Math 267a - Propositional Proof Complexity

Lecture #5: 29 January 2002

Lecturer: Sam Buss

Scribe Notes by: Tamsen Dunn

1 The Pigeon Hole Principle

Last time we finished our introduction to Frege Proof Systems. In this lecture we will give a propositional formulation of and a proof of the Pigeon Hole Principle. Its an interesting side note that this theorem was considered self evident until it was brought under the scrutiny of discrete mathematicians. Now the Pigeon Hole Principle is considered quite subtle. We will begin by analyzing the familiar form of the theorem.

1.1 The Familiar Form of the Pigeon Hole Principle

Theorem 1 (Pigeon Hole Principle A)

$$PHP_n^{n+1} : \forall n \in N \neg\exists f : \{1, 2, ..., n+1\} \to \{1, 2, ..., n\}$$

The above formulation of the Pigeon Hole Principle is sometimes taken in and of itself as the definition of n being finite.

1.2 The Pigeon Hole Principle by Induction

Now, we want to write the Pigeon Hole Principle as a family of propositional tautologies. Fix $n \geq 1$ and let our variables be $P_{i,j}$, where $1 \leq i \leq n+1$ and $1 \leq j \leq n$ and $P_{i,j}$ means $f(i) = j$. In this way, we no longer have a set of ordered pairs but a set of graphs.

Theorem 2 (Pigeon Hole Principle B)

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

This ought to be a tautology. Let's check:

Example $[PHP_1^2{:}]$ $(P_{1,1} \vee P_{1,2}) \to (P_{1,1} \vee P_{2,1}\ )$

So that works. Now for $n = 2$.

Example $[PHP_2^3$:]

Left hand side: $(P_{1,1} \vee P_{1,2}) \wedge (P_{2,1} \vee P_{2,2}) \wedge (P_{3,1} \vee P_{3,2})$
should imply
Right hand side: $(P_{1,1} \wedge P_{2,1}) \vee (P_{1,2} \wedge P_{2,2}) \vee (P_{1,1} \wedge P_{3,1}) \vee (P_{1,2} \wedge P_{3,2}) \vee (P_{2,1} \wedge P_{3,1}) \vee (P_{2,2} \wedge P_{3,2})$
and it does.

In the above formulation, the Pigeon Hole Principle has been reduced to a family of tautologies, each polynomial in size.

Proof Complexity On the right hand side we see that there are n^3 ways to select the mapping, so these formulas have $O(n^3)$ symbols.

Cook and Reckhow were the first to show that the Pigeon Hole Principle could be given a polynomial-size $e\mathcal{F}$-proof.

Idea of Proof: Given a mapping $f : [n+1] \to [n]$ where $[n]$ and $[n+1]$ are sets such that $[n] = \{1, 2, ..., n\}$, we want to show that this mapping causes a contradiction.

Define $f^n = f$ and

$$f^m(i) = \begin{cases} f^{m+1}(i) & \text{when } f^{m+1}(i) < m+1 \\ f^{m+1}(m+2) & \text{otherwise} \end{cases}$$

So, given an f^{m+1} we want to find an f^m. Suppose the mapping is as follows:

$$\begin{array}{ccc} \multicolumn{3}{c}{domain - - - - - range} \\ m+2 & & --- \\ m+1 & \searrow & m+1 \\ m & & m \\ \vdots & & \vdots \\ 2 & \nearrow & 2 \\ 1 & & 1 \end{array}$$

The idea of this proof is to successively use induction to prove $f^m : [m+1] \to [m]$ is a one-to-one mapping. At each inductive step drop a pair, such as $m+2$ from the domain and $m+1$ from the range, and reconnect the respective arrows to which ever empty slots are available.

Assuming $f^m + 1 : [m+2] \to [m+1]$, we use the inductive claims that

(1) f^{m+1} is one-to-one $\to$ f^m is one-to-one, and

(2) $f^{m+1} : [m+1] \to [m]$

The induction will finally stop at the bottom, at $m = 1$ where

$$f^1 : [2] \to [1]$$

It is reasonable to claim this is impossible, a contradiction by definition.

Now, let's translate this into an $e\mathcal{F}$-proof:

1.3 $e\mathcal{F}$-Proof of the Pigeon Hole Principle

Proof

Idea of Proof: We begin by presuming the hypothesis $\neg PHP_n^{n+1}$. Then we derive some instance of $\neg PHP_1^2$ which can be disproved, and allow that to negate the hypothesis.

First introduce some new variables: For $\neg PHP_n^{n+1}$, we need to have at least the set of $\{P_{i,j}\}$ variables.

Define $\neg PHP_m^{m+1}(q^m)$ to have new variables $q_{i,j}^m$ for $m = n, ..., 2, 1$. Let $q_{i,j}^n \leftrightarrow P_{i,j}$. Now the extension rule is used to introduce $q_{i,j}^m$ by

$$q_{i,j}^m \leftrightarrow (q_{i,j}^{m+1} \vee (q_{i,m+1}^{m+1} \wedge q_{m+2,j}^{m+1}))$$

where $1 \leq i \leq m+1$, and $1 \leq j \leq m$. Since each q^m is so defined by the previous q^{m+1}, they are allowed by the extension rule.

Now we claim that $e\mathcal{F}$ has polynomial size proofs of $\neg PHP_{m+1}^{m+2} \rightarrow \neg PHP_m^{m+1}$. Proving this claim below is equivalent to proving the main theorem.

$$\neg PHP_{m+1}^{m+2}(q^{m+1}) \rightarrow \neg PHP_m^{m+1}(q^m)$$

To finish, we need to give an $e\mathcal{F}$-proof of the conjuncts of $\neg PHP_m^{m+1}(q^m)$ from the conjuncts of $\neg PHP_{m+1}^{m+2}(q^{m+1})$. This is basically a brute-force case analysis. The idea of the case analysis comes back to the picture we drew earlier. Its simply not possible to map two (or more) elements of the domain to a single slot in the range. Any time it did would violate one-to-oneness. The full proof can be found in Cook and Reckhow, JSL 1979.

Proof Complexity All formulas given in this $e\mathcal{F}$-proof are of $O(n^3)$ since in the PHP there are n^3 steps for that many conjuncts. We step down from n, so that gives us $O(n^4)$ lines, and each line had $O(n^3)$ symbols.

Suppose we were instead thinking of an ordinary $\mathcal{F}$-proof. Straightforward conversion fails with exponential blow up. We have to re-express every $q_{i,j}$ in terms of its original variables, thus eliminating all the extension variables from $m = n$ to $m = 1$. That means we would have roughly 3 times as many symbols. For example, q^m uses three q^{m+1} 's, so by straightforward replacement substitution the formulas increase in size by a factor of 3^n.

For a different $\mathcal{F}$-proof which is polynomial in size, see Buss, JSL 1978. Buss's proof rests on a counting argument: "The idea behind the proof is that one can't [not have the PHP] because then one set would have more than the other."

We have very few examples of $e\mathcal{F}$ and $\mathcal{F}$ size comparisons. However, we still tend to believe the separation is maintained from arguments made in circuit theory. We will come back to this.

2 Tree-Like versus Non-Tree-Like Proofs

Definition A $\mathcal{F}$ or $e\mathcal{F}$-proof is *tree-like* if each formula in the proof is used at most once as a hypothesis of an inference. Other proofs may be dag-like or sequence-like.

Theorem 3 (Krajíček) *Tree-like (extended) $\mathcal{F}$-proofs p-simulate ordinary (extended) $\mathcal{F}$-proofs.*

Intuitively, you might expect the transition to tree-like proofs would cause an an exponential blow up. But that is not the case.

Proof Given a sequence-like proof, $\phi_1, \phi_2, ..., \phi_n = \phi$ one wants to create a tree-like proof from $\psi_1, \psi_2, ..., \psi_n$ where $\psi_i = \bigwedge_{j=1}^{i} \phi_i$. We hope that if multiple formulas are necessary we can use conjunctions for it once and only once. Now, we claim that the sequence $\psi_1, \psi_2, ..., \psi_n$ can be "patched up" to be a tree-like proof. The patching is done by cases:

Case (1) : ϕ_i is an axiom.

Assume ψ_{i-1} has already been derived. We have the axiom ϕ_i. We can derive

$$\psi_{i-1} \to \phi_i \to (\psi_{i-1} \wedge \phi_i)$$

as an instance of $A \to B \to (A \wedge B)$. So MP twice gave us

$$\psi_{i-1} \wedge \phi_i$$

which is equivalent to ψ_i. And case (1) is proven.

Case (2) :

ϕ_i is inferred from ϕ_j and ϕ_k by MP. ϕ_k is $(\phi_j \to \phi_i)$. By assuming we have a proof of ψ_{i-1}, we can complete the rest of the proof by a straightforward unwinding of conjunctions. See the example below to see how this will work:

Example The following are tautologies: $A \wedge B \to A$ and $A \wedge B \to B$, $(A \to B) \wedge (B \to C) \to (A \to B)$. Given an instance

$$(\alpha \wedge \beta) \wedge \gamma \to (\alpha \wedge \beta) \to \alpha.$$

$$(\alpha \wedge \beta) \wedge \gamma \to (\alpha \wedge \beta) \to ((\alpha \wedge \beta) \to \alpha) \to ((\alpha \wedge \beta) \wedge \gamma) \to \alpha.$$

Using MP twice, for two conjuncts we have

$$((\alpha \wedge \beta) \wedge \gamma) \to \alpha.$$

Substituting the above equations into our proof, we now have the desired

$$\psi_{i-1} \to \phi_j$$

and

$$\psi_{i-1} \to \phi_k$$

Each of the above is tree like. Now, using a substitution instance of the following tautology:

$$A \to (A \to B) \to (A \to (B \to C)) \to (A \wedge C)$$

we can derive from the 3 MP's that

$$\psi_{i-1} \to (\psi_{i-1} \to \phi_j) \to (\phi_{j-1} \to \phi_k) \to (\psi_{i-1} \wedge \phi_i)$$

We are done with case (2) because

$$\psi_{i-1} \wedge \phi = \psi_i$$

Therefore, in either case, each ψ_i can be created for the tree-like proof. That concludes our proof and this lecture.