Princeton University Spring'00	COS 598g: Proof Complexity
Lecture 2: Equational and First-order Theories	
Lecturer: *Alexander Razborov*	Notes: *Subhash Khot*

1 Equational Logic

Let $x_1, x_2, \ldots$ be variables, this time with the intended meaning "objects from some domain". A *language* consists of function symbols f^k where k is the arity of the function symbol. A 0-ary function is a constant.

A *term* over L is defined inductively as:

1. A variable is a term.
2. If $t_1, \ldots, t_k$ are terms and f^k is a function symbol then $f^k(t_1, \ldots, t_k)$ is a term.

Definition 1 *A structure for L is a domain M equipped with interpretation for each function symbol. The structure associates a function $\|f^k\|$ to each function symbol,*

$$\|f^k\| : M^k \to M.$$

We can extend interpretation for function symbols to interpretation for any term. If $Vars(t)$ denotes the set of variables of term t then $\|t\| : M^{Vars(t)} \to M$.

Example 2 *Language of formal arithmetic (Peano arithmetic) is:*

$$L_{PA} = \ < 0, 1, +, \cdot, S > .$$

The set of non-negative integers $\mathbf{N}$ *is a natural interpretation for* L_{PA}.

Example 3 *Group language* L_G *is:*

$$L_G = \ < 1, \cdot, x^{-1} > .$$

Any group is an interpretation for this language with 1 as identity element and $\cdot$ as multiplication operation.

Example 4 *Propositional Calculus can be also considered as the* **equational** *language*

$$L_{PC} = \; < \neg, \vee, \wedge, \rightarrow, \equiv > .$$

A propositional formula is a term over this language. This language has a natural structure $M = \{0, 1\}$.

Definition 5 *An equation is a statement of the form $t = s$ where s, t are terms. Given a structure M, we say that $t = s$ is valid on M iff $\|t\|$ and $\|s\|$ define the same function.*

In Example 1, there is a unique polynomial p_t for every term t such that $t = p_t$ is valid on structure $\mathbf{N}$. In Example 3, $t = s$ is valid iff the propositional formula $t \equiv s$ is a tautology. For every term t, there is a CNF formula ϕ_t such that $t = \phi_t$ is valid.

Definition 6 *For equation $E : t = s$, $\models E$ means E is valid on every structure. For equations $E_1, \ldots, E_k$, we say $E_1 \ldots, E_k \models E$ if for every structure on which $E_1, \ldots, E_k$ are valid, E is valid too.*

Axioms of equational logic are :

1. $$t = t$$

2. $$\frac{t = r, r = s}{t = s}$$

3. $$\frac{t_1 = s_1, \ldots, t_k = s_k}{f^k(t_1, \ldots, t_k) = f^k(s_1, \ldots, s_k)}$$

4. Closure under substitution :

$$\frac{t(x_1, \ldots, x_k) = s(x_1, \ldots, x_k)}{t(r_1, \ldots, r_k) = s(r_1, \ldots, r_k)}$$

   where $r_1, \ldots, r_k$ are terms.

We say $E_1, \ldots, E_k \vdash E$ if there exists a proof of E using axioms of equational logic and $E_1, \ldots, E_k$.

Theorem 7 *(Adequacy Theorem)*

$$E_1, \ldots, E_k \models E \;\; \textit{iff} \;\; E_1, \ldots, E_k \vdash E.$$

Proof The backward direction is obvious. To prove the forward implication, assuming $E_1, \ldots, E_k \not\vdash E$ we construct a structure M on which $E_1, \ldots, E_k$ are valid but E is not valid.

Let $\mathbf{T}$ be the set of all terms. Define the equivalence relation $\approx$ on $\mathbf{T}$ as follows : $t \approx s$ iff $E_1, \ldots, E_k \vdash t = s$. Let $M = \mathbf{T}/\approx$, i.e. M is the set of all terms modulo the relation $\approx$. Let $[t]$ denote the equivalence class of t. We define interpretation of function symbols on M in a natural way:

$$\|f\|([t_1], \ldots, [t_k]) = [f(t_1, \ldots, t_k)].$$

This interpretation is unambiguous due to rule 3. It follows from the definition of M that $E_1, \ldots, E_k$ are valid on M but E is not.

2 First-order Theories

Let the variables $x_1, x_2, \ldots$ have the same meaning as before. A *first-order language* L consists of function symbols f^k and predicate symbols P^k.

A *first-order formula* is defined inductively as:

1. If t, s are terms then $t = s$ is a formula.
2. If P^k is a predicate symbol with arity k, and $t_1, \ldots, t_k$ are terms then $P^k(t_1, \ldots, t_k)$ is a formula.
3. If A, B are formulas then so are $(\neg A), (A \vee B), (A \wedge B), (A \to B), (A \equiv B)$.
4. If A is a formula, then $(\forall x)A$ and $(\exists x)A$ are formula where $\forall, \exists$ are universal and existential quantifiers respectively.

If A is obtained by rules 1,2 alone, then A is called *atomic* formula. If we additionally allow rule 3, we get the set of *open* formulas. Let $Vars(A)$ denote the set of all free variables of A. If A is atomic formula, then $Vars(A)$ is the set of all variables in A. $Vars(\neg A) = Vars(A)$, $Vars(A \vee B) = Vars(A) \cup Vars(B)$, $Vars(A \wedge B) = Vars(A) \cup Vars(B)$, $Vars((\forall x)A) = Vars(A) \setminus \{x\}$.

We write $A(x_1, \ldots, x_k)$ to say that A is a formula with free variables $x_1, \ldots, x_k$ and possibly more free variables.

A *structure* for a language is a domain M with interpretation $\|f^k\| : M^k \to M$ for every function symbol and interpretation $\|P^k\| : M^k \to \{0, 1\}$ for every predicate symbol. The interpretation is extended to every formula as follows :

$\|A\|$ is a function $\|A\| : M^{Vars(A)} \to \{0,1\}$. If A is formed using rules 1,2,3 above, the interpretation $\|A\|$ is defined in a natural way. If A is obtained by rule 4, say, $A = (\forall x_1)B$ where $Vars(B) = \{x_1, \ldots, x_k\}$, we define

$$\|A\|(a_2, \ldots, a_k) = 1 \quad \text{iff} \quad \forall a_1 \in M \;\; \|B\|(a_1, \ldots, a_k) = 1.$$

If $A = (\exists x_1)B$, we define

$$\|A\|(a_2, \ldots, a_k) = 1 \quad \text{iff} \quad \exists a_1 \in M \;\; \|B\|(a_1, \ldots, a_k) = 1.$$

Definition 8 *A formula A is valid on M if $\|A\|$ is identically 1. We say $A_1, \ldots, A_k \models A$ if for every structure on which $A_1, \ldots, A_k$ are valid, A is valid too. A sentence is a formula with no free variables.*

The axioms of first-order logic include all axioms of propositional calculus and equational logic with several additional axioms (and one rule) describing the behaviour of quantifiers, like

1. $A([t/x]) \to (\exists x)A(x)$ where $A([t/x])$ is a formula obtained from A by replacing every free occurrence of x by term t.
2. $(\forall x(A \to B(x)) \to (A \to \forall x B(x))$ if $x \notin Vars(A)$.

first-order logic has two inference rules:

$$Modus\ Ponens : \frac{A \quad A \to B}{B}$$

$$Generalization : \frac{A(x)}{\forall x A(x)}$$

We state the following important theorems about first-order logic. The proofs can be found in any standard book on mathematical logic.

Theorem 9 *(Gödel's Completeness Theorem)*

$$A_1, \ldots, A_m \models A \quad \textit{iff} \quad A_1, \ldots, A_m \vdash A.$$

Theorem 10 *(Deduction Theorem) For any sentences $A_1, \ldots, A_m, A$,*

$$A_1, \ldots, A_m \vdash A \quad \textit{iff} \quad \vdash (A_1 \wedge \ldots \wedge A_m) \to A.$$

A *first-order theory* is any set of sentences containing all axioms of the first-order logic and closed under its rules. In particular, the *first-order theory of a structure* is the set of all sentences valid on that structure.

Sasha stated the following facts:

- First-order theory of integers (not to be confused with Peano arithmetic which we will be considering in the next lecture) is highly non-recursive.
- First-order theory of groups is undecidable.
- First-order theory of the Boolean algebra $\{0, 1\}$ (and of any finite structure) is decidable. First-order theory of the class of all Boolean algebras is also decidable but this is a highly non-trivial result.