Q. Inf. Science II (6.443/8.371/18.436) — Spring 2018

Assignment 5b - written part

Due: **Monday**, *May 7, 2018 at* ***5pm***

1. **Simultaneous block-diagonalization of two reflections**

Let Π_A, Π_B be two projectors onto subspaces of a d-dimensional space, let $R_A := 2\Pi_A - I_d, R_B := 2\Pi_B - I_d$ be the corresponding reflections, and let $S := -R_A R_B$ be their product (up to a phase). Let $a = \operatorname{tr}\Pi_A, b = \operatorname{tr}\Pi_B$ and choose orthonormal sets of vectors $|\alpha_1\rangle, \ldots, |\alpha_a\rangle, |\beta_1\rangle, \ldots, |\beta_b\rangle$ such that

$$\Pi_A = \sum_{i=1}^{a} |\alpha_i\rangle\langle\alpha_i| \qquad \Pi_B = \sum_{i=1}^{b} |\beta_i\rangle\langle\beta_i| \tag{1}$$

Let D be the $a \times b$ matrix with entries $D_{ij} = \langle\alpha_i|\beta_j\rangle$. Let the singular value decomposition of D be

$$D = \sum_i d_i |l_i\rangle\langle r_i|. \tag{2}$$

This problem will relate the singular values of D to the spectrum of S.

(a) Define isometries $V_A = \sum_{i=1}^{a} |\alpha_i\rangle\langle i|$ and $V_B = \sum_{i=1}^{b} |\beta_i\rangle\langle i|$. Express Π_A, Π_B, D in terms of V_A, V_B. Show that the subspace spanned by $\{V_A|l_i\rangle, V_B|r_i\rangle\}$ is invariant under the action of both Π_A and Π_B.

(b) From the previous part we know that S is block diagonal with block i corresponding to the space spanned by $\{V_A|l_i\rangle, V_B|r_i\rangle\}$. Find the eigenvalues of S corresponding to these blocks. When do we get a rank-1 matrix? (Hint: consider an orthonormal basis for $\operatorname{Span}\{V_A|l_i\rangle, V_B|r_i\rangle\}$ and write down S in terms of these bases.)

(c) *Oblivious amplitude amplification.* Suppose we know how to perform a unitary U on $m+n$ qubits such that there exist linear operators V, W such that for any $|\psi\rangle \in \mathbb{C}^{2^n}$,

$$U|0^m\rangle|\psi\rangle = \sin(\theta)|0^m\rangle V|\psi\rangle + \cos(\theta)W|\psi\rangle. \tag{3}$$

Here V is a $2^n \times 2^n$ unitary matrix, W is a $2^{m+n} \times 2^n$ isometry and $(\langle 0^m| \otimes I_{2^n})W = 0$. We can think of V as the desired evolution and W as some unwanted evolution; i.e. our goal is to map $|\psi\rangle$ to $V|\psi\rangle$. One way to do this is to perform U and measure the first m qubits, keeping the outcomes where we obtain 0^m. However this has probability of success only $\sin^2(\theta)$ and upon failure can damage the state.

Instead we will construct two reflections:

$$R_A = (I_{2^m} - 2|0^m\rangle\langle 0^m|) \otimes I_2^n \tag{4}$$

$$R_B = U^\dagger R_A U. \tag{5}$$

What are the eigenvalues of $S = -R_A R_B$? (Hint: use part b) How can we apply powers of S to increase our chances of obtaining $V|\psi\rangle$?

Describe qualitatively what happens if we drop the assumption that V, W are isometries? (However, note that (3) and the fact that U is unitary will still impose some constraints on the possible choices of V, W.)

2. **Types.** Given a sequence $x^n = x_1, x_2, \ldots, x_n \in [d]^n$ and a symbol $a \in [d]$, let $N(a|x^n)$ be the number of occurrences of a in x^n. The *type* (or empirical probability distribution) of x^n is the distribution that results from choosing a random letter from x^n, i.e. $P_{x^n}(a) = N(a|x^n)/n$. Here we use P_{x^n} to denote the type of x^n. Let $\mathcal{P}_n$ denote the set of all possible types of sequences in $[d]^n$; equivalently $\mathcal{P}_n$ is the set of probability distributions on $[d]$ whose entries are integer multiples of $1/n$. Let $\mathcal{T}_p^n := \{x^n : P_{x^n} = p\}$. Note that

$$|\mathcal{T}_p^n| = \binom{n}{np} := \frac{n!}{np_1! np_2! \cdots np_d!}. \tag{6}$$

(a) List the elements of $\mathcal{P}_3$ when $d = 3$.

(b) Prove the upper bound
$$|\mathcal{P}_n| \leq (n+1)^{d-1}. \tag{7}$$

(c) Prove that for $x^n \in \mathcal{T}_p^n$,
$$p^n(x^n) := p(x_1) \cdots p(x_n) = 2^{-nH(p)} \tag{8}$$

(d) For types $p, q \in \mathcal{P}_n$, compute $p^n(\mathcal{T}_q^n)$ where we use the notation $p^n(S)$ to mean $\sum_{x^n \in S} p^n(x^n)$. Express your answer in terms of $H(q) = \sum_x q(x) \log(1/q(x))$ and $D(q\|p) = \sum_x q(x) \log(q(x)/p(x))$.

(e) It turns out that $p^n(\mathcal{T}_q^n)$ takes on its maximum value (as a function of q) when $q = p$. You do not need to prove this. Use this fact, along with the previous parts, to prove that
$$\frac{2^{nH(p)}}{(n+1)^d} \leq |\mathcal{T}_p^n| \leq 2^{nH(p)}. \tag{9}$$

(f) Pinsker's inequality (which you can use without proof) states that
$$D(q\|p) \geq \frac{1}{2 \ln 2} \|p - q\|_1^2. \tag{10}$$

Combine this with the last two parts to prove that
$$p^n(\mathcal{T}_q^n) \leq e^{-n \frac{\|p-q\|_1^2}{2}}. \tag{11}$$

(g) One consequence of (11) is a weak version of a Chernoff bound. Suppose that we have a coin with probability a of heads and probability $1-a$ of tails. If we flip it n times show that the probability of $\geq nb$ heads for $b > a$ decreases exponentially with n.

(h) We can also use types to define a sharper version of typical sets. Define

$$\mathcal{T}^n_{p,\delta} = \bigcup_{q:\|p-q\|_1\leq\delta} \mathcal{T}^n_q. \tag{12}$$

Prove that $1 - p^n(\mathcal{T}^n_{p,\delta})$ is exponentially small for fixed p and fixed $\delta > 0$.

3. **Unweighted Quantum Adversary Bound**

In this problem, we will walk you through a simple version of the quantum adversary bound. Suppose we are given a quantum query algorithm to compute a function $f(x)$ that, with the initial state $|0^n\rangle$ and an N-bit input x produces the output state $|\phi_x\rangle$ using T queries to the input. The input is specified by an oracle $O_x = \sum_{i=1}^{N}(-1)^{x_i}|i\rangle\langle i|$. The algorithm consists of a sequence of unitary transformations and calls to the oracle:

$$U = U_T O_x U_{T-1} O_x \dots U_1 O_x U_0.$$

(a) Suppose that the input x is encoded in an additional N-qubit register. From the algorithm U, construct a unitary V such that $V|0^n\rangle \otimes |x\rangle = |\phi_x\rangle \otimes |x\rangle$. Your unitary should have the form $V = V_T O' V_{T-1} \dots V_1 O' V_0$, where V_t and O' are unitaries that act on the full $n+N$-qubit space. What are these matrices in terms of U_t and O_x?

(b) The advantage of writing the algorithm in this way is that we can work with superpositions over possible inputs. Let S be a set of input strings, and let the initial state be

$$|\psi_0\rangle = |0^n\rangle \otimes \sum_{x\in S} \alpha_x |x\rangle. \tag{13}$$

The final state after applying the algorithm V is

$$|\psi_T\rangle = \sum_{x\in S} \alpha_x |\phi_x\rangle \otimes |x\rangle. \tag{14}$$

Find the N-qubit reduced density matrices ρ_0 and ρ_T describing the input (i.e. second) register of $|\psi_0\rangle$ and $|\psi_T\rangle$. (In general, we will denote the reduced state of this register at time t, i.e. immediately after the application of V_t, by ρ_t).

(c) Now, suppose that the algorithm computes f on all inputs with probability of error $\leq \epsilon$, and choose two inputs x, y such that $f(x) \neq f(y)$. Recall from the trace distance problem (TD4.4) on pset 1a that this implies that

$$|\langle\phi_x|\phi_y\rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}. \tag{15}$$

Show that

$$|\langle x|\rho_T|y\rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}|\alpha_x||\alpha_y|. \tag{16}$$

(d) Choose sets X, Y such that $f(x) \neq f(y)$ for all $x \in X, y \in Y$. Let $S = X \cup Y$ and set the weights $\alpha_x = \frac{1}{\sqrt{2|X|}}$ for $x \in X$ and $\alpha_y = \frac{1}{\sqrt{2|Y|}}$ for $y \in Y$. Further suppose that there exists a relation $R \subseteq X \times Y$ such that for every $x \in X$, there exist at least m different $y \in Y$ such that $(x, y) \in R$, and for every $y \in Y$, there exist at least m' different $x \in X$ such that $(x, y) \in R$. For each timestep, define $S_t = \sum_{(x,y)\in R} | \langle x| \rho_t |y\rangle |$. Show that

$$S_0 - S_T \geq (\frac{1}{2} - \sqrt{\epsilon(1-\epsilon)})\sqrt{mm'}. \tag{17}$$

(e) Now suppose the relation R from the previous part has the further property that for every $x \in X$ and $i \in [N]$, there exist at most ℓ values $y \in Y$ such that $(x, y) \in R$ and $x_i \neq y_i$. Likewise, for every $y \in Y$ and $i \in [N]$, there exist at most ℓ' values $x \in X$ such that $(x, y) \in R$ and $x_i \neq y_i$. It turns out that for any two successive timesteps $t, t+1$, the difference $S_{t+1} - S_t$ is upper bounded by

$$|S_{t+1} - S_t| \leq \sqrt{\ell\ell'}. \tag{18}$$

(proving this is not a required part of this problem - but you are encouraged to try).

Conclude that any algorithm to compute f with error $\leq 1/3$ must make at least $\Omega(\sqrt{\frac{mm'}{\ell\ell'}})$ queries. Use this to deduce that it takes at least $\Omega(\sqrt{N})$ queries to compute the OR function. Specify your choice of X, Y, and R.

(f) Suppose $f : \{0,1\}^N \to \{0,1\}$ is a symmetric function meaning that $f(x)$ depends only on the Hamming weight $k = |x| = x_1 + \ldots + x_N$. In other words $f(x) = g(|x|)$ for some function $g : \{0, 1, \ldots, N\} \to \{0,1\}$. Suppose that $g(k^*) \neq g(k^* + 1)$ for some k^*. Prove that the quantum query complexity of f is lower bounded by

$$Q(f) = \Omega(\sqrt{(N - k^*)(k^* + 1)}). \tag{19}$$

What bound do you get for the MAJORITY function? (MAJORITY is 1 if $|x| \geq N/2$ and 0 if $|x| < N/2$.)