Princeton University Spring'00	COS 598g: Proof Complexity
Lecture 1: Basic Propositional Calculus	
Lecturer: *Alexander Razborov*	Notes: *Subhash Khot*

This lecture gave a brief introduction to propositional calulus and Frege Proof System.

1 Propositional Logic

Let $p_1, p_2, \ldots$ be propositional variables where each variable can take value 0 or 1. The logical connectives are $\wedge, \vee, \neg, \equiv, \rightarrow$.

Definition 1 *A propositional formula is defined inductively as :*

1. *Each variable p_i is a formula.*
2. *If A and B are formulas then $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \equiv B)$ are formulas.*
3. *A is a formula iff it follows from 1 and 2.*

Notations : p_i^ϵ denotes p_i if $\epsilon = 1$ and denotes $\neg p_i$ if $\epsilon = 0$.

Definition 2 *A literal is a variable or a negated variable. A clause is a disjunction of literals. A formula in conjunctive normal form (CNF) is conjunction of clauses.*

Every propositional formula $A(p_1, \ldots, p_n)$ defines a Boolean function from $\{0,1\}^n$ to $\{0,1\}$ which is denoted by $\|A\|$. Note that for every Boolean function f there exists a formula A such that $\|A\| = f$.

A formula A is called *tautology* if the function $\|A\|$ is identically equal to 1. It is called *unsatisfiable* if $\|A\|$ is identiaclly 0. Note that A is a tautology iff $(\neg A)$ is unsatisfiable. Therefore, from the complexity point of view the sets of tautologies and unsatisfiable formulas are indistinguishable (and both are $co - NP$-complete).

Let $A(p_1, \ldots, p_n), B_1, \ldots, B_n$ be formulas. Then $A(B_1, \ldots, B_n)$ denotes a formula where every instance of variable p_i is replaced by the formula B_i. It is called a *substitutional instance* of A. Every substitutional instance of a tautology is a tautology.

2 Frege Proof System

Frege Proof System is a set of *logical axioms* and a single inference rule called *modus ponens*. There are about 20 logical axioms some of which are

1. $p \to p$.
2. $p \to p \vee q$.
3. $((p \to q) \wedge (r \to q)) \to ((p \vee r) \to q)$.
4. $(p \to q) \to ((p \to (q \to r)) \to (p \to r))$.

Modus Ponens is a rule which enables us to infer B from the formulas A and $A \to B$. This rule is written as $\frac{A \ \ A \to B}{B}$.

Definition 3 *A Frege proof is a sequence of formulas $A_1, \ldots, A_t$ such that every A_i is either a substitutional instance of a logical axiom or is inferred from two previous formulas A_j and $A_j \to A_i$ using modus ponens.*

Notation : $\vdash_F A$ denotes that there exists a Frege proof where $A_t = A$.

We say that $A_1, \ldots, A_k \vdash_F A$ if there is a Frege proof of A in which every formula is a substitutional instance of a logical axiom, is some A_i, or it is derived by modus ponens from two previous formulas. We call $A_1, \ldots, A_k$ *non-logical axioms*.

Theorem 4 *(Adequacy theorem for propositional logic)*

A formula A is provable iff A is a tautology.

The soundness (i.e. the forward implication) is obvious. To prove completeness, we need the following theorem.

Theorem 5 *(Deduction theorem)*

$$A_1, \ldots, A_k \vdash_F B \quad \textit{iff} \quad \vdash_F (A_1 \wedge A_2 \wedge \ldots \wedge A_k) \to B.$$

Exercise : Prove Deduction Theorem using induction on number of steps of proof of B with non-logical axioms $A_1, \ldots, A_k$.

Lemma 6 *Let $a_1, \ldots, a_n \in \{0, 1\}$ and A be any propositional formula on variables $p_1, \ldots, p_n$. Then*

$$p_1^{a_1}, \ldots, p_n^{a_n} \vdash_F A^{A(a_1, \ldots, a_n)}.$$

Here $A(a_1, \ldots, a_n)$ denotes the value of $||A||$ under Boolean assignment $p_i = a_i$, A^1 denotes A and A^0 denotes $\neg A$.

The proof of lemma is an easy exercise using inductive definition of propositional formula.

Proof of completeness in Adequacy theorem :

Let $\vec{a} = (a_1, \ldots, a_n)$ be a Boolean vector. Since A is a tautology, $A^{A(\vec{a})} = A$ for all $\vec{a}$. Using Lemma 6,

$$p_1^{a_1}, \ldots, p_n^{a_n} \vdash_F A,$$

for all $\vec{a}$. By deduction theorem,

$$\vdash_F p_1^{a_1} \wedge \ldots \wedge p_n^{a_n} \rightarrow A,$$

again for all $\vec{a}$. Using modus ponens and 3^{rd} Frege axiom 2^n times we have

$$\vdash_F \vee_{\vec{a}}(p_1^{a_1} \wedge \ldots \wedge p_n^{a_n}) \rightarrow A$$

We note that $\vee_{\vec{a}}(p_1^{a_1} \wedge \ldots \wedge p_n^{a_n})$ is a tautology that has an obvious Frege proof. Hence $\vdash_F A$.

Theorem 7 *(Craig's Interpolation Theorem)*

Suppose $\vdash_F A(\vec{p}, \vec{q}) \rightarrow B(\vec{q}, \vec{r})$, *then there exists a formula* $C(\vec{q})$ *called interpolant such that* $\vdash_F A(\vec{p}, \vec{q}) \rightarrow C(\vec{q})$ *and* $\vdash_F C(\vec{q}) \rightarrow B(\vec{q}, \vec{r})$.

Proof We give a semantic proof of Theorem 7. Let f be the Boolean function defined by

$$f(\vec{q}) = 1 \ \text{ iff } \ \exists\, \vec{x}\ \|A\|(\vec{x}, \vec{q}) = 1.$$

Let $C(\vec{q})$ be a formula such that $\|C\| = f$. It can be easily verified that C is the required interpolant.

The question whether Theorem 7, as well as its analogues for other proof systems, possesses a constructive semantic proof turns out to be of extreme importance for the whole theory of feasible proofs. We will extensively discuss it later.