Math 267a - Propositional Proof Complexity

Lecture #8: 11 February 2002

Lecturer: Sam Buss

Scribe Notes by: Bryant Forsgren

1 Last Time

In Lecture 7 we proved the "strong" Pigeon Hole Principle (PHP_n^{n+1}) by giving a resolution refutation of its negation. The refutation was tree-like and had size $2^{O(n \log n)}$. We claim without proof that a non-tree-like refutation of size $2^{O(n)}$ exists. Today our goal is to prove exponential lower bounds ($2^{\Omega(n)}$) on the size of any refutation of the $\neg PHP_n^{n+1}$ clauses.

2 Views of Resolution Refutations

2.1 Resolution Proof as a Decision dag

Any resolution proof starts with a set of initial clauses $C_1, C_2, \ldots C_k$, and ends with the empty clause $\emptyset$. Clearly all of the variables need to be eliminated to reach this conclusion. For example, the variable x can be eliminated from two clauses of the form $D \cup \{x\}$ and $E \cup \{\overline{x}\}$ to derive $D \cup E$. In particular, there exists some variable y such that the empty clause $\emptyset$ is derived from $\{y\}$ and $\{\overline{y}\}$. We can view this pictorially as follows:

$$
\begin{array}{c}
C_1 \qquad \ldots \qquad C_k \\[1em]
\ddots \quad \vdots \quad \iddots \\[0.5em]
\dfrac{D \cup \{x\} \quad E \cup \{\overline{x}\}}{D \cup E} \\[1em]
\ddots \quad \vdots \quad \iddots \\[0.5em]
\dfrac{\{y\} \ \{\overline{y}\}}{\emptyset}
\end{array}
$$

Given any such refutation and a truth assignment τ, it is clear that there exists an initial clause C_i such that τ falsifies C_i. We wish to use the refutation as a decision dag to find such a C_i. We start with $\emptyset$, and work toward the initial clauses, making a decision at each clause we encounter. Suppose we are at the clause $D \cup E$ in the diagram. We do the following:

If $\tau(x) = \top$
 go to $E \cup \{\overline{x}\}$
Else
 go to $D \cup \{x\}$

Our invariant is the following: we are always at a clause C which is falsified by τ. Furthermore, we are guaranteed to eventually reach one of the initial clauses C_i. By our easily verified invariant, C_i is an initial clause which is falsified by τ.

2.2 Resolution Proof as Guiding a Game

The game is played between a Prover and an Adversary . The Prover wishes to find a clause that is false, and the adversary wishes to prevent this from happening. A round of the game is played as follows:

1. Prover asks a query "y?".
2. Adversary answers *True* ($\top$) or *False* ($\bot$).
3. Prover remembers the answer (but is allowed to forget later).

Claim There is an exact correspondence between resolution proofs and winning strategies for the Prover.

This is true because at any particular point in the game, the Prover and Adversary are at some clause in the refutation. This clause contains exactly those literals $\overline{y}$ such that the Prover knows y holds.

3 Exponential Lower Bounds on Refutation Proofs of the Pigeon Hole Principle

3.1 The "weak" Pigeon Hole Principle

We now define the "weak" Pigeon Hole Principle. Intuitively, it states that

$$\forall m > n \nexists f : [m] \overset{1-1}{\to} [n]$$

over the natural numbers.

Definition Let $m > n$; $m, n \in \mathbb{N}$

$$PHP_n^m : \bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} P_{i,j} \to \bigvee_{i=1}^{m-1} \bigvee_{j=i+1}^{m} \bigvee_{k=1}^{n} (P_{i,k} \wedge P_{j,k})$$

The clauses of $\neg PHP_n^m$ are as follows:

$$\{P_{i,1}, \ldots, P_{i,n}\} \quad \text{for } i = 1, \ldots, m$$

$$\{\overline{P_{i,k}}, \overline{P_{j,k}}\} \qquad \text{for } 1 \leq i < j \leq m, 1 \leq k \leq n$$

Note that it is often easier to prove PHP_n^m for $m >> n$, than for $m = n + 1$.

Definition The *width* of a refutation R is $\max\{|C| : C \text{ is a clause in } R\}$.

Note that the refutation of $\neg PHP_n^{n+1}$ from the previous lecture had width $O(n)$.

Theorem 1 (Dantchev 2002) *Let $m > n >> 0$. Then any resolution refutation of $\neg PHP_n^m$ of width $\leq \frac{n^2}{32}$ has size $\geq 2^{\frac{n}{8}}$ (where size is understood to mean the number of clauses in the proof).*

Proof Suppose we have a refutation R of width $\leq \frac{n^2}{32}$ and size $< 2^{\frac{n}{8}}$, for "large enough" n. Let $H_1 = \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$, $H_2 = \{\lfloor \frac{n}{2} \rfloor + 1, \ldots, n\}$. Now fix a π which maps each pigeon i to either H_1 or H_2. Denote this by $i \in H_{\pi(i)}$.

Definition Pigeon i is *busy* if either:

(1) The Prover knows $P_{i,j} = \top$ for some $j \in H_{\pi(i)}$. (call this case busy$_1$)

(2) The Prover knows $P_{i,j} = \bot$ for $\geq \frac{n}{4}$ many $j \in H_{\pi(i)}$. (call this case busy$_2$)

As described above, the Prover views R as a decision dag and chooses the queries accordingly. When the Prover queries a variable $P_{i,j}$, the Adversary responds as follows:

(1) If $j \notin H_{\pi(i)}$, Adversary answers "$\bot$".

(2) If $j \in H_{\pi(i)}$ and i is not busy, Adversary answers "$\bot$".

(3) Otherwise ($j \in H_{\pi(i)}$ and i is busy), the Adversary chooses an unassigned hole $k \in H_{\pi(i)}$ for which $P_{i,k}$ is not known and assigns pigeon i to that hole. The Adversary then answers accordingly, and remembers this assignment until (if ever) pigeon i becomes unbusy.

Claim The Adversary can keep going as long as there are $< \frac{n}{4}$ busy pigeons.

The game stops when there are $\geq \frac{n}{4}$ busy pigeons at some clause C_π. By assumption, C_π has width $\leq \frac{n^2}{32}$ and has $\frac{n}{4}$ busy pigeons.

Notice that each pigeon of type busy$_2$ contributes $\frac{n}{4}$ literals into C_π. Suppose C_π has $> \frac{n}{8}$ pigeons which are busy$_2$. Then C_π has width $> \frac{n^2}{32}$ which is a contradiction. Therefore, at most $\frac{n}{8}$ of the $\frac{n}{4}$ busy pigeons can be busy$_2$.

So at least $\frac{n}{8}$ i's in C_π are of type busy$_1$. In other words, for at least $\frac{n}{8}$ i's there exists a $j \in H_{\pi(i)}$ such that $\overline{P_{i,j}} \in C_\pi$. We wish to address the following question: "For how many π's can *this* clause be C_π?" But this is only possible for $\leq 2^{(m-\frac{n}{8})}$ many π's. So there are $\geq 2^{\frac{n}{8}}$ distinct C_π's, contradicting the assumption that size $< 2^{\frac{n}{8}}$.

3.2 The "strong" Pigeon Hole Principle

Definition A *restriction* is a partial truth assignment that maps some variables to $\{\top, \bot\}$, leaving other variables unassigned ($*$). A restriction can be expressed in the following way:

$$\rho(x) = \begin{cases} \top & \text{if } Cond_A(x) \\ \bot & \text{if } Cond_B(x) \\ * & \text{if } Cond_C(x) \end{cases}$$

Where each $Cond_i$ is an arbitrary condition.

Definition If Σ is a set of clauses, $\Sigma_{\restriction\rho}$ is the set of clauses constructed as follows:

> **Foreach** $C = \{x_1, \ldots, x_k\} \in \Sigma$
>   **If** $\exists i$ such that $\rho(x_i) = \top$
>   discard C
>   **Else**
>   put $\{x_i : \rho(x_i) = *\}$ into $\Sigma_{\restriction\rho}$

Theorem 2 *If R is a refutation of Σ, then $R_{\restriction\rho}$ is a refutation of $\Sigma_{\restriction\rho}$ (to be precise, it is a resolution and subsumption refutation).*

What this means is that size and width do not increase under restrictions.

Theorem 3 *For any $\alpha \in (0, \frac{n}{8})$, any refutation of $\Sigma = \neg PHP_n^{n+1}$ has size $\geq 2^{\epsilon n}$ where $\epsilon = \frac{1}{8} - \alpha$ (for large enough n).*

Proof Assume there is a refutation R of size $< 2^{\epsilon n}$. We construct a restriction ρ as follows:

> Fix $\beta \in (0, 1)$
>   (note that α and β satisfy this relationship: $\beta = 1 - 8\alpha$)
> **Foreach** pigeon i
>   pick i with probability $1 - \beta$
>   **If** pigeon i is picked
>   map it to a unique, randomly selected hole j_i
>   set $\rho(P_{i,j_i}) = \top$
>   **Foreach** $k \neq j_i$
>   set $\rho(P_{i,k}) = \bot$
>   **Foreach** $k \neq i$
>   set $\rho(P_{k,j_i}) = \bot$

We apply this restriction to Σ, yielding $\Sigma_{\restriction\rho}$. The expected number of holes in $\Sigma_{\restriction\rho}$ is

$$n - (1 - \beta)(n + 1) = \beta n - 1 + \beta$$

So with some fixed non-zero probability, the number of remaining holes is at least βn. We also apply ρ to the refutation R which yields $R_{\restriction\rho}$, a refutation of $\neg PHP_{\lceil\beta n\rceil}^{\lceil\beta n\rceil+1}$ of size $\leq 2^{\epsilon n}$.

Claim $R_{\restriction\rho}$ has width $\leq \frac{(\beta n)^2}{32}$ with probability approaching 1 as $n \to \infty$. This will be a contradiction, provided $\epsilon > \frac{\beta}{8}$.

This last claim will be proved next time, finishing the proof of Theorem 3. The idea is that any clause in R will get mapped to $\top$ by ρ and vanish from $R_{\restriction\rho}$.