QIC 710 / CO 681 / AMATH 871 / CS 768 / PHYS 767 Fall 2017

Homework 4

Due date: Thursday, November 29

Completed homeworks will be submitted online in Crowdmark. You will receive an email with instructions closer to the due date. A requirement for this is that each of your solutions *must begin on a new page.* Typesetting solutions in LaTeX is recommended but not required. If you do write your solutions by hand, please ensure that your scans are legible before you upload them.

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

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

   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

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

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 $\mathcal{C}_1$.

(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 $\mathcal{C}_1$.

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

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

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

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

(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. $|0\rangle = |0\cdots0\rangle$ and $|2^k - 1\rangle = |1\cdots1\rangle$. 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 $\mathcal{C}_2$?

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

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

(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.

(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.

(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.

(e) Numerically compute the value of p at which $I_c(I/2, \mathcal{N}_p) = 0$.
(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 $p < 1/3$.)