the value of p at which $I_c(I/2, \mathcal{N}_p) = 0$.

Solution. We have $I_c(I/2, \mathcal{N}_p) = 1 - H(3p/4) - \frac{3p}{4}\log_2(3)$. Numerically, we can extract the value of p such that $I_c(I/2, \mathcal{N}_p) = 0$ to be $p = .252386\cdots$.

(By the above remarks, this means that good codes exist agains depolarizing noise up to that value. Good codes exist that surpass this bound, and it is an active research problem to determine the ultimate bound – as far as we currently know, good codes might ultimately exist for all $p < 1/3$.)