Math 267a - Propositional Proof Complexity

Lecture #6: 4 February 2002

Lecturer: Sam Buss

Scribe Notes by: Rosalie Iemhoff

1 Substitution Frege systems

In a previous lecture we encountered certain proof systems for which it is *conjectured* that they are stronger than Frege systems (in the sense that Frege systems do not p-simulate them). These were the extended Frege systems. Here we will define other such proof systems: the substitution Frege systems. We will see that these systems are as strong as extended Frege systems; they p-simulate extended Frege systems and vice versa. As in the case of extended Frege systems, it is an open question whether Frege systems p-simulate substitution Frege systems or not.

Definition A *substitution Frege system*, $s\mathcal{F}$, is a Frege system augmented with a substitution rule $A/A\sigma$. Thus a proof in a substitution Frege system $s\mathcal{F}$ is a sequence $\varphi_1, \ldots, \varphi_n$, where every φ_i is an axiom of $\mathcal{F}$, or inferred from earlier φ_j by a rule of $\mathcal{F}$, or $\varphi_i = \varphi_j\sigma$, for some $j < i$ and some substitution σ.

Note that substitution Frege systems are indeed complete proof systems; it is not difficult to see that they are sound and complete (the substitution rule is clearly sound, and completeness follows from the fact that Frege systems are complete). Note however that they are not implicationally sound. This is not a problem since implicational soundness is not required for a proof system.

Theorem 1 *$s\mathcal{F}$-systems and $e\mathcal{F}$-systems p-simulate each other.*

Proof We will only show that $s\mathcal{F}$-systems p-simulate $e\mathcal{F}$-systems, the other direction can be found in [4] or [3] (Lemma 4.5.5). For this proof we consider extended Frege systems of the second type, i.e. with an extension rule. Let $\varphi_1, \ldots, \varphi_n$ be a proof in an extended Frege system $e\mathcal{F}$ of size k. Thus $k = \mathcal{O}(n + |\varphi_n|)$. W.l.o.g. we can assume that the first m lines in the proof are extension rules and that the others are not: for $i \leq m$, $\varphi_i = z_i \leftrightarrow \chi_i(\bar{x}, z_1, \ldots, z_{i-1})$, i.e. φ_i is an instance of the extension rule, and for $i > m$, φ_i is not an instance of the extension rule. Clearly, we have

$$\varphi_1, \ldots, \varphi_m \vdash_{\mathcal{F}} \varphi_n.$$

Observe that this Frege proof has size at most k. By the Deduction Theorem (Lecture #2) we have

$$\vdash_{\mathcal{F}} \left(\bigwedge_{i=1}^{m}(z_i \leftrightarrow \chi_i)\right) \rightarrow \varphi_n, \tag{1}$$

where the proof has size polynomial in k. W.l.o.g. we associate the brackets in the big conjunction to the left. From (1) we get

$$\vdash_{\mathcal{F}} \left(\bigwedge_{i=1}^{m-1} (z_i \leftrightarrow \chi_i) \wedge (z_m \leftrightarrow \chi_m) \right) \rightarrow \varphi_n. \tag{2}$$

Note that the variable z_m only occurs at one place in the whole formula. Now we hit the formula in (2) with a substitution $\sigma(z_m) = \chi_m$ and obtain

$$\vdash_{\mathcal{F}} \left(\bigwedge_{i=1}^{m-1} (z_i \leftrightarrow \chi_i) \wedge (\chi_m \leftrightarrow \chi_m) \right) \rightarrow \varphi_n.$$

From this we get

$$\vdash_{\mathcal{F}} \left(\bigwedge_{i=1}^{m-1} (z_i \leftrightarrow \chi_i) \right) \rightarrow \varphi_n.$$

Then we repeat this procedure for $m-1$, then for $m-2$, etc., so that we finally end up with

$$\vdash_{\mathcal{F}} \varphi_n.$$

About the size of the proof: for (1) we have already observed that the proof is of size polynomial in k. From this it is easy to conclude that the other proofs have size polynomial in k as well.

It is interesting to ask whether one can restrict the substitutions in the substitution rule and still get systems that are as strong as $s\mathcal{F}$ systems. Renaming Frege systems are an example of this. A substitution is a *renaming substitution* if its range is contained in the set of propositional variables. A *renaming Frege system*, $r\mathcal{F}$, is a substitution Frege system for which in the substitution rule only renaming substitutions are allowed. A renaming substitutions σ replaces the variables in A by (possibly) other variables (hence the name renaming). At first sight renaming Frege systems may seem weaker than substitution Frege systems, but it turns out that both systems p-simulate each other (a proof can be found in [2]). Hence extended Frege systems and renaming Frege systems p-simulate each other as well.

One could try to restrict the substitutions that are allowed in the substitution rule even further than in renaming Frege systems. For example, one could require that the substitutions map variables only to variables that occur in the last line of the proof, or one could require that the renaming substitutions are injective. For these systems it is no longer known whether they are as strong as extended Frege systems or not.

A propositional proof systems that is considered stronger than extended Frege systems, is quantified propositional logic QBF. QBF is an extension of propositional logic by propositional quantifiers

$$\forall x \text{ (intended meaning } A(x/\top) \wedge A(x/\bot))$$

$$\exists x \text{ (intended meaning } A(x/\top) \vee A(x/\bot))$$

It is known that QBF p-simulates extended Frege systems [3]. It is conjectured that the converse does not hold, but this is open.

2 The best known lower bounds on proof lengths

In this section we will discuss the best known lower bounds on Frege and extended Frege proofs. For Frege proofs we have a linear lower bound on the number of lines and a quadratic lower bound on the size. Hence for extended Frege proofs we have a linear lower bound on the size of proofs. Since the best known upper bounds on Frege proofs are exponential, there is still a large gap between the lower bounds and the upper bounds. To prove the lower bounds we need some terminology.

Definition Given a Frege proof P, a formula A is called *active* in P if it occurs in P as a subformula in an inference that explicitly uses the principal connective of A. We tacitly assume here that there is no ambiguity as to what rule is applied in a certain inference; one can always label the rules to avoid ambiguity of this kind.

Example In the rule Modus Ponens

$$\frac{A \quad A \to B}{B}$$

the formula $A \to B$ is the only formula that is made active by this inference. The axiom $A \to (B \to A)$ makes the formulas $A \to (B \to A)$ and $(B \to A)$ active.

The intuition here is that in a proof the inactive formulas can be changed while the proof remains valid. This is the content of the next claim, of which we omit the proof.

Claim If A is not active in a proof P, then if A is everywhere replaced by B, the result is still a valid proof.

Claim Let c be the maximum number of connectives shown in any inference rule or axiom of a Frege system $\mathcal{F}$ (for $\mathcal{F}_0$, $c = 6$), and let $A_1, \ldots, A_k$ be all the distinct active formulas in an $\mathcal{F}$-proof P, then $|P| \geq \frac{1}{c}(\sum_{i=1}^{k} |A_i|)$.

Proof Observe that any inference activates at most c formulas, and that if a subformula of a formula is active, then so is the formula of which it is a subformula. Therefore, given a symbol in the proof P, it lies in at most c activated occurrences of $A_1, \ldots, A_k$. Moreover, every A_i is activated somewhere. This implies that $c \cdot |P| \geq \sum_{i=1}^{k} |A_i|$. Hence $|P| \geq \frac{1}{c}(\sum_{i=1}^{k} |A_i|)$.

Let φ_n be the formula

$$\bot \vee (\bot \vee (\ldots (\bot \vee \top) \ldots)$$

in which n $\bot$'s occur. $\top$ denotes "true": $\top = x \vee \neg x$. $\bot$ denotes "falsum": $\bot = x \wedge \neg x$ (sometimes these symbols are added to the language of propositional logic).

Claim In any proof of φ_n all the n subformulas of φ_n that are distinct from $\bot$ and $\top$ are active.

Proof If not, by Claim 2 we could replace such an inactive subformula by $\bot$ and obtain a valid formula as well. This cannot be, as such a formula would not be a tautology.

By the previous two claims, any Frege proof of φ_n has at least $\sum_{i=1}^{n} i$ symbols. Thus any Frege proof of φ_n has $\Omega(n^2)$ symbols.

Claim Let c be the maximum number of connectives shown in any inference rule or axiom of a Frege system $\mathcal{F}$. If an $\mathcal{F}$-proof P has k distinct active subformulas, then P has at least $\frac{k}{c}$ lines.

Thus any Frege proof of φ_n has $\Omega(n)$ lines. Hence any extended Frege proof of φ_n has size $\Omega(n)$.

3 Resolution

Resolution is an algorithm to prove formulas that are of a certain syntactic form. It arose in the 50's when people were looking for efficient theorem provers. The algorithm is simple; it has only one rule, the so-called Resolution Rule. The drawback is that certain formulas have long Resolution proofs compared to their Frege proofs. The Pigeonhole Principle is an example of this. In one of the next lectures we will see that it has no polynomial size Resolution proof, while it has polynomial size Frege proofs [1]. As said, Resolution can only be applied to formulas of a special kind. Namely, the formulas in Conjunctive Normal Form (CNF). A formula is said to be in CNF if it is the conjunction of disjunctions of variables and negated variables, i.e. if it is of the form

$$\bigwedge_i \left(\bigvee_j A_{ij} \right)$$

where the A_{ij}'s are of the form x or $\neg x$, for some variable x. Note that every formula can be written in CNF. For example,

$$\begin{array}{lcl} (x \to y) & \leftrightarrow & (\neg x \vee y) \\ (\neg(x \wedge y) \wedge z) & \leftrightarrow & ((\neg x \vee \neg y) \wedge z) \\ (x \vee (y \wedge z)) & \leftrightarrow & ((x \vee y) \wedge (x \vee z)) \end{array}$$

where the formulas at the right side are in CNF. Observe that in going to CNF the size of a formula can increase exponentially.

Definition We define what a Resolution Refutation is.
Syntax: variables $x_1, x_2, \ldots$
Literals: x_i, $\bar{x}_i$ (the intended meaning of $\bar{x}_i$ is $\neg x_i$). If x is a literal, then $\bar{x}$ is defined so that $\bar{\bar{x}} = x$: $\bar{x} = y$, when $x = \bar{y}$, and $\bar{x} = \bar{x}$ otherwise.
A *Clause* is a set of literals. The intended meaning of a clause is the disjunction of its members. We call a set of clauses Γ satisfiable if there exists a truth-assignment that satisfies all clauses in Γ.

Example

- $\{\bar{x}, y\}$ means $\neg x \vee y$.
- $\{x, \bar{x}\}$ is always valid.
- $\{\} = \emptyset$ is the unsatisfiable clause.

The *Resolution Rule*: (C and D denote clauses)

$$\frac{C \cup \{x\} \quad D \cup \{\bar{x}\}}{C \cup D}$$

The clause $C \cup D$ is called the *resolvent* of the rule. A *Resolution Refutation* of a set of clauses Γ consists of a sequence of clauses $C_1, \ldots, C_n$, where $C_n = \emptyset$, and for each $i \leq n$ either

1. $C_i \in \Gamma$

2. C_i is inferred by the Resolution Rule from C_j and C_h, for some $j, h < i$.

The idea behind a Resolution Refutation is the following. Assuming that Γ is satisfiable we infer other clauses that are also satisfiable till we end up with the empty clause. Since the empty clause is not satisfiable, the assumption that Γ is satisfiable is refuted. Thus Γ is not satisfiable. The following claims make this precise. W.l.o.g. we can disallow having both x and $\bar{x}$ in a clause in a proof.

Claim If the truth-assignment τ satisfies the clauses $C \cup \{x\}$ and $D \cup \{\bar{x}\}$, then τ satisfies the resolvent $C \cup D$.

Theorem 2 (Soundness Theorem) *If there exists a Resolution Refutation for* Γ*, then* Γ *is unsatisfiable.*

Proof Suppose Γ has a Resolution Refutation $C_1, \ldots, C_n$. If there would exist a truth-assignment τ that satisfies Γ, then by the previous claim τ would satisfy all C_i. Hence τ would satisfy the unsatisfiable empty clause C_n, quod non. Thus Γ is unsatisfiable.

References

[1] S. R. Buss, *Polynomial size proofs of the propositional pigeonhole principle*, Journal of Symbolic Logic, 52 (1987), pp. 916–927.

[2] ——, *Some remarks on lengths of propositional proofs*, Archive for Mathematical Logic, 34 (1995), pp. 377–394.

[3] J. Krajíček, *Bounded Arithmetic, Propositional Calculus and Complexity Theory*, Cambridge University Press, 1995.

[4] J. Krajíček and P. Pudlák, *Propositional proof systems, the consistency of first-order theories and the complexity of computations*, Journal of Symbolic Logic, 54 (1989), pp. 1063–1079.