Math 267a - Propositional Proof Complexity

Lecture #1: 14 January 2002

Lecturer: Sam Buss

Scribe Notes by: Robert Ellis

1 Introduction to Propositional Logic

1.1 Symbols and Definitions

The language of propositional logic consists of connectives, propositional variables, parentheses and formulas, shown in the table below. The meanings of the symbols are given by their corresponding

connectives	$\vee, \wedge, \neg, \rightarrow$
variables	$x_1, x_2, \ldots$
parentheses	(,)
formulas	$(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, $(\neg\phi)$, etc.

Table 1: Components of Statements of Propositional Logic

truth tables. The $\vee$ ("logical or"), $\wedge$ ("logical and") and $\rightarrow$ ("logical implication") operators are binary, while the $\neg$ ("logical negation") operator is unary. The truth tables for these operators are constructed by exhaustively assigning all possible truth values to the variables and listing the result defined by the operator.

x_1	x_2	$x_1 \vee x_2$
T	T	T
T	F	T
F	T	T
F	F	F

x_1	x_2	$x_1 \wedge x_2$
T	T	T
T	F	F
F	T	F
F	F	F

x_1	x_2	$x_1 \rightarrow x_2$
T	T	T
T	F	F
F	T	T
F	F	T

x_1	$\neg x_1$
T	F
F	T

A *truth assignment*

$$\tau : \{x_1, x_2, \ldots\} \rightarrow \{\mathrm{T}, \mathrm{F}\}$$

assigns logical truth values to the variables. A truth assignment τ extends to a truth assignment $\overline{\tau} : \{\phi\} \rightarrow \{\mathrm{T}, \mathrm{F}\}$ on the set of formulas $\{\phi\}$ by assigning truth values to variables in the formula and determining the truth of the formula by invoking the definitions of the connectives. The truth of a compound formula depends on the truth of its constituents. For example,

$$\overline{\tau}(\phi \rightarrow \psi) = \begin{cases} \mathrm{T} & \text{if } \overline{\tau}(\phi) = \mathrm{F} \text{ or } \overline{\tau}(\psi) = \mathrm{T} \\ \mathrm{F} & \text{otherwise.} \end{cases}$$

Two other common symbols, $\oplus$ and $|$, are the "exclusive or" and "nand" binary operators expressible in terms of the first four symbols. Specifically, $x_1|x_2 := \neg(x_1 \wedge x_2)$ and $x_1 \oplus x_2 := \neg((x_1 \wedge x_2) \vee (x_1|x_2))$.

1.2 SAT, TAUT, $\mathcal{P}$ and $\mathcal{NP}$

Statements in propositional logic, or *predicates*, which are of special interest are those for which there exists a truth assignment for which the predicate is true, and those for which the predicate is true for all truth assignments.

Definition The predicate ϕ is a *tautology* if for all truth assignments τ, $\overline{\tau}(\phi) = \mathrm{T}$.

Definition The predicate ϕ is *satisfiable* if there exists a truth assignment τ such that $\overline{\tau}(\phi) = \mathrm{T}$.

Based on their definitions, tautologies and satisfiable predicates are related as follows.

Fact If ϕ is a tautology then $(\neg\phi)$ is not satisfiable.

Definition *TAUT* is the set of all tautologies.

Definition *SAT* is the set of all satisfiable formulas.

The problem of recognizing a member of SAT is fundamental in computational complexity. $\mathcal{P}$ is defined to be the set of all predicates that are polynomial time recognizable. In this context, a predicate is a decision procedure yielding either 'T' or 'F'. *Polynomial time recognizable* means there exists an algorithm implementing the decision procedure which is bounded in the number of steps by a polynomial in the size of the input.

Example Let WFF, the set of well-formed formulas, be defined as the set of strings which are validly formed formulas build on connectives, parentheses and variables. Then the predicate WFF is a member of $\mathcal{P}$.

Definition $\mathcal{NP}$ is the set of predicates Q which can be expressed as

$$Q(x) = (\exists y, |y| < p(|x|))R(x, y),$$

where p is a polynomial, $|x|$ is the length of x viewed as a string, y is the "witness" to x, and R is a polynomial time algorithm which verifies that y is a witness to x. Thus $Q(x) = \mathrm{T}$ if and only if a witness y exists such that the time property $R(x, y)$ holds.

To show that SAT is in $\mathcal{NP}$, simply express it in the above form; e.g.,

$$SAT(X) \equiv (\exists y, (|y| \leq |x|))TRU(x, y),$$

where $TRU(x, y)$ is the algorithm which verifies that y encodes a truth assignment which satisfies x. We may take y to be weakly less than x in length, because it can simply encode truth values of the variables in the formula x as binary digits.

Homework 1 *Turn in a proof of $\mathcal{P} = \mathcal{NP}$ or $\mathcal{P} \neq \mathcal{NP}$ for \$1,000,000 (from the Clay Mathematics Institute) and an A+.*

2 Propositional Proof Systems

One purpose of propositional proof systems is to provide evidence of the membership of a formula ϕ in the set of tautologies TAUT. Of particular interest is the size of the proof of a tautology.

2.1 Truth Tables

Truth tables provide straightforward but lengthy verifications of tautologies. The proof of a tautology proceeds by exhaustively writing down all 2^n truth assignments for a predicate in n variables, and resolving the truth in each case by the logical rules. The written-out truth table is the actual proof. A proof of the tautology $A \to (B \to A)$ is given by the following table.

A	B	$B \to A$	$A \to (B \to A)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

We can easily obtain an estimate for the size of a truth table proof for a tautology ϕ. Let p be the number of distinct variables, and let m be the total number of unary or binary logical operators. The the truth table has approximately $m2^p = 2^{O(p)}$ entries. The size of such a table for $p = 100$ would be at least 1000 times the age of the universe in nanoseconds.

The exponential growth rate of the size of the truth table makes this kind of proof infeasible for even relatively small numbers of variables. Growth rates like 2^n, $2^{\epsilon n}$ and 2^{n^ϵ} are all "too big" in this sense. We prefer growth rates like n, $n \log n$, n^2 and n^3, which are feasible for large values of n.

2.2 Frege Proof Systems

A *Frege Proof System* consists of axioms, substitution rules and a rule of inference from which all tautologies can be proved in a much more tractable form that that of truth tables. Informally, a proof of a formula ϕ consists of a sequence of formulas in which each step is either an axiom, a substitution of a previous step, or derived by inference, and the last step is ϕ.

2.2.1 Proof System Components

We formalize these notions in the following definitions.

Definition The *schematic axiom* of a Frege proof system are a list of tautologies called *schematic tautologies* which may be used as the starting point of a Frege proof.

The list of schematic tautologies in a common Frege proof system, which allows any tautology to be proved, appears in Table 2. Here, A, B and C are variables, and for well-definedness of associativity we adopt the shorthand $\phi \to \psi \to \chi := \phi \to (\psi \to \chi)$.

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

Table 2: Schematic Tautologies for a Frege proof system

Definition A *schematic substitution* σ is a mapping $\sigma : V \to WFF$ from a set $V \subseteq \{x_1, x_2, \ldots\}$ of variables to the set of well-formed formulas, written by

$$\sigma = (x_1/\phi_1, \ldots, x_k/\phi_k),$$

where $\phi_i = \sigma(x_i) = x_i\sigma$.

Informally, a schematic substitution σ replaces a variable x_i with some formula ϕ_i.

Definition $A\sigma$ is defined to be the result of replacing (simultaneously) each occurrence of x_i in the formula A by $x_i\sigma = \sigma(x_i)$.

Example Let $A = x_1 \to x_2$ and let $\sigma = (x_1/(x_1 \wedge x_2), x_2/x_1)$. Then

$$A\sigma = (x_1 \wedge x_2) \to x_1.$$

Fact If $\phi \in TAUT$, then for all σ, $\phi\sigma \in TAUT$.

Definition The *schematic rule of inference* called *modus ponens*, or MP, is represented by

$$\frac{x_1 \quad x_1 \to x_2}{x_2},$$

and is invoked by confirming that x_2 is true whenever x_1 is true and x_1 implies x_2.

Definition A *schematic inference*, denoted

$$\frac{A_1, \quad \ldots, \quad A_k}{B},$$

means that for all σ, if $A_1\sigma, \ldots, A_k\sigma$ have been proved, then $B\sigma$ can be inferred. Taking $k = 0$ yields a schematic axiom.

The above definitions are used to develop a schematic proof that some formula ϕ is a tautology. We formalize this type of Frege proof as follows.

Definition An $\mathcal{F}_0$-proof is a sequence of formulas $\phi_1, \phi_2, \ldots, \phi_k$ such that each ϕ_i is either an axiom or is inferred by *modus ponens* from some ϕ_j and ϕ_l, for $j, l < i$. It is called a *proof* of ϕ_k.

2.2.2 Proof System Characteristics

In the Frege proof system just described, the properties of soundness and completeness are highly desirable. *Soundness* means that no proof exists for a formula that is not a tautology. *Completeness* means that every tautology has a corresponding proof. We introduce the symbolism $\vdash_{\overline{\mathcal{F}_0}} \phi$ to denote that $\mathcal{F}_0$ is a proof of ϕ, and use $\models \phi$ to denote $\phi \in TAUT$.

Theorem 1 (Soundness) *If* $\vdash_{\overline{\mathcal{F}_0}} \phi$ *then* $\phi \in TAUT$*.*

Proof The proof is by induction on the number of steps in the $\mathcal{F}_0$ proof. The proof starts with a schematic axiom which is a tautology, every step in the proof by substitution is a tautology, and MP preserves tautologies, and so ϕ is a tautology.

Theorem 2 (Completeness) *If* $\phi \in TAUT$*, then* $\vdash_{\overline{\mathcal{F}_0}} \phi$ *for some proof* $\mathcal{F}_0$*.*

Proof The proof of completeness for this Frege proof system is deferred until Lecture #2.

Generally, we require an expanded notion of soundness and completeness than what is outlined above. In particular, we may wish to prove a tautology in a proof system starting from an extra set of axiomatically tautological formulas.

Definition Let Γ be a set of formulas. Then $\Gamma \models \phi$ provided that for all truth assignments τ, if for all $\gamma \in \Gamma$ we have $\overline{\tau}(\gamma) = \mathrm{T}$, then $\overline{\tau}(\phi) = \mathrm{T}$. We call $\Gamma \models \phi$ a *tautological implication.*

The corresponding version of a $\mathcal{F}_0$-proof is as follows.

Definition Let Γ be a set of formulas. Then $\Gamma \vdash_{\overline{\mathcal{F}_0}} \phi$ provided there exists a sequence $\phi_1, \ldots, \phi_k = \phi$ such that each ϕ_i is in Γ or is an (instance of an) axiom or is inferred by MP. We call the sequence an $\mathcal{F}_0$*-proof with hypotheses.*

We would certainly like to know how to deal with implicational tautologies when Γ is an infinite set. Fortunately, a compactness result simplifies things.

Theorem 3 (Compactness of tautological implication) *If* $\Gamma \models \phi$*, then there exists a finite subset* $\Gamma_0 \subseteq \Gamma$ *such that* $\Gamma_0 \models \phi$*.*

Proof The proof is left as an exercise.

Proposition 4 (Derived substitution rule)

1. *If* $\vdash_{\overline{\mathcal{F}_0}} A$ *and* σ *is a substitution, then* $\vdash_{\overline{\mathcal{F}_0}} A\sigma$*.*
2. *If* $\Gamma \vdash_{\overline{\mathcal{F}_0}} \phi$*, then* $\Gamma\sigma \vdash_{\overline{\mathcal{F}_0}} \phi\sigma$*.*

Proof Part 1 proceeds by applying σ to the whole $\mathcal{F}_0$-proof. Start with the sequence $\phi_1, \phi_2, \ldots, \phi_k = A$ and replace ϕ_i with $\phi_i\sigma$ to obtain $\phi_1\sigma, \phi_2\sigma, \ldots, \phi_k\sigma = A\sigma$. Part 2 proceeds similarly.

Note that a double substitution into a schematic axiom, such as ϕ_i replaced with $\phi_i\sigma$ can be simplified to a single substitution. Define

$$\begin{aligned} \sigma : x_i \mapsto x_i\sigma &= \phi_i, \qquad \text{and} \\ \tau : x_i \mapsto x_i\tau &= \psi_i. \end{aligned}$$

Then the double substitution $(A\sigma)\tau$ can be written as $A(\sigma\tau)$ since

$$(\sigma\tau) : x_i \mapsto \phi_i\tau = x_i\sigma\tau.$$

The implicational soundness and completeness theorems are as follows.

Theorem 5 (Implicational soundness of $\mathcal{F}_0$) *If* $\Gamma \vdash_{\mathcal{F}_0} \phi$, *then* $\Gamma \models \phi$.

Proof The proof proceeds by induction on the number of steps in the $\mathcal{F}_0$-proof.

Theorem 6 (Implicational completeness of $\mathcal{F}_0$) *If* $\Gamma \models \phi$, *then* $\Gamma \vdash_{\mathcal{F}_0} \phi$.

Proof The proof is deferred until Lecture #2.