Math 267a - Propositional Proof Complexity

Lecture #9: 13 February 2002

Lecturer: Sam Buss

Scribe Notes by: Nathan Segerlind

1 Last Time

In this lecture, we prove exponential an lower bound on the sizes of resolution refutations of PHP_n^{n+1}. We also discuss recent results on the size needed to prove certain formulations of circuit lower bounds in resolution.

2 A Size Lower Bound for Resolution Refutations of PHP_n^{n+1}

The main result of this lecture is the proof that resolution refutations of PHP_n^{n+1} require size $2^{\Omega(n)}$. We show that clauses of high width are likely to be satisfied by a random restriction selected according to the distribution given in lecture 8. These restrictions transform the refutation into a refutation of a slightly smaller instance of the pigeonhole principle, and by the results of lecture 8, this new refutation must have either large width or large size. Because the restricted refutation has small width, it must have large size. Therefore, the original refutation must also have large size.

Recall that the width of a clause is the number of variables appearing in the clause, and the width of a resolution refutation is the maximum width of a clause in the refutation. We also assume that in a resolution refutation, there are no clauses that contain both a variable and its negation.

First, we show that clauses of high width must have many pigeons that appear in many literals.

Definition Let $s > 0$ be given. Let C be a clause. Let $i \in [n]$ be a pigeon. We say that i is an s-heavy pigeon of C if $|\{j \in [n] | X_{i,j} \in C \vee \neg X_{i,j} \in C\}| \geq s$.

Lemma 1 *Let n be an integer strictly greater than 1. For any clause C and any $\gamma > 0$, if C has width at least γn^2, then C contains at least $\frac{\gamma n}{2}$ many $\frac{\gamma n}{2}$-heavy pigeons.*

Proof Let h be the number of $\frac{\gamma n}{2}$-heavy pigeons in C.

First, we show that $h \geq 1$. Because each pigeon that is not $\frac{\gamma n}{2}$-heavy can contribute at most $\frac{\gamma n}{2}$ literals to C, if every pigeon were not $\frac{\gamma n}{2}$-heavy, then there would be at most $(n+1)\frac{\gamma n}{2} = \frac{\gamma n^2}{2} + \frac{\gamma n}{2}$ many literals in C. Because $n > 1$, this is quantity is less than $\gamma n^2/2$ and we would have a contradiction to the fact C has width at least γn^2.

Moreover, each $\frac{\gamma n}{2}$-heavy pigeon can contribute at most n literals to C, so we have the following inequalities.

$$\gamma n^2 \leq (n+1-h)\frac{\gamma n}{2} + hn$$

$$\gamma n^2 \leq \frac{\gamma n^2}{2} + hn$$

$$\frac{\gamma n^2}{2} \leq hn$$

$$\frac{\gamma n}{2} \leq h$$

Recall the definition on partial assignments given in lecture 8: for a fixed parameter $\beta \in (0,1)$, we choose to match each pigeon from $[n]$ with independent probability $1-\beta$. Then, we uniformly choose a matching between the selected pigeons and the holes. In the sequel of this lecture, this distribution will be referred to as $\mathcal{R}_{n,\beta}$.

We now show that a clause that has many heavy pigeons is very likely to be satisfied by a restriction chosen according to $\mathcal{R}_{n,\beta}$.

Lemma 2 *If C is a clause that contains t many αn-heavy pigeons, then*

$$Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[C\restriction_\rho \neq 1\right] \leq (1-(1-\beta)\alpha/2)^{t-1}$$

Proof Let F be the set of pigeons from $[1,n]$ that are αn-heavy in C. Notice that $|F| \geq t-1$. For each $i \in F$, let H_i be the set of holes so that the variable $X_{i,j}$ occurs in C. For each $i \in F$, $j \in H_i$ notice that exactly one of $X_{i,j}, \neg X_{i,j}$ occurs in C: let $l_{i,j}$ be this literal. In this notation, C can be written as $\bigvee_{i\in F}\bigvee_{j\in H_i} l_{i,j} \vee C'$. where C' is a clause that contains only literals whose pigeons are not in F. Furthermore, we may assume without loss of generality that F consists of the pigeons 1 through $|F|$ because permuting the first n pigeons does not change the distribution $\mathcal{R}_{n,p}$.

For each $i \in F$, let E_i be the event that $\left(\bigvee_{\substack{k\in F\\ k<i}} \bigvee_{j\in H_k} l_{k,j}\right)\restriction_\rho \neq 1$.

Now we bound, for each $i \in F$, the probability that, conditioned on E_i, $\rho \in \mathcal{R}_{n,\beta}$ satisfies $\bigvee_{j\in H_i} l_{i,j}$.

First of all, if $\bigvee_{j\in H_i} l_{i,j}$ contains two or more negative literals, then ρ satisfies $\bigvee_{j\in H_i} l_{i,j}$ if and only if ρ matches the pigeon i to some hole, and this occurs with probability $1-\beta$.

If $\bigvee_{j\in H_i} l_{i,j}$ contains no negative literals, then at worst the preceding elements of F were each matched to an element of H_i, and the chance of satisfying $\bigvee_{j\in H_i} l_{i,j}$ is at most $(1-\beta)\left(\frac{|H_i|-i+1}{n-i+1}\right)$. Because $|H_i| \geq \alpha n$ and $t \leq \alpha n/2$, we have that this probability exceeds $(1-\beta)\alpha/2$.

If $\bigvee_{j\in H_i} l_{i,j}$ contains exactly one negative literal, then $\bigvee_{j\in H_i} l_{i,j}$ is satisfied with the probability that ρ matches i to some hole besides the forbidden hole. At the very worst, ρ did not match any of the preceding pigeons of F to the forbidden hole, so the probability of satisfaction is at least $(1-\beta)(1-1/(n-i+1))$. This is equal to $(1-\beta)(n-i)/(n-i+1)$ which is at least $(1-\beta)\alpha/2$.

Therefore, for any $i \in F$, we have the following inequalities:

$$\mathrm{Pr}_{\rho\in\mathcal{R}_{n,\beta}}\left[(\bigvee_{j\in H_i} l_{i,j})\restriction_\rho = 1 \mid E_i\right] \geq (1-\beta)\alpha/2$$

$$\Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[(\bigvee_{j\in H_i} l_{i,j})\restriction_\rho \neq 1 \mid E_i\right] \leq 1-(1-\beta)\alpha/2$$

Examination of the conditional probabilities of satisfying the literals involved with each heavy pigeon reveals the following.

$$\Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[C\restriction_\rho\neq 1\right] \leq \Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[(\bigvee_{i\in F}\bigvee_{j\in H_i} l_{i,j})\restriction_\rho\neq 1\right] = \prod_{i\in F}\Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[(\bigvee_{j\in H_i} l_{i,j})\restriction_\rho\neq 1 \mid E_i\right]$$

$$\leq \prod_{i\in F}(1-(1-\beta)\alpha/2) = (1-(1-\beta)\alpha/2)^{t-1}$$

We now show that a random restriction will almost certainly satisfy every wide clause of a small proof.

Lemma 3 *Let $\epsilon,\beta\in(0,1)$ be a constants so that $\epsilon < -(\beta^2/64)\log_2(1-(1-\beta)\beta^2/128)$. For n sufficiently large, if R is resolution refutation of PHP_n^{n+1} of size at most $2^{\epsilon n}$, then the following inequality holds.*

$$Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[w(R\restriction_\rho)\geq\beta^2n^2/32\right] = o(1)$$

Proof For each clause C of R that has width at least $\beta^2n^2/32$, by lemma 1, C contains at least $\beta^2n/64$ many $\beta^2n/64$-heavy pigeons. Therefore, by lemma 2, each clause C of R of width at least $\beta^2n^2/32$ is not satisfied with probability at most $(1-(1-\beta)\beta^2/128)^{(\beta^2n/64)-1}$. Therefore, by an application of the union bound, we have the following inequality.

$$\Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[w(R\restriction_\rho)\geq\beta^2n^2/32\right] \leq 2^{\epsilon n}(1-(1-\beta)\beta^2/128)^{(\beta^2n/64)-1} = 2^{\epsilon n}2^{((\beta^2n/64)-1)\log_2(1-(1-\beta)\beta^2/128)}$$

$$= 2^{n(\epsilon+((\beta^2/64)-1/n)\log_2(1-(1-\beta)\beta^2/128))}$$

Because ϵ and β are constants with $\epsilon < -(\beta^2/64)\log_2(1-(1-\beta)\beta^2/128)$, this probability is $o(1)$ as n tends to infinity.

We now combine these lemmas with Danchev's theorem to prove the size lower bounds for resolution refutations of PHP_n^{n+1}.

Theorem 4 *There exists an $\epsilon>0$ so that every resolution refutation of PHP_n^{n+1} has size at least $2^{\epsilon n}$.*

Proof

We will show that for constants $\epsilon,\beta\in(0,1)$ with $\epsilon<\beta/8$ and $\epsilon < -(\beta^2/64)\log_2(1-(1-\beta)\beta^2/128)$ there is no resolution refutation of PHP_n^{n+1} of size $2^{\epsilon n}$. There are constants satisfying these bounds because for any $\beta\in(0,1)$, $-\log_2\left(1-(1-\beta)\beta^2/128\right)>0$ and therefore we can take ϵ to be the minimum of $\beta/8$ and $-(\beta^2/64)\log_2(1-(1-\beta)\beta^2/128)$, and we will have that $\epsilon\in(0,1)$.

For the sake of contradiction, assume that R is a resolution refutation of PHP_n^{n+1} of size less than $2^{\epsilon n}$.

Let $\rho\in\mathcal{R}_{n,\beta}$ be given. Let M be the set of pigeons matched by ρ, and let $m=|M|$. Notice that for the set of clauses PHP_n^{n+1}, the set of clauses $PHP_n^{n+1}\restriction_\rho$ is is just a renaming of PHP_{n-m}^{n-m+1}.

Because the number of pigeons matched by $\rho \in \mathcal{R}_{n,\beta}$ is distributed according to a binomial distribution, the expected number of pigeons matched by ρ is $(1-\beta)n$. By the central limit theorem as n tends to infinity, the probability that the number of matched pigeons exceeds $(1-\beta)n$ tends to $1/2$. Therefore, for sufficiently large n, the probability that ρ leaves at least $\beta n+1$ many pigeons unmatched is at least $1/4$.

Lemma 3 tells us that $\Pr_{\rho\in\mathcal{R}_{n,\beta}}\left[w(R\restriction_\rho) \geq \beta^2 n^2/32\right]$ is $o(1)$

Therefore, for sufficiently large n, we may choose $\rho \in \mathcal{R}_{n,\beta}$ so that $w(R\restriction_\rho) < \beta^2 n^2/32$ and ρ leaves at least βn many pigeons unmatched.

Because the restriction of a resolution refutation is a resolution refutation (see lecture 8), $R\restriction_\rho$ is a resolution refutation of $PHP^{n+1}_{n}\restriction_\rho$. Therefore, up to renaming the variables, $R\restriction_\rho$ is a resolution refutation of $PHP^{\beta n+1}_{\beta n}$ with each clause of width strictly less than $\beta^2 n^2/32$ and of size at most $2^{\epsilon n}$. By Danchev's theorem, every resolution refutation of $PHP^{\beta n+1}_{\beta n}$ requires width at least $\beta n^2/32$ or size at least $2^{\beta n/8}$, but because $\epsilon < \beta/8$, we have obtained a contradiction.

3 Lower Bounds for Resolution Proofs of Circuit Lower Bounds

Recently, Razborov has shown that certain formulations of circuit lower bounds require exponential size refutations in resolution. Given the truth-table of a boolean function, $f_n : \{0,1\}^n \to \{0,1\}$, and a a parameter $t \leq 2^n$, a CNF $Circuit_t(f_n)$ is constructed which is satisfiable if and only if f_n can be computed by a circuit of size t. If f_n is a function which is not computed by any circuit of size $\leq t$, then this formula is unsatisfiable. The formula is constructed in a brute force way, with $\mathrm{O}(t)$ many variables encoding the circuit, and with $\mathrm{O}(t2^n)$ many variables representing the value of each gate on each assignment to the inputs. The clauses state that the output of each gate is consistent with the output of its inputs.

Razborov's result shows that for any function f_n and size t, $Circuit_t(f_n)$ has no resolution refutation of size less than $2^{\Omega(t/n^3)}$. The proof works by reducing the onto-functional weak pigeonhole principle to the principle $Circuit_t(f_n)$.