CSE 599d Quantum Computing Problem Set 3 Solutions

Author: Dave Bacon (*Department of Computer Science & Engineering, University of Washington*)
Due: February 17, 2006

For this problem set recall that the Pauli X, Y, and Z are

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1}$$

Exercise 1: Tsirel'son's Inequality

Suppose that A, A', B, B' are operators on some Hilbert space $\mathcal{H}$ which satisfy $A^2 = A'^2 = B^2 = B'^2 = I$ and $[A, B] = [A, B'] = [A', B] = [A', B'] = 0$ (where the commutator is $[M, N] = MN - NM$.)
(a) Define $C = AB + AB' + A'B - A'B'$. Show that $C^2 = 4I - [A, A'][B, B']$.

Write $C = A(B + B') + A'(B - B')$. Then

$$C^2 = [A(B + B') + A'(B - B')]\,[A(B + B') + A'(B - B')] \tag{2}$$

The A, A' and B, B' variables commute, so we can move them freely through each other and obtain

$$C^2 = A^2(B + B')^2 + (A')^2(B - B')^2 + AA'(B + B')(B - B') + A'A(B - B')(B + B') \tag{3}$$

Now use the fact that $A^2 = (A')^2 = I$ we obtain

$$C^2 = (B + B')^2 + (B - B')^2 + AA'(B + B')(B - B') + A'A(B - B')(B + B') \tag{4}$$

Using $B^2 = (B')^2 = I$, this becomes

$$C^2 = 4I + AA'(B + B')(B - B') + A'A(B - B')(B + B') \tag{5}$$

Using this again we obtain

$$\begin{aligned} C^2 &= 4I + AA'(B'B - BB') + A'A(BB' - B'B) \\ &= 4I - AA'[B, B'] + A'[B, B'] \\ &= 4I - [A, A'][B, B'] \end{aligned} \tag{6}$$

as desired.

(b) The *sup norm* of an operator M is defined as

$$||M||_{\sup} = \sup_{|\psi\rangle \neq 0} \frac{||M|\psi\rangle||}{|||\psi\rangle||} \tag{7}$$

where $||\cdot||$ is the standard norm on our Hilbert space. Prove that

$$||M + N||_{\sup} \leq ||M||_{\sup} + ||N||_{\sup} \tag{8}$$

and

$$||MN||_{sup} \leq ||M||_{\sup}||N||_{\sup} \tag{9}$$

To show the first inequality, note that

$$||M + N||_{\sup} = \sup_{|\psi\rangle \neq 0} \frac{||(M + N)|\psi\rangle||}{|||\psi\rangle||} \tag{10}$$

The triangle inequality says that $||M|\psi\rangle + N|\psi\rangle|| \leq ||M|\psi\rangle|| + ||N|\psi\rangle||$, so

$$||M + N||_{\sup} \leq \sup_{|\psi\rangle \neq 0} \frac{||M|\psi\rangle||}{|||\psi\rangle||} + \frac{||N|\psi\rangle||}{|||\psi\rangle||} \tag{11}$$

But the maximum over the sum of two dependent terms is less than the maximum over the sum of these two terms when they are independent:

$$||M+N||_{\text{sup}} \leq \sup_{|\psi\rangle\neq 0} \frac{||M|\psi\rangle||}{|||\psi\rangle||} + \sup_{|\phi\rangle\neq 0} \frac{||N|\phi\rangle||}{|||\phi\rangle||} \tag{12}$$

Thus proving that $||M+N||_{\text{sup}} \leq ||M||_{\text{sup}} + ||N||_{\text{sup}}$.
We will prove $||MN||_{\text{sup}} \leq ||M||_{\text{sup}}||N||_{\text{sup}}$ by contradiction. Assume that

$$||MN||_{\text{sup}} > ||M||_{\text{sup}}||N||_{\text{sup}} \tag{13}$$

Let $|\psi\rangle$ be a state which maximizes $\frac{||MN|\psi\rangle||}{|||\psi\rangle||}$ and define $|\phi\rangle = N|\psi\rangle$. Then by our assumption,

$$||MN||_{\text{sup}} > \sup_{|\psi_1\rangle\neq 0} \frac{||M|\psi_1\rangle||}{|||\psi_1\rangle||} \sup_{|\psi_2\rangle\neq 0} \frac{||N|\psi_2\rangle||}{|||\psi_2\rangle||} \tag{14}$$

which by the definition of supremum is

$$||MN||_{\text{sup}} > \frac{||M|\phi\rangle||}{|||\phi\rangle||} \frac{||N|\psi\rangle||}{|||\psi\rangle||} = \frac{||M|\phi\rangle||}{||\psi\rangle||} = \frac{||MN|\psi\rangle||}{|\psi\rangle} \tag{15}$$

which is a contradiction.

(c) Use these properties of the sup norm to show that

$$||C||_{\text{sup}} \leq 2\sqrt{2} \tag{16}$$

From part (a), $C^2 = 4I - [A, A'][B, B']$. Thus

$$||C^2||_{\text{sup}} = ||4I - [A, A'][B, B']||_{\text{sup}} \tag{17}$$

Using part (b), this can be expressed as

$$||C^2||_{\text{sup}} \leq ||4I||_{\text{sup}} + ||[A, A'][B, B']||_{\text{sup}} \leq 4 + ||[A', A]||_{\text{sup}}||[B, B']||_{\text{sup}} \tag{18}$$

Also, using part (b), $||[M, N]||_{\text{sup}} \leq ||MN||_{\text{sup}} + || - NM||_{\text{sup}} \leq ||M||_{\text{sup}}||N||_{\text{sup}} + ||N||_{\text{sup}}||M||_{\text{sup}} = 2||M||_{\text{sup}}||N||_{\text{sup}}$, so

$$||C^2||_{\text{sup}} \leq 4 + 4||A'||_{\text{sup}}||A||_{\text{sup}}||B'||_{\text{sup}}||B||_{\text{sup}} \tag{19}$$

But since $A^2 = (A')^2 = B^2 = (B')^2 = I$, this implies that

$$||C^2||_{\text{sup}} \leq 8 \tag{20}$$

Using $||C^2||_{\text{sup}} = ||C||^2_{\text{sup}}$ this becomes $||C||_{\text{sup}} \leq 2\sqrt{2}$.

This is Tsirel'son's (or Cirel'son's) inequality. Suppose we are working on a Hilbert space of two qubits. If we take $A = A_1 \otimes I$, $A' = A_2 \otimes I$, $B = I \otimes B_1$, and $B' = I \otimes B_2$, then this expression is

$$||A_1 \otimes B_1 + A_1 \otimes B_1 + A_2 \otimes B_1 - A_2 \otimes B_2||_{\text{sup}} \leq 2\sqrt{2} \tag{21}$$

Recall that from class we saw that for local hidden variable theories satisfy the CHSH inequality: $|\langle C\rangle| \leq 2$. So Tsirel'son's inequality bounds the "amount" of violation that quantum states can have over the CHSH inequality. In fact quantum theory can saturate this bound.

Exercise 2: A Quantum Error Detecting Code

In this problem we will examine a quantum error detecting code on four qubits.

(a) Show that the three four-qubit Pauli group operators $S_1 = X \otimes X \otimes I \otimes I$, $S_2 = I \otimes I \otimes X \otimes X$, $S_3 = Z \otimes Z \otimes Z \otimes Z$ all commute with each other (two operators commute if $AB = BA$.)

S_1 and S_2 commute because they act on different qubits. S_1 and S_3 commute since $S_1 S_3 = (XZ) \otimes (XZ) \otimes Z \otimes Z = (-ZX) \otimes (-ZX) \otimes Z \otimes Z = (ZX) \otimes (ZX) \otimes Z \otimes Z = S_3 S_1$. Similarly S_2 and S_3 commute since $S_2 S_3 = Z \otimes Z \otimes (XZ) \otimes (XZ) = Z \otimes Z \otimes (-ZX) \otimes (-ZX) = Z \otimes Z \otimes (ZX) \otimes (ZX) = S_3 S_2$.

(b) The subspace defined by the simultaneous equations $S_i|\psi\rangle = |\psi\rangle$ is two dimensional. Construct an operator made up of a sum of products of S_i operators which projects onto this subspace. Such an operator should satisfy $P|\psi\rangle = |\psi\rangle$ for $|\psi\rangle$ in the subspace and $P|\psi\rangle = 0$ for all $|\psi\rangle$ orthogonal to states in the subspace.

Since $S_i^2 = I$, S_i each have eigenvalues either $+1$ or -1. To project onto the $+1$ eigenvalues, we can use the projector $P_i = \frac{1}{2}(I + S_i)$. To project onto the simultaneous subspace, construct the projector

$$P = \frac{1}{2}(I + S_1)\frac{1}{2}(I + S_2)\frac{1}{2}(I + S_3) \tag{22}$$

(c) Use the projector you constructed in the last problem to find a basis for the subspace defined by the simultaneous equations $S_i|\psi\rangle = |\psi\rangle$.

From the theory of stabilizer codes this subspace will be two dimensional. Project onto the state $|0000\rangle$

$$P|0000\rangle = \frac{1}{8}(I+S_1)(I+S_2)(I+S_3)|0000\rangle = \frac{1}{4}(I+S_1)(I+S_2)|0000\rangle = \frac{1}{4}(|0000\rangle+|1100\rangle+|0011\rangle+|1111\rangle) \tag{23}$$

Normalize this produces on basis state:

$$|\phi_1\rangle = \frac{1}{2}(|0000\rangle + |1100\rangle + |0011\rangle + |1111\rangle) \tag{24}$$

To obtain a second vector, start with the vector $|0110\rangle$, which is orthogonal to this state, and project:

$$P|0110\rangle = \frac{1}{8}(I+S_1)(I+S_2)(I+S_3)|0110\rangle = \frac{1}{4}(I+S_1)(I+S_2)|0110\rangle = \frac{1}{4}(|0110\rangle+|1010\rangle+|0101\rangle+|1001\rangle) \tag{25}$$

Normalizing, we obtain a second basis element

$$|\phi_2\rangle = \frac{1}{2}(|0110\rangle + |1010\rangle + |0101\rangle + |1001\rangle) \tag{26}$$

(d) Find a Pauli group operator (i.e. one that can be written as a product of Pauli matrices, see problem set 1) which commutes with each of the S_i but which is not a product of the S_is (and is not identity).

An example of such a Pauli is $I \otimes X \otimes X \otimes I$, which commutes with S_1 and S_2 since both operators are made of I and X operators and which commutes with S_3 by a similar argument to part (a).

(e) Prove that $P \otimes I \otimes I \otimes I$ where P is a Pauli matrix anti-commutes (two operators anticommute if $AB = -BA$) with at least one of the elements S_i. Argue why this is true for $I \otimes P \otimes I \otimes I$, $I \otimes I \otimes P \otimes I$, and $I \otimes I \otimes I \otimes P$ where again P is a Pauli matrix.

We can easily check the three cases $P = X$, $P = Y$ and $P = Z$. First note that $XZ = -ZX$. Thus if $P = X$, then $(X \otimes I \otimes I \otimes I)S_3 = -S_3(X \otimes I \otimes I \otimes I)$ since $(X \otimes I \otimes I \otimes I)$ only acts nontrivially on one qubit and it anticommutes with S_3 ont his qubit. Similarly if $P = Y$ then $(Y \otimes I \otimes I \otimes I)S_3 = -S_3(Y \otimes I \otimes I \otimes I)$ and if $P = Z$ then $(Z \otimes I \otimes I \otimes I)S_1 = -S_1(Z \otimes I \otimes I \otimes I)$. We can further see that all other single qubit Paulis anticommute with either S_3 (if $P = X$ or $P = Y$) or with S_1 (if $P = Z$ and acts on the first two qubits) or with S_2 (if $P = Z$ and acts on the second two qubits.)

(f) If $S_i|\psi\rangle = |\psi\rangle$ and $QS_i = -S_iQ$, prove that $S_i(Q|\psi\rangle) = -(Q|\psi\rangle)$.

By definitions, $S_i(Q|\psi\rangle) = -QS_i|\psi\rangle = -Q|\psi\rangle$.

(g) Suppose we encode a single qubit into the subspace defined by $S_i|\psi\rangle = |\psi\rangle$. Now suppose a malicious person comes along and applies a Pauli operator of the form $P \otimes I \otimes I \otimes I$, $I \otimes P \otimes I \otimes I$, $I \otimes I \otimes P \otimes I$, $I \otimes I \otimes I \otimes P$, or $I \otimes I \otimes I \otimes I$ producing the new state $|\psi'\rangle$. Explain how determining the value of $S_i|\psi'\rangle$ can tell you whether one of the nontrivial Pauli operators was applied to $|\psi\rangle$ or whether $I \otimes I \otimes I \otimes I$ was applied to $|\psi\rangle$.

From part (f), we see that if an operator anticommutes with an S_j, then it moves the state out of the subspace defined by $S_j|\psi\rangle$ into a subspace where $S_j|\psi\rangle = -|\psi\rangle$. Notice that by part (e), all single qubit Pauli's anticommute with at least one S_j. Thus if you determine whether you are in the $+1$ or -1 eigenstates of the S_i, if a single Pauli has occurred, then at least one of these will be -1. If no Pauli has occured, then you will be in the $+1$ eigenstate of all S_i.

The subspace you've considered above is an example of a four qubit error detecting code: we can use measurements of the eigenvalues of the S_i operators to detect when a single error has happened on our encoded qubit.

Exercise 3: Decoherence-Free Subspaces

(a) Consider the following two qubit operators $X_2 = X \otimes I + I \otimes X$, $Y_2 = Y \otimes I + I \otimes Y$ and $Z_2 = Z \otimes I + I \otimes Z$. Find the two qubit state $|\psi\rangle$ which is annihilated by these three operators: $X_2|\psi\rangle = Y_2|\psi\rangle = Z_2|\psi\rangle = 0$.

Express $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$. Then $Z_2|\psi\rangle = 0$ implies that $a_{00} = a_{11} = 0$. Also $X_2|\psi\rangle = 0$ implies that $a_{01} + a_{10} = 0$, or $a_{01} = -a_10$. Thus, up to a global phase, the state is $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

(b) Suppose that we evolve a two qubit quantum system according to the Hamiltonian

$$H = s_x X_2 + s_y Y_2 + s_z Z_2. \tag{27}$$

In other words the evolution after a time t is $U(t) = \exp(-iHt)$. Prove that $U(t)|\psi\rangle = |\psi\rangle$ where $|\psi\rangle$ is the state you found in part (a).

$$\exp(-iHt)|\psi\rangle = \sum_{j=0}^{\infty} \frac{(-iHt)^j}{j!}|\psi\rangle = \sum_{j=0}^{\infty} \frac{(-it)^j}{j!} H^j|\psi\rangle \tag{28}$$

But $H|\psi\rangle = (s_x X_2 + s_y Y_2 + s_z Z_2)|\psi\rangle = 0$, so that $H^j|\psi\rangle = 0$ if $j \neq 0$. Thus the only term that survives is the $j = 0$ term:

$$\exp(-iHt)|\psi\rangle = H^0|\psi\rangle = |\psi\rangle \tag{29}$$

(c) Now consider two qubits which are attached to another quantum system whose Hilbert space is $\mathcal{H}$. Suppose that the two qubits and the bath interact via the Hamiltonian

$$H_{SB} = X_2 \otimes B_X + Y_2 \otimes B_Y + Z_2 \otimes B_Z \tag{30}$$

where the B_α operators act on $\mathcal{H}$. Show that if we start with the two qubits in the state from part (a) and the bath in an arbitrary state, then evolving using H_{SB} does change the state. In other words, defining $U_{SB}(t) = \exp(-iH_{SB}t)$, show that $U_{SB}(t)|\psi\rangle \otimes |\phi\rangle = |\psi\rangle \otimes |\phi\rangle$ where $|\psi\rangle$ is the state from part (a) and $|\phi\rangle$ is an arbitrary state in $\mathcal{H}$. What you've just shown is that for couplings between the system and bath of the above form, the state $|\psi\rangle$ is protected.

$$\exp(-iHt)(|\psi\rangle \otimes |\phi\rangle) = \sum_{j=0}^{\infty} \frac{(-iHt)^j}{j!}(|\psi\rangle \otimes |\phi\rangle) = \sum_{j=0}^{\infty} \frac{(-it)^j}{j!} H^j(|\psi\rangle \otimes |\phi\rangle) \tag{31}$$

But now $H(|\psi\rangle \otimes |\phi\rangle) = (X_2 \otimes B_X + Y_2 \otimes B_Y + Z_2 \otimes B_Z)(|\psi\rangle \otimes |\phi\rangle) = 0$, so again the only term that survives is the $j = 0$ term,

$$\exp(-iHt)(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\phi\rangle \tag{32}$$

(d) Now consider the four qubit operators

$$\begin{aligned} X_4 &= X \otimes I \otimes I \otimes I + I \otimes X \otimes I \otimes I + I \otimes I \otimes X \otimes I + I \otimes I \otimes I \otimes X \\ Y_4 &= Y \otimes I \otimes I \otimes I + I \otimes Y \otimes I \otimes I + I \otimes I \otimes Y \otimes I + I \otimes I \otimes I \otimes Y \\ Z_4 &= Z \otimes I \otimes I \otimes I + I \otimes Z \otimes I \otimes I + I \otimes I \otimes Z \otimes I + I \otimes I \otimes I \otimes Z \end{aligned} \tag{33}$$

Show that each of these operators annihilates the states $|\psi\rangle_{12} \otimes |\psi\rangle_{34}$, $|\psi\rangle_{13} \otimes |\psi\rangle_{24}$ and $|\psi\rangle_{14} \otimes |\psi\rangle_{23}$ where $|\psi\rangle_{ij}$ is the state from part (a) shared between qubits i and j.

Let $P^{(i)}$ be the Pauli operator P operating on the ith qubit and identity on all other qubits. Then, let $i \neq j \neq k \neq l$,

$$P_4|\psi\rangle_{ij} \otimes |\psi\rangle_{kl} = (P^{(i)} + P^{(j)} + P^{(k)} + P^{(l)})|\psi\rangle_{ij} \otimes |\psi\rangle_{kl} = (P^{(i)} + P^{(j)})|\psi\rangle_{ij} \otimes |\psi\rangle_{kl} + |\psi\rangle_{ij} \otimes (P^{(k)} + P^{(l)})|\psi\rangle_{kl} \tag{34}$$

But, via part (a), each of these vanishes. For $P \in \{X, Y, Z\}$ and i, j, k, l appropriately chosen, this yields what we wish to prove.

(e) Show that the states $|\psi\rangle_{12} \otimes |\psi\rangle_{34}$, $|\psi\rangle_{13} \otimes |\psi\rangle_{24}$ and $|\psi\rangle_{14} \otimes |\psi\rangle_{23}$ are not linearly independent.

$$\begin{aligned} -|\psi\rangle_{12} \otimes |\psi\rangle_{34} + |\psi\rangle_{13} \otimes |\psi\rangle_{24} + |\psi\rangle_{14} \otimes |\psi\rangle_{23} &= \frac{1}{2}(-|0101\rangle + |0110\rangle + |1001\rangle - |1010\rangle) \\ &+ \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle) \\ &+ \frac{1}{2}(|0101\rangle - |0011\rangle - |1100\rangle + |1010\rangle) \\ &= 0 \end{aligned} \tag{35}$$

Thus these vectors are not linearly independent.

(f) Construct a basis for the two dimensional space spanned by the states $|\psi\rangle_{12} \otimes |\psi\rangle_{34}$, $|\psi\rangle_{13} \otimes |\psi\rangle_{24}$ and $|\psi\rangle_{14} \otimes |\psi\rangle_{23}$.

Take the first basis state to be $|\phi_1\rangle = |\psi\rangle_{12} \otimes |\psi\rangle_{34}$. Then the second state must be a superposition of $|\psi\rangle_{13} \otimes |\psi\rangle_{24}$ and $|\psi\rangle_{14} \otimes |\psi\rangle_{23}$

$$|\phi_2\rangle = a|\psi\rangle_{13} \otimes |\psi\rangle_{24} + b|\psi\rangle_{14} \otimes |\psi\rangle_{23} \tag{36}$$

and orthogonal to $|\phi_1\rangle$,

$$\langle\psi|_{12} \otimes \langle\psi|_{34}(a|\psi\rangle_{13} \otimes |\psi\rangle_{24} + b|\psi\rangle_{14} \otimes |\psi\rangle_{23}) = 0. \tag{37}$$

This latter equation yields

$$\frac{1}{2}(a + b) = 0 \tag{38}$$

or $a = -b$. Up to a global phase the second basis state is thus

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle_{13} \otimes |\psi\rangle_{24} - |\psi\rangle_{14} \otimes |\psi\rangle_{23}) \tag{39}$$

(g) Suppose we encode a qubit of information into the subspace spanned by the two basis states in part (f). If these four qubits now interact with a bath via the Hamiltonian

$$H_4 = X_4 \otimes B_X + Y_4 \otimes B_Y + Z_4 \otimes B_Z \tag{40}$$

then show that the quantum information encoded into this subspace is unaffected by this evolution.

This follows via an argument nearly identical to part (c), but now using part (d). The fact that it is a subspace doesn't make much difference since all states in the subspace will be annihilated by the appropriate P_4 operator.

The two dimensional subspace described above is an example of a decoherence-free subspace. Such subspaces exist when the coupling between a system and its environment possess a symmetry: in this case the symmetry is that the qubits couple collectively to the bath. Such codes avoid symmetric decoherence without the need for quantum error correction.