Homework 6
Due 2006/4/30

Oded Regev & Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

1. As we have seen, if Alice and Bob share EPR pairs, they are able to perform the following task without any communication between them: if Alice has some bit a, and Bob some bit b, Alice can compute a bit s and Bob can compute a bit t such that

$$\Pr[s \oplus t = a \wedge b] \approx 0.85$$

(make sure you remember how this is done). By a result of Tsirelson we know that this is the best possible under the laws of quantum mechanics. But what would happen if we had some magical way to improve this probability (say, under some yet-unknown laws of nature)?

- So let us assume that Alice and Bob have some way to compute, given any a and b, s and t such that the above probability is 100%. Show that if Alice is given a bit string $a = (a_1, \ldots, a_n)$ and Bob is given a bit string $b = (b_1, \ldots, b_n)$, they can compute bits s, t such that $s \oplus t = \mathrm{IP}(a, b)$ where

$$\mathrm{IP}(a,b) = \sum_{i=1}^{n} a_i \wedge b_i \text{ mod } 2.$$

- Generalize this by showing that for any Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$, Alice and Bob, given bit strings a, b, can compute bits s, t such that $s \oplus t = f(a, b)$. Hint: any Boolean function can be computed using AND gates and NOT gates.
- Deduce that the (classical) communication complexity of any function $f : \{0,1\}^{2n} \to \{0,1\}$ becomes just one bit.

2. Recall that in an exact communication protocol for a function $f(x, y)$, Alice and Bob start in the state $|x,0\rangle_A |y,0\rangle_B |0\rangle_C |\Phi\rangle_E$ with A being Alice's system, B being Bob's system, C being the one-qubit communication channel, and $|\Phi\rangle_E$ being some fixed state shared between them. At the end of the protocol, the C qubit contains the value $f(x, y)$.

- Show that any such protocol with q communication, can be converted into a protocol that performs the unitary mapping

$$|x,0\rangle_A |y,0\rangle_B |0\rangle_C |\Phi\rangle_E \to (-1)^{f(x,y)} |x,0\rangle_A |y,0\rangle_B |0\rangle_C |\Phi\rangle_E$$

and in which Alice sends q qubits (and also Bob sends q qubits).
- Assume there exists an exact communication protocol for the inner product on two n-bit strings with q qubits of communication. Show how Alice can use this protocol to transfer to Bob n bits of information while sending only q qubits to Bob.
- It follows from a theorem by Holevo that in order for Alice to transfer n classical bits of information to Bob, she must send him at least $\lceil n/2 \rceil$ qubits, even if they share unlimited entanglement. Use this fact to prove a lower bound of $\lceil n/2 \rceil$ on the exact quantum communication complexity of the inner product function, even in the presence of unlimited entanglement.

Oded Regev & Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

3. Our goal is to extend the lower bounds on communication complexity to the case where Alice and Bob share unlimited entanglement. Recall that if Alice and Bob share the E-dimensional maximally entangled state (equivalently, $\log E$ EPR pairs) then their initial state can be written as

$$\frac{1}{\sqrt{E}} \sum_{e=1}^{E} |e, x, 0\rangle_A |0\rangle_C |e, y, 0\rangle_B.$$

Recall also that we define the Frobenius norm as $\|A\|_F = (\sum_i s_i^2)^{1/2} = (\mathrm{tr}(A^\dagger A))^{1/2} = (\sum_{ij} |a_{ij}|^2)^{1/2}$, the operator norm as $\|A\| = \max s_i = \max_{x:\|x\|=1} \|Ax\|$, and the trace norm as $\|A\|_{tr} = \sum_i s_i$ where s_i are the singular values of A. All three norms are invariant under unitary transformations, $\|UAV\| = \|A\|$.

- It can be shown that for any matrices A and B, $\|AB\|_{tr} \le \|A\|_F \|B\|_F$ (try). Show how this can be used to give a slightly different proof to the inequality $\|P\|_{tr} \le 2^{2q-2}\sqrt{|X| \cdot |Y|}$ (without entanglement).
- Show that for any protocol with entanglement as above, we can find a $|X| \times 2^{2q-2}E^2$ matrix A and a $2^{2q-2}E^2 \times |Y|$ matrix B such that $P = \frac{1}{E}AB$.
- Let R_1, R_2 be linear operators with operator norm $\|R_1\|, \|R_2\| \le 1$ and let $u_1, \ldots, u_E$ be E orthonormal vectors. Show that

  $$\sum_{i,j} |\langle u_i | R_1^\dagger R_2 | u_j \rangle|^2 \le E$$

  (for $R_1 = R_2 = I$ we have equality). Hint: this expression can be written as $\|U^\dagger R_1^\dagger R_2 U\|_F^2$ where U is the matrix whose columns are $u_1, \ldots, u_E$; then prove and use the fact that for any $E \times E$ matrix W, $\|W\|_F \le \sqrt{E}\|W\|$.
- Prove that $\|P\|_{tr} \le 2^{2q-2}\sqrt{|X| \cdot |Y|}$ holds even if Alice and Bob share an unlimited number of EPR pairs (and hence our lower bounds on disjointness and inner product hold also with shared EPR pairs).