CS286.2 Around the Quantum PCP Conjecture

Exercise sheet 1

9/30/2014

Multiplayer games.

1. Define the *randomized* value $\omega_r(G)$ of a k-player game $G = (Q_i, A_i, \pi, V)$ as the maximum success probability of players that are allowed to use private as well as shared randomness as part of their strategies. Formally,

$$\omega_r(G) \;=\; \sup_{R,\mu,f_i} \sum_{q_i} \pi(q_1,\ldots,q_k) \sum_{r\in\{0,1\}^R} \mu(r) V\big(f_1(q_1,r),\ldots,f_k(q_k,r);q_1,\ldots,q_k\big),$$

   where the supremum runs over all integers R, probability disributions μ on $\{0,1\}^R$ (the shared randomness), and functions $f_i : [Q_i] \times \{0,1\}^R \to [A_i]$. Show that $\omega_r(G) = \omega(G)$.

2. Give a transformation from any k-player game G to a 2-player game G such that

$$\omega(G) \leq \omega(G') \leq 1 - \frac{C}{k}\big(1-\omega(G)\big),$$

   for some universal (independent of the game G and of k) constant C.

Error reduction. Recall that $\mathrm{PCP}_{c,s}(r,q)_\Sigma$ is the set of languages L that have a PCP verifier that uses at most r random bits, makes at most q queries to a proof over the alphabet Σ, and accepts $x \in L$ with probability at least c and $x \notin L$ with probability at most s.

1. Show that for any $0 < \varepsilon \leq 1/2$ and functions $r, q : \mathbb{N} \to \mathbb{N}$ there exists k', q' such that $\mathrm{PCP}_{1,1/2}(r,q)_\Sigma \subseteq \mathrm{PCP}_{1,\varepsilon}(r',q')_\Sigma$. How do k' and q' depend on k, q and ε? Can you do better?

2. Answer the same questions for the inclusion $\mathrm{PCP}_{2/3,1/3}(r,q)_\Sigma \subseteq \mathrm{PCP}_{1-\delta,\varepsilon}(r'',q'')_\Sigma$ for arbitrary $\varepsilon, \delta > 0$.

3. For any $\varepsilon, \delta > 0$ give a transformation mapping any k-player game G to a k'-player game G' such that $\omega(G) = 1 \implies \omega(G') = 1$ and $\omega(G) \leq 1-\delta \implies \omega(G') \leq \varepsilon$. How does k' depend on k, δ and ε? Can you suggest a transformation achieving the same, while keeping k' constant (perhaps changing other parameters of the game)?

Hardness of approximation for CLIQUE.

1. Show that the PCP theorem implies that there exists an $\alpha < 1$ such that the following is NP-hard: given a graph G and an integer k, decide whether

   - (YES) G has a clique of size at least k, or
   - (NO) All cliques in G have size at most αk.

2. Given a graph $G = (V, E)$ and an integer k, define the k-th product of G, G^k, as the graph with vertex set $V' = V^k$ (the cartesian product of V with itself k times) and edge set $E' = \{((u_1, \ldots, u_k), (v_1, \ldots, v_k))\}$ such that $\{u_1, \ldots, u_k, v_1, \ldots, v_k\}$ is a clique in G.

   Show that the size of the largest clique in G^k is the k-th power of the size of the largest clique in G.

3. Deduce that MAXCLIQUE is NP-hard to approximate to within *any* $0 < \alpha < 1$.

Local decodability. In class we saw that the class $\mathcal{C}$ of linear functions $f : \{-1,1\}^n \to \{-1,1\}$ was locally testable: there exists a randomized procedure, making three queries to the table of values of f, that is such that if $f \in \mathcal{C}$ the test always accepts, but if f is not ε-close to $\mathcal{C}$ then the test accepts with probability at most $1 - \Omega(\varepsilon)$.

Call a class $\mathcal{D}$ *locally decodable* if there exists a randomized procedure such that, given access to the table of values of an $f : \{-1,1\}^n \to \{-1,1\}$ that is promised to be ε-close to some $g \in \mathcal{D}$, and any $x \in \{-1,1\}^n$, makes a constant number of queries to f and outputs a value y such that $y = g(x)$ with probability at least $1 - \Omega(\varepsilon)$.

1. Give a simple example of a class $\mathcal{D}$ that is locally testable but not locally decodable.

2. Show that the class $\mathcal{C}$ of all linear functions is locally decodable with only two queries.

3. Suppose f is ε-close to some $g \in \mathcal{C}$. How many queries (as a function of ε and n) do you need to recover the complete function g with probability at least $2/3$?

The "Long Code" test. Let $\mathcal{D} = \{\chi_i : i \in [n]\}$ be the set of "dictator functions" (recall that for any $S \subseteq [n]$, χ_S is the function from $\{-1,1\}^n$ to $\{-1,1\}$ such that $\chi_S : x \mapsto \prod_{i \in S} x_i$). In this problem we show that $\mathcal{D}$ is locally testable with 6 queries.

1. Explain why a class $\mathcal{C}$ being locally testable does not imply that a subclass $\mathcal{C}' \subseteq \mathcal{C}$ is automatically locally testable. Give an example of a function that demonstrates that the BLR linearity test is not a proper local test for $\mathcal{D}$.

2. Let $a, b, c \in \{-1,1\}$. Write an expression that is 1 they are not all equal (NAE) and is 0 if they are all equal.

3. Consider the following 3-query test, called the NAE test, on an unknown function f: Pick 3 strings $x, y, z \in \{-1,1\}^n$ at random by choosing each triple (x_i, y_i, z_i) independently and uniformly at

random from the set of strings $\{-1,1\}^3 \setminus \{(-1,-1,-1),(1,1,1)\}$; then test that $f(x)$, $f(y)$, and $f(z)$ are NAE. Show that

$$\Pr[\text{NAE test accepts}] = \frac{3}{4} - \frac{3}{4} \sum_{S \subseteq [n]} \widehat{f(S)}^2 (-1/3)^{|S|}.$$

Clearly if $f \in \mathcal{D}$ the NAE test accepts with probability 1.

4. Show that $\mathcal{D}$ is locally testable with 6 queries. (Hint: combine the BLR test and the NAE test.)

$(**)$ **Quantum PCP.** Formulate "quantum" analogues of the three concepts — proof-checking verifiers, multiplayer games, and constraint satisfaction problems. What would a "quantum PCP theorem" say about them? Are the three resulting statements equivalent?