Workshop V - PCP basics

September 30, 2016

The first three presentations should take 5-10 minutes each, while the latter two should take fifteen minutes each.

1 Hardness of Approximation for Max-Clique

Recall that the Max-Clique problem for a graph $G = (V, E)$ is to find the size of the largest clique in the graph. We can define the gap version as well: For $s < 1$, Gap-Clique-s is the problem of given some G and number k, deciding whether G contains a clique of size k or if all cliques in G are of size at most sk. Show that there is some constant s such that Gap-Clique-s is NP-Hard.

2 Randomness Efficient Error Amplification

For a vertex v denote by $\Gamma(v)$ the set of its neighbors. We define a (δ, ϵ)-sampler as a bi-regular bipartite graph (A, B, E) with the following property: given any set $B' \subset B$ the fraction of vertices $a \in A$ such that $\frac{|\Gamma(a) \cap B'|}{|\Gamma(a)|} > \frac{|B'|}{|B|} + \epsilon$ is at most δ.

Show that for any $\delta > 0$ if $L \in PCP_{0.9,0.8}[r, q]$, then $L \in PCP_{1-\delta,\delta}[r + O(\log(\frac{1}{\delta})), q \cdot O(\log\log(\frac{1}{\delta})]$. You may use without proof that for any set B and number $\delta > 0$, there is a $(\delta, 0.001)$-sampler (A, B, E) where $|A| = |B| \cdot O((1/\delta)^{O(1)})$ and the degree of the A vertices is $O(\log\log(1/\delta))$.

3 Two Queries Suffice

3.1

Suppose $L \in PCP_{1,s}[r, q]_{\{0,1\}}$. Show that $L \in PCP_{1,1-1/q+s/q}[r + \log(q), 2]_{\{0,1\}^q}$. Notice that going to two queries can cause a significant loss in soundness.

3.2

The *agreement* between two strings $a, a' \in \Sigma^n$ is the fraction of indices $i \in [n]$ in which $a_i = a'_i$. The *agreement* between a string $a \in \Sigma^n$ and a set of strings $A \subseteq \Sigma^n$ is the largest

agreement between a and a' where $a' \in A$.

Suppose that we start with a PCP verifier that makes q queries to a proof over alphabet Σ, and whose soundness guarantee is stronger in the following way. On an input not in L, instead of requiring the verifier to accept the prover's answers with probability at most s, we require that in expectation over the randomness of the verifier, the agreement between the provers' answers as a string in Σ^q and the set of strings in Σ^q that the verifier would have accepted on this randomness, is at most s. Show that with this stronger notion of PCP soundness we can reduce the number of queries to two with no loss in soundness. (The soundness guarantee of the new PCP verifier would be the usual one; only the soundness of the initial PCP verifier is stronger).

4 Degree Reduction

We will denote by Label Cover-s the problem of distinguishing label cover instances which are completely satisfiable from those that are at most s satisfiable. Let $\alpha < 1$ be some parameter. For some constants c, c' give an efficient reduction from Label Cover-s instances $I = (L, R, E, \Sigma_L, \Sigma_R, \{f_e\})$ with average right degree d to Label Cover-$(s + c\alpha)$ instances $I' = (L', R', E', \Sigma_L, \Sigma_R, \{f_e\})$ such that the underlying graph is right c'/α^4 regular, and there are $d|R|$ right vertices. You may use without proof that we can efficiently construct an (α, α^2) sampler $G = (L, R, E)$ with $|L| = |R| = n$ for any size n.

5 Alphabet Reduction

Let Σ, σ be finite alphabets. You can think of σ being smaller than Σ. We say $C : \Sigma \to \sigma^k$ is a code with relative distance $1 - \epsilon$ if for any $a \neq b$, $C(a)$ and $C(b)$ differ in at least $(1 - \epsilon)k$ indices.

You may assume without proof that there exists a code $C : \Sigma_R' \to \sigma^k$ with relative distance $1-\eta^3$ for some $\eta < 1/4$. Give an efficient reduction from Label Cover-s instances $I = (L, R, E, \Sigma_L, \Sigma_R, \{f_e\})$ to Label Cover-$(s+3\eta)$ instances $I' = (L', R' \times [k], E', \Sigma_R, \sigma, \{f_e\})$.