Math 267a - Propositional Proof Complexity

Lecture #2: 16 January 2002

Lecturer: Sam Buss

Scribe Notes by: Sashka Davis

1 Introduction to Frege Proof Systems

Last time we stated the Completeness and the Soundness theorems for the Frege Proof Systems, today we focus on the Completeness Theorem. The main point of the Completeness Theorem is that there exists a Frege Proof System which is complete.

We begin with an example of $\mathcal{F}_0$-proof. The axioms of the Frege system we will use, are the Schematic Tautologies, defined in the previous lecture (**Ax1** denoting the first axiom, **Ax2** the second, etc.).

Example $(A \to A)$ has an $\mathcal{F}_0$-proof.

Proof
The following five lines form an $\mathcal{F}_0$-proof of $(A \to A)$.
$A \to (A \to A) \to A$, an instance of axiom **Ax1**
$A \to A \to A$, an instance of axiom **Ax1**
$(A \to (A \to A)) \to (A \to (A \to A) \to A)) \to (A \to A)$, an instance of axiom **Ax2**
$(A \to (A \to A) \to A) \to (A \to A)$, by **MP**
$A \to A$. $\square$

Proof Complexity The $\mathcal{F}_\mathbf{0}$-proof has $O(1)$ lines and $O(|A|)$ symbols.

Theorem 1 (Deduction Theorem) $\Gamma \vdash_{\mathcal{F}_0} A \to B$ *iff* $\Gamma, A \vdash_{\mathcal{F}} B$.

Proof

1. $\Gamma \vdash_{\mathcal{F}_0} A \to B \Longrightarrow \Gamma, A \vdash_{\mathcal{F}} B$.
   Suppose an $\mathcal{F}_0$-proof of $\Gamma \vdash_{\mathcal{F}_0} A \to B$ is given by lines (1)-(3). We can form an $\mathcal{F}_0$ proof of $\Gamma, A \vdash_{\mathcal{F}} B$ by adding two lines as shown:

$$\mathcal{F}_0: \quad \Gamma \tag{1}$$
$$\vdots \tag{2}$$
$$A \to B \tag{3}$$
$$A \tag{4}$$
$$B \tag{5}$$

Line (4) is the added new hypothesis. Line (5) is derived by MP. Thus we obtain $\mathcal{F}_0$-proof for $\Gamma, A \vdash_{\mathcal{F}} B$.

Proof Complexity $O(n)$ lines and $O(nm)$ symbols.

2. $\Gamma, A \vdash_{\mathcal{F}_0} B \Longrightarrow \Gamma \vdash_{\mathcal{F}} A \to B$.

   Proof Idea: Let the $\mathcal{F}_0$-proof of $\Gamma, A \vdash_{\mathcal{F}_0} B$ be a sequence $B = \varphi_1, \ldots, \varphi_n$. We shall use the substitution rule and replace each φ_i by $A \to \varphi_i$. The sequence of formulas $A \to \varphi_i$ is not a valid proof, but it can be converted into a valid proof as follows. Each φ_i either is A, or is inferred from A by MP, or is an axiom, or is a member of Γ. Thus to patch the proof we need to exhaust the following four cases.

   - Case 1: φ_i is A
     Then we re-use the 5-line proof of $A \to A$.
   - Case 2: φ_i is inferred by MP: $\dfrac{\varphi_j \quad \varphi_k = \varphi_j \to \varphi_i}{\varphi_i}$, $j, k < i$
     $A \to \varphi_j$
     $A \to \varphi_j \to \varphi_i$
     $(A \to \varphi_j) \to (A \to (\varphi_i \to \varphi_j)) \to (A \to \varphi_i)$, by **Ax2**
     $A \to \varphi_i$, by **MP**.
   - Case 3: φ_i is an axiom
     $\varphi_i \to (A \to \varphi_i)$, by **Ax1** .
     So φ_i can be replaced by the three line proof of $A \to \varphi_i$.
   - Case 4: $\varphi_i \in \Gamma$
     $\varphi_i \to (A \to \varphi_i)$, by **Ax1** .

   □

   Proof Complexity
   Each line in the original $\mathcal{F}_0$-proof becomes either three or five lines in the $\mathcal{F}_0$-proof of $\Gamma \vdash_{\mathcal{F}_0} A \to B$. The proof complexity remains $O(n)$ lines and $O(nm)$ symbols.

1.1 Usage of the Deduction Theorem

Let $\bigwedge\!\!\!\bigwedge_{i=1}^{k} A_i$, denotes any parenthesization of the conjunction of $A_1, \ldots, A_n$.

Example Given $\vdash_{\mathcal{F}_0} \bigwedge\!\!\!\bigwedge_{i=1}^{k} A_i \to A_{i0}$, with proof complexity $O(k)$ lines and $O(k|B|)$ symbols, where $B = \bigwedge\!\!\!\bigwedge_{i=1}^{k} A_i$, prove that $\bigwedge\!\!\!\bigwedge_{i=1}^{k} A_i \vdash_{\mathcal{F}_0} A_{i0}$.

Proof We follow the $\mathcal{F}_0$-proof. Begin with $\bigwedge\!\!\!\bigwedge_{i=1}^{k} A_i$. Repeatedly use the axioms $(A \wedge B \to B)$ and $(A \wedge B \to A)$ with MP. All the lines are well behaved. □

2 The Completeness and Implicational Completeness Theorems

Recall that the Completeness theorem states: $\phi \in TAUT \implies \vdash_{\mathcal{F}_0} \phi$, for some proof $\mathcal{F}_0$. Now we state and prove the Implicational Completeness Theorem.

Theorem 2 (Implicational Completeness Theorem) *If* $\Gamma \models A$ *then* $\Gamma \overset{\mathcal{F}_0}{\vdash} A$.

Proof If $\Gamma \models A$, then there exists a finite Σ, $\Sigma \subset \Gamma$, s.t. $\Sigma \models A$. So w.l.o.g. Γ is finite. Let $\Gamma = \{B_1, \ldots B_k\}$, then $\models B_1 \to (B_2 \to (\ldots \to (B_k \to A) \ldots))$.
By the Completeness Theorem there exists an $\mathcal{F}_0$-proof of the tautology. By applying the Deduction Theorem k times we obtain $\Gamma \overset{\mathcal{F}_0}{\vdash} A$. $\square$

Theorem 3 (Completeness Theorem) $A \in TAUT$*, then* $\vdash_{\mathcal{F}_0} A$.

Proof We mimic the method of the Truth Table proofs. We consider all possible truth assignments. Let $A = A(x_1, \ldots, x_k)$ and $A \in TAUT$. Let τ is a truth assignment, and

$$x_i^\tau = \begin{cases} x_i & \text{if } \tau(x_i) = \mathrm{T} \\ \neg x_i & \text{if } \tau(x_i) = \mathrm{F} \end{cases}$$

$$A^\tau = \begin{cases} A & \text{if } \tau(A) = \mathrm{T} \\ \neg A & \text{if } \tau(A) = \mathrm{F} \end{cases}$$

The proof follows from the following three claims:

Claim If $\vdash_{\mathcal{F}_0} \bigwedge_{i=1}^k x_i^\tau \to A^{(\tau)}$ then $\bigwedge_{i=1}^k x_i^\tau \vdash_{\mathcal{F}_0} A^{(\tau)}$

Proof The proof of the claim is based on the complexity of A.
Base case: If A is atomic then A is one of the x_i.
Suppose $A = B \bullet C$, where $\bullet$ is one of $\{\vee, \wedge, \to, \neg\}$, then $B^\tau, C^\tau \overset{\mathcal{F}_0}{\vdash} A^\tau$.
For each connective there are four cases for B and C. For example let "$\bullet$" = "$\to$" then:
$B, C \vdash_{\mathcal{F}} (B \to C)$
$B, \neg C \vdash_{\mathcal{F}} \neg(B \to C)$
$\neg B, C \vdash_{\mathcal{F}} (B \to C)$
$\neg B, \neg C \vdash_{\mathcal{F}} (B \to C)$

Proof Complexity The base case contributes $O(k)$ line, and for each connective the proof grows by finitely many lines, thus the total number of lines is $O(k + |A|) = O(|A|)$. Each line has $O(|A|)$ symbols, thus in total the proof has $O(|A|^2)$ symbols. However, we have to repeat this for all 2^k truth assignments to $x_1, x_2, \cdots, x_k$.

The following two claims would be used without a proof:

Claim $\vdash_{\mathcal{F}_0} ((Z \wedge C) \to D) \to ((\neg Z \wedge C) \to D) \to (C \to D)$

Claim $\vdash_{\mathcal{F}_0} ((Z \to A) \to (\neg Z \to A) \to A$

Now associating the conjunctions, $\bigwedge_{i=1}^{k} x_i^{\tau}$, from right to left w.l.o.g. we obtain:
$\pm x_1 \wedge (\pm x_2 \wedge (\ldots(\pm x_{k-1} \wedge \pm x_k)\ldots) \to A$. We peel off all the variables one by one to obtain A. E.g. the last steps (using the second claim) are:

$$\left.\begin{array}{r} x_{k-1} \wedge x_k \to A \\ \neg x_{k-1} \wedge x_k \to A \end{array}\right\} x_k \to A$$

$$\left.\begin{array}{r} x_{k-1} \wedge \neg x_k \to A \\ \neg x_{k-1} \wedge \neg x_k \to A \end{array}\right\} \neg x_k \to A$$

thus $\vdash_{\mathcal{F}_0} x_k \to A$ and $\vdash_{\mathcal{F}_0} \neg x_k \to A$. From this and the third claim, $\vdash_{\mathcal{F}_0} A$.
$\square$

Proof Complexity The last part of the proof contributes $O(2^k)$ new lines, with $O(|A|)$ symbols per line. Thus A has $\mathcal{F}_0$-proof of $O(|A|2^k)$ lines. The total number of symbols is $O(|A|^2 2^k)$, where k is the number of distinct variables in A.

3 Observations

The Completeness Theorem states that all valid tautologies can be proved. We observe that the size bounds of the $\mathcal{F}_0$-proofs are the same as the size bounds of the Truth Table Proofs (TTP). However, the $\mathcal{F}_0$ can be separated from the TTP. We demonstrate the separation by the following example.

Example $\phi = (A_1 \wedge \neg A_1) \vee (A_2 \wedge A_3 \wedge \cdots \wedge A_k)$.

ϕ has a short $\mathcal{F}_0$-proof and exponentially large TTP. Thus in the best case $\mathcal{F}_0$-proofs are better than TTP, but it is an open question whether they are better than TTP in the worst case.

A Proof System must be *sound* and the proofs ought to be *checkable efficiently* (in polynomial time). *Completeness* is another property which is nice and desirable, but not required.

4 P-simulate

The next theorem states that Truth Table Proofs (TTP) can be converted into $\mathcal{F}_0$ proofs by a polynomial time algorithm.

Theorem 4 (Simulation) *Frege Proof Systems p-simulate Truth Table Proofs.*

The converse does not hold as it can be seen from the example above. Thus TTP do not simulate Frege Proof System.

Definition An abstract propositional proof system over the propositional language
$L = \{\vee, \wedge, \to, \neg\}$ is a polynomial time computable function f with domain strings of symbols and $range(f) \subset TAUT$.

Definition The function f is complete if the $range(f) = TAUT$.

Definition An f-proof of a formula φ is any x s.t. $f(x) = \varphi$.

Definition $\mathcal{F}_0$ as an abstract proof system is defined as:

$$f_{\mathcal{F}_0}(x) = \begin{cases} \varphi & \text{if } x \text{ codes a valid } \mathcal{F}_0\text{-proof of } \varphi \\ (x_1 \vee \neg x_1) & \text{otherwise} \end{cases}$$

This idea for constructing an abstract proof systems works for many other proof systems too. For example, let ZF be the usual theory of set theory, then

$$f_{ZF}(x) = \begin{cases} \varphi & \text{if } x \text{ codes a valid } ZF \text{ proof of "}\varphi \text{ is a tautology"} \\ (x_1 \vee \neg x_1) & \text{otherwise} \end{cases}$$

is an abstract proof system.