6.896 Sublinear Time Algorithms		September 11, 2004
	Lecture 17	
Lecturer: Eli Ben-Sasson		*Scribe: Rafael Pass*

1 Lower Bounds for Property Testing: Rest of the Proof

This lecture is the continuation of the previous one, in which we prove the following Theorem, stated last time:

Theorem 1 ([1]) *There exists integers c, d, and values $\delta > 0, 0 < \epsilon < 1/2, \gamma > 0$ such that for all sufficiently large n, with high probability, for a random low density parity check code (LDPC) every $(\delta, 0, \epsilon, q)$ linear test requires $q \geq \gamma n$ queries.*

As mentioned in the previous lecture, this result also extends to *any* test, and not just linear tests. Towards the goal of proving the above theorem we rely on Yao's minmax principle, which (in our case) boils down to showing one "bad" distribution over inputs, such that every deterministic linear test fails with probability larger than ϵ. We continue to use the notation and definitions from previous lecture.

1.1 The "bad" distribution

Recall that the code V defined by the constraint matrix A is $V = \ker(A) = \{x \in F_2^n | Ax = 0\}$. Let B_i be the uniform distribution over strings that *falsify* constraint A_i, but satify the rest, i.e., $B_i = \ker(A_{-i}) - \ker(A)$, where A_{-i} is the matrix obtained by removing row i from A. Define the "bad" distribution to be the uniform convex combination of B_i's. In other words, the "bad" distribution is obtained by uniformly chosing $i \in [m]$ (recall m is the number of rows in A) and then uniformly chosing an element in B_i. Note that it follows from the definition of B that for every $w \in B$, $w \notin V$. In fact, every $w \in B$ is "far" from V, as is shown in the following lemma (a proof sketch of the lemma is given in the next section).

Lemma 2 *For every sufficiently large c, d there exists $\delta > 0$ such that with high probability (over random (c, d)-regular LDPC codes) every $w \in B$ is δ-far from V.*

We next show that every linear test will accept a random word in B. Towards this goal we define the concept of "locality", and rely on the following lemmas:

Definition 3 *A is called (q, ϵ')-local if for all $u \in F_2^n$ such that u is a sum of more than $\epsilon' m$ rows of A, $|\text{Supp}(u)| \geq q$ (where $|\text{Supp}(u)| =$ number of non-zero entries of u).*

Lemma 4 *For all sufficiently large integers c, d, there exist constants $\gamma, \epsilon' > 0$ such that with high probability (over A), A is (q, ϵ')-local where $q = \gamma n$*

Lemma 5 *If A is (q, ϵ')-local then $\Pr_{w \in B}[w \not\perp V_I^\perp] < 2\epsilon'$. (Recall that $V_I^\perp = \{u \in V^\perp : \text{Supp}(u) \subseteq I\}$.)*

Proof of Theorem 1 Armed with the above lemmas we return to showing the main theorem. Recall that we need to show that every *fixed* linear test accepts (with high probability) random instances in B (i.e., the "bad" distribution). Fix a linear test making the queries indexed by $I \subset [n], |I| \leq q = \gamma n$. We need to show that $\Pr_{w \in B}[w \perp V_I^\perp] \geq 1 - \epsilon$. This follows directly by combining Lemma 4 and Lemma 5. By Lemma 4, a random code is $(\gamma n, \epsilon')$-local. By Lemma 5, this implies $\Pr[w \not\perp V_I^\perp] \leq 2\epsilon'$. Finally, by Lemma 2, B is "far" from being in V. We conclude the fixed linear test accepts with high probability instances from a distribution B that is far from V. Yao's minmax Theorem implies any randomized linear tester must fail on some input with high probability, completing the proof of Theorem 1.

1.2 Proof Sketches of the Lemmas

To prove the Lemmas we need to work with expander graphs and their application to low density parity check (LDPC) codes, introduced by Gallagher [2].

Expansion and Random Codes We start by defining expander graphs. Intuitively a bipartite graph G, with vertices $L \cup R$ is an expander if every "small" subset of vertices in L, has a "large" number of neighbors in R.

Definition 6 (Bipartite Expanders) *A (c,d)-regular bipartite graph G, with vertices $L \cup R|L| = n, |R| = m$, is called a (α, ϵ) expander if for every subset $S \subseteq L$, such that $|S| \leq \epsilon n$, $|N(S)| > \alpha|S|$, where $N(S)$ denotes the set of neighbours of the vertices in S.*

We state without proof the following claim about random regular graphs. Its proof is a standard application of the probabilistic method (see [1] for details).

Claim 7 *For all $c, d \geq 2$, any constant $\alpha \leq c-1$, there exists an $\epsilon = \epsilon_{c,d,\alpha}$ such that, with high probability over random (c,d)-regular graphs, G is (α, ϵ)-expanding.*

We continue by noting that expanders are good codes. Recall that the distance of a code C is defined as follows, $\delta(C) = min_{x,y \in C, x \neq y} \delta(x,y)$. If C is linear, then $\delta(C) = min_{u \in C, u \neq 0} |u|$.

For G a (c,d)-regular bipartite graph with n left vertices (vertex set is denoted L) and m right vertices (vertex set is denoted R), we define the constraint matrix $A = A_G$ to be the $m \times n$ matrix with entries in F_2. The rows of the matrix are labeled by elements of R and the columns by elements of L. The i,j entry is one iff $(i,j) \in E(G)$ (and zero otherwise). Notice each row of A has support of size d. Finally, the LDPC code defined by G is $LDPC_G = \ker(A_G)$.

Theorem 8 (Expanders give good codes) *[2] If G is a (c,d)-regular graph that is (α, ϵ)-expanding and $\alpha > c/2$, then $LDPC_G$ has a minimum distance $> \epsilon n$.*

Proof Let $S = \mathrm{Supp}(u), u \in C, u \neq 0$. Assume, for contradiction, that $|S| \leq \epsilon n$. By the expansion property, $|N(S)| > \alpha|S| > c/2|S|$. However, in order for u to be in C, we must have $A_G \cdot u = 0$. This implies each vertex of R must have either zero, or at least two neighbors in S. Since each element in S has c neighbors and each such neighbor has at least two incoming edges from S, this means that $c|S|/2 \geq |N(S)|$, contradiction. ■

Proof of Lemma 2 It suffices to prove that for every i, $\ker(A_{-i})$ has large distance. Indeed, if we prove this, then $|\ker(A_{-i})| = 2|\ker(A)|$ (removing a constraint from A increases the dimension of the kernel), and $\ker(A) \subset \ker(A_{-i})$. Thus, every element of $\ker(A_{-i}) - \ker(A)$ must be far from our code ($= \ker(A)$). By Theorem 8, proving $\ker(A_{-i})$ has large distance boils down to showing that the expander graph G remains a good expander, even when a single vertex in R is removed. But this is immediate, as removing a single vertex on the left can only decrease the size of the neighbor set of $S \subseteq L$ by at most one.

Proof of Lemma 4 The proof of lemma 4 is similar in spirit to that of Lemma 2 (but more complicated), so we omit it.

Proof of Lemma 5 For $u \in V^{\perp}$, let $u = b_u^T \cdot A$. Let $J_I = \cup_{u \in V_I^{\perp}} \mathrm{Supp}(b_u)$. Note that, clearly, $J_I \subseteq [m]$.

Claim 9 *For $w \in B_i$, it holds that $w \not\perp V_I^{\perp}$ iff $i \in J_I$.*

Proof By construction, $\langle w, A_j \rangle$ is one if $j = i$ and is zero otherwise. If $i \in J_I$, then $A_i \in V_I^{\perp}$ and $\langle w, A_i \rangle = 1$ so $w \not\perp V_I^{\perp}$.

On the other hand, if $i \notin J_I$, consider any $u \in V_I^{\perp}$ and express u as a sum of rows of A in the following manner: $u = \sum_{j \in J_I} \alpha_j A_j$ where $\alpha_j \in F_2$. We get $\langle u, w \rangle = \sum_{j \in J_I} \alpha_j \langle A_i, w \rangle = 0$. This happens for all $u \in V_I^{\perp}$, implying $w \perp V_I^{\perp}$. ■

We state the following claim without proof.

Claim 10 *If A is (q, ϵ')-local, then for all $I \subset [n], |I| \leq q$ we have $|J_I| \leq 2\epsilon' m$.*

We now finish the proof of Lemma 5. Recall our random "bad" input w is selected uniformly at random from $\{B_1, \ldots, B_m\}$. Let i be such that $w \in B_i$. By Claim 10, with probability $\geq 1 - 2\epsilon'$ we have $i \notin J_I$. By Claim 10 in this case we have $w \perp V_I^{\perp}$. Thus, the probability that w is not orthogonal to $V_I^{\perp}$ is at most $2\epsilon'$, as claimed.

References

[1] E. Ben-Sasson, P. Harsha and S. Raskhodnikova. Some 3CNF Properties are Hard to Test. To appear in SIAM Journal on Computing. Preliminary version appeared in STOC 2003.

[2] R. G. Gallager, *Low Density Parity-Check Codes.* MIT Press, Cambridge, MA, 1963.