CS 880: Advanced Complexity Theory 4/14/06

Lecture 27: Resolution Lower Bounds

Instructor: Dieter van Melkebeek Scribe: Michael Kowalczyk

Today we will finish our application to proof complexity where we prove lower bounds on the resolution proof system using expanders. We will also say a few words about Tseitin tautologies.

1 Resolution Lower Bounds

1.1 Proving that last lemma

Recall that we proved the following result last time.

Theorem 1. *Let ϕ be a k-CNF, $\phi \notin SAT$. Then the minimum refutation length is*

$$\ell(\phi) = 2^{\Omega\left(\frac{(w(\phi)-k))^2}{n}\right)}$$

where $w(\phi)$ is the minimum width of the refutation of ϕ and n is the number of variables.

So in order to prove an exponential lower bound on $\ell(\phi)$, it suffices to prove a linear lower bound on $w(\phi)$. Recall we also defined G_ϕ, which is a bipartite graph with the clauses of ϕ on the left, the variables of ϕ on the right, and edges between each clause and the variables in that clause. This construction was used in the following theorem.

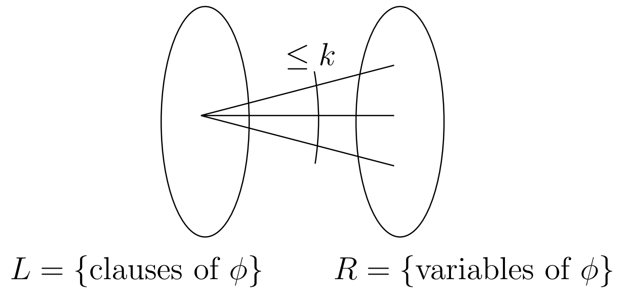

Figure 1: The underlying graph G_ϕ corresponding to formula ϕ

Theorem 2. *If G_ϕ is (K, c)-expanding then $w(\phi) > \frac{K}{2}(c-1)$.*

But to complete the proof of this, we still need to prove a lemma which was also stated last time.

Lemma 1. *Let C be a clause and $S \subseteq L$ from which C can be minimally derived (that is, we cannot derive C from a proper subset of S). If $|S| \leq K$ then $|C| \geq (c-1)|S|$.*

The idea here is that it is not possible to derive a small C from some small set S. If we consider small S and C, then many of the variables which influence S will be outside of C because of the expansion. If we have just one variable outside of C in each case, then we can set all the literals in C to false so that C is not satisfied, but still have enough degrees of freedom so that S can be satisfied, which is a contradiction.

Proof. We will show $|C| \geq |\Gamma(S)| - |S|$, which immediately gives the result. Certainly, this is true when $S = \emptyset$, so let S' be a maximal subset of S for which $|C| \geq |\Gamma(S')| - |S'|$ (the fact that the condition is satisfied by $\emptyset$ means S' is well-defined). If $S = S'$ then we are done so assume that $S' \neq S$ and we will derive a contradiction.

We claim that for any $S'' \subseteq S \setminus S'$ that $|\Gamma(S'') \setminus (\Gamma(S') \cup C)| - |S''| \geq 0$. Too see this, suppose otherwise. Then $S'' \neq \emptyset$, but then $S'' \cup S'$ has the property that $|C| \geq |\Gamma(S'' \cup S')| - |S'' \cup S'|$, which contradicts the maximality of S'. But this condition on all $S'' \subseteq S \setminus S'$ is precisely the hypothesis of Hall's Theorem applied to the subgraph induced by $S \setminus S'$ and $\Gamma(S) \setminus (\Gamma(S') \cup C)$, so we can conclude that there is a perfect matching from $S \setminus S'$ into $\Gamma(S) \setminus (\Gamma(S') \cup C)$ (in the sense that every element on the left has a unique element on the right; there may be unmatched elements on the right).

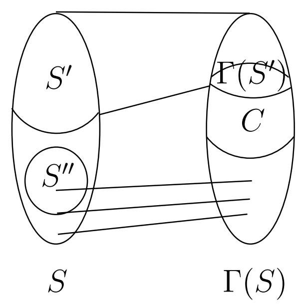

Figure 2: There is a matching from $S \setminus S'$ to $\Gamma(S) \setminus (\Gamma(S') \cup C)$

Now since $S' \neq S$ it follows by minimality of S that there exists an assignment to the variables of S' and C such that all clauses in S' are satisfied but C is not. Furthermore, we can extend the assignment such that all of $S \setminus S'$ are also satisfied because of the matching (with every clause we can associate a unique variable which hasn't been set yet). This contradicts the fact that we can derive C from S and we are done. $\square$

1.2 Application to the Pigeon Hole Principle

For our purposes, the pigeon hole principle $\phi = PHP_n^m$ will be a CNF that expresses the existence of a one to one mapping from m pigeons to n holes (which is unsatisfiable when $m > n$). Two types of clauses comprise ϕ: pigeon clauses and hole clauses. Each pigeon clause expresses that the pigeon is assigned to at least one hole, and each hole clause says that for some pair of pigeons and some hole, at least one of them is not assigned to that hole. We use variables $x_{i,j}$ where $1 \leq i \leq m$, $1 \leq j \leq n$ and $x_{i,j} = 1$ if pigeon i is assigned to hole j. The pigeon clause for pigeon i is simply $\vee_{j=1}^{n} x_{i,j}$, and the hole clause for hole j and pigeons $i \neq i'$ is $\wedge_{i<i'} (\overline{x_{i,j}} \vee \overline{x_{i',j}})$.

We will use the strong pigeon hole principle where $m = n+1$. We would like to apply Theorem 1 to this situation, but there are a couple of complications. First of all, the pigeon clauses involve n

variables each so we have an n-CNF, and it turns out that $w(\phi) = n$. Also, the number of variables is $mn > n^2$, so this is a problem, too. So currently, our bound only tells us that the proof length is at least constant, even if we could get the number of variables to be zero!

We are going to restrict the number of holes in which every pigeon can be placed. We consider the bipartite graph $G = (L, R, E)$ where L is the set of pigeons, R is the set of holes, and for every pigeon, we explicitly specify the holes in which that pigeon can be placed. We will take this graph to be an expander with constant left degree d. We denote this variant of the pigeon hole principle as PHP_G. The hole clauses are the same as before, but the pigeons are restricted to d choices. Now we have a d-CNF and the number of variables is just dm. It is only easier to derive a contradiction with these constraints, so

$$\ell(PHP_G) \leq \ell(PHP_{K_{m,n}}) = \ell(PHP_n^m).$$

We want Theorem 2 to give us a bound on $w(\phi)$, but G_ϕ is not expanding. To see this, consider all clauses containing $x_{i,j}$ of the form $\overline{x_{i,j}} \vee \overline{x_{i',j}}$. There are $m-1$ such hole clauses, and these are left vertices of G_ϕ. But only m variables are involved, so the neighbor set of this subset of size $m-1$ is of size m, and we don't have an expansion.

Since the hole clauses are not expanding, we will take them for granted. That is, we now look at the minimum number of pigeon clauses in ϕ such that these pigeon clauses together with all of the hole clauses are enough to derive C. We let μ denote this, so working in G, we write

$$\mu(C) = \min\{|S| : S \subseteq L \text{ and pigeon clauses in } S \text{ together with all hole clauses imply } C\}.$$

Lemma 2. *Let C be a clause and $S \subseteq L$ be minimal such that the pigeon clauses in S together with all hole clauses imply C. If G is (K, c)-expanding with degree d and $|S| \leq K$ then $|C| \geq (2c-d)|S|$.*

Proof. Let $U \subseteq \Gamma(S)$ denote the unique neighbors of S. Then similar to what we have seen in earlier arguments, $|U| \geq (2c - d)|S|$. Now for each hole $j \in U$, we claim that $x_{i,j}$ is in C where i the unique neighbor of j in S. To see this, suppose otherwise. Since S is minimal, we can take $S' = S \setminus \{i\} \subset S$ and there must be an assignment which satisfies S' and all of the hole clauses but doesn't satisfy C. Further we can assume that this assignment has all $x_{i',j}$ unset for $i' \neq i$. Thus since j is a unique neighbor of S, we can set $x_{i,j}$ to 1, and we know that all of S is satisfied, all the hole clauses are satisfied (we don't violate any hole clause by setting $x_{i,j}$ to 1) but if $x_{i,j}$ is not involved in C then C remains false. This contradiction establishes that all of U is in C, so $|C| \geq |U| \geq (2c - d)|S|$. $\square$

Now we just argue that any refutation of the pigeon hole principle must contain a clause C for which $\mu(C)$ is just under the threshold for expansion, as this implies that the corresponding line in the proof is wide. We need at least $n+1$ pigeon clauses to derive a contradiction i.e. $\mu(\emptyset) = n+1$. In this case we can use lossless expanders to realize $K = \Omega(n)$ and $c \geq \frac{3}{4}d$. This measure μ is subadditive, so in every refutation there has to be some clause C for which $\frac{K}{2} \leq \mu(C) < K$, thus $w(\phi) = \Omega(n)$, and we plug in values to get $\ell(\phi) = 2^{\Omega(n)}$.

2 Tseitin Tautologies

Note that in the above result that $2^{\Omega(n)} \leq \ell(PHP_n^{n+1})$ we used a quadratic number of variables (in n). So if, say, w is the number of variables used, we would have a lower bound of $2^{\Omega(\sqrt{w})}$ and we might hope to do better. Tseitin tautologies allow us to get bounds of $2^{\Omega(w)}$.

Tseitin tautologies use a graph G with $0-1$ variables assigned to the vertices of the graph. The formulae themselves express that there exists a $0-1$ assignment to the edges of the graph such that at every vertex the parity of the incoming edges is equal to the assignment at that vertex. This is only possible exactly if the weight of the assignment to the vertices is even. Thus, if it is odd, we have a contradiction, and we can look for a minimal length refutation for that contradiction. But if G is an expander, we can apply modifications of our previous ideas to show that the width is at least linear in the number of vertices so we get a linear exponential lower bound on the length in terms of the number of variables (since there are few edges in an expander). The difficulty is that the conditions are not clauses, so these need to be translated into CNF conditions. This can be accomplished directly or through auxiliary variables. If we look at G_ϕ and we want to compute the unique neighbors for some subset S, it turns out that these are exactly the edges between S and $\overline{S}$ in the original graph, so we can use the edge expansion to get a lower bound.