FO Logic & PEANO ARITHMETIC

First Order Logic

Language $\mathcal{L}$ specified by:

(1) A set of function symbols, each with a specified arity

Ex: $\underbrace{+}_{2}, \underbrace{\cdot}_{2}, \underbrace{0}_{0}, \underbrace{S}_{1}$ ← arity

(2) A set of predicate symbols, each with a specified arity

Ex: $<, \leq, =$

(3) A set of variable symbols $x, y, z, \ldots \; a, b, c$

(4) Logical symbols $\vee, \wedge, \neg, \forall, \exists$

Example: $\mathcal{L}_A$ Language of arithmetic: (1) function symbols $0, S, +, \cdot$

(2) Relation symbols $=, \leq$

Terms over $\mathcal{L}$

Formally defined inductively by composing function symbols

Examples of terms over $\mathcal{L}_A$:

→ $+\,s0\,sss0$: we will write as $s0 + sss0$ for readability

→ $(x + (ssy \cdot ss0)) \cdot sx$

First Order Formulas over $\mathcal{L}$

Again defined inductively:

(1) If P is a k-ary predicate symbol of $\mathcal{L}$,

and $t_1, .., t_k$ are terms

then $P(t_1, .., t_k)$ is an atomic formula of $\mathcal{L}$

(2) If A, B are $\mathcal{L}$-formulas, so is:

$\neg A$, $A \vee B$, $A \wedge B$, $\forall x A$, $\exists x B$

Semantics of FO Logic over $\mathcal{L}$

An $\mathcal{L}$-structure $\mathfrak{M}$ consists of

(1) A nonempty set M called the underlying universe

(2) for every k-ary function symbol f, an associated k-ary function $f^{\mathfrak{M}} : M^k \to M$

(3) For every k-ary relation symbol R, an associated k-ary relation $R^{\mathfrak{M}} : M^k \to \{0,1\}$

Free and Bound Variables

Defn A variable x in a formula is called free if it is not quantified, and otherwise is called bound. A formula A is a sentence if all variables in A are quantified.

Example $\forall x \, \exists y \, A(x, y, a)$

bound variables

free variable

Convention: x, y, z denote bound variables,

a, b, c " free "

Evaluating a Sentence over $\mathfrak{M}$

given a model $\mathfrak{M}$, we can evaluate a sentence A as either true (1), or false (0).

Notation: $\mathfrak{M} \models A$ means A evaluates to true under $\mathfrak{M}$

(1) $\mathfrak{M} \models P(t_1, \ldots, t_k)$ if $P^{\mathfrak{M}}(t_1, \ldots t_k) = 1$

(2) $\mathfrak{M} \models \neg A$ if $\mathfrak{M} \not\models A$

(3) $\mathfrak{M} \models A \vee B$ if either $\mathfrak{M} \models A$ or $\mathfrak{M} \models B$

(4) $\mathfrak{M} \models A \wedge B$ if $\mathfrak{M} \models A$ and $\mathfrak{M} \models B$

(5) $\mathfrak{M} \models \forall x\, A(x)$ if $\forall m \in M$ $\mathfrak{M} \models A(\frac{m}{x})$

(6) $\mathfrak{M} \models \exists x\, A(x)$ if $\exists m \in M$ $\mathfrak{M} \models A(\frac{m}{x})$

Defn $\models A$ (A is valid) iff for every model $\mathcal{M}$, $\mathcal{M} \models A$

Examples Let $\mathcal{M} = (\mathbb{N}$, usual definitions of $+, \cdot, s, 0)$

(1) $\mathcal{M} \models s0 + ss0 \leq sss0$, but $s0 + ss0 \leq sss0$ is not valid

(2) $\mathcal{M} \models \forall x \exists y (x + x = y)$, but not valid

First Order Proof System LK (extends propositional sequent calculus)

Lines are **sequents** $A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_\ell$

intended meaning : $A_1 \wedge \ldots \wedge A_k \supset B_1 \vee \ldots \vee B_\ell$

LK Rules

I. Structural Rules

Weakening

$$\frac{\Gamma \rightarrow \Delta}{\Gamma, A \rightarrow \Delta} \qquad \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, B}$$

Exchange

$$\frac{\Gamma, A, B, \Gamma' \rightarrow \Delta}{\Gamma, B, A, \Gamma' \rightarrow \Delta} \qquad \frac{\Gamma \rightarrow \Delta, A, B, \Delta'}{\Gamma \rightarrow \Delta, B, A, \Delta'}$$

Contraction

$$\frac{\Gamma, A, A \rightarrow \Delta}{\Gamma, A \rightarrow \Delta} \qquad \frac{\Gamma \rightarrow \Delta, A, A}{\Gamma \rightarrow \Delta, A}$$

II. Logical Rules

Negation

$$\frac{\Gamma \to \Delta, A}{\Gamma, \neg A \to \Delta} \qquad \frac{\Gamma, A \to \Delta}{\Gamma \to \Delta, \neg A}$$

AND

$$\frac{A, B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A \quad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}$$

OR

$$\frac{A, \Gamma \to \Delta \quad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A, B}{\Gamma \to \Delta, A \vee B}$$

$\forall$

$$\frac{A(t), \Gamma \to \Delta}{\forall x A(x), \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A(b)}{\Gamma \to \Delta, \forall x A(x)}$$

b is a free variable only occurring in A

$\exists$

$$\frac{A(b), \Gamma \to \Delta}{\exists x A(x), \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, \exists x A(x)}$$

II. Logical Rules cont'd

Axiom $\quad A \to A$

Cut Rule $\quad \dfrac{\Gamma, A \to \Delta \qquad \Gamma \to \Delta, A}{\Gamma \to \Delta}$

Soundness and completeness of FO Logic

Defn A First order sequent $A_1, \ldots, A_k \to B_1, \ldots, B_\ell$ is valid iff

$$\models \neg(A_1 \wedge \ldots \wedge A_k) \vee (B_1 \vee \ldots \vee B_\ell)$$

Theorem

(1) (Soundness) If a sequent has an LK proof, then it is valid

(2) (Completeness) Every valid sequent has an LK proof

Peano Arithmetic Proofs

- Underlying language $\mathcal{L}_A = \{0, +, \cdot, s \,;\, =, \leq\}$
- Lines are sequents over $\mathcal{L}_A$
- All rules/axioms of LK PLUS
  - A SET OF 6 BASIC AXIOMS (e.g. $\forall x \forall y (x+y = y+x)$)
  - INDUCTION RULE: $$\frac{A(b), \Gamma \to \Delta, A(b+1)}{A(0), \Gamma \to \Delta, \forall x A(x)}$$

1 abbreviates S0

Bounded Arithmetic S_2^i, T_2^i [Buss]

A constructive proof system is one in which proofs of existence implicitly contain or imply the existence of an algorithm to find the object which is proved to exist

A feasibly constructive proof system: the algorithm will be feasible

S_2^i, T_2^i : Restrictions of Peano arithmetic. Witnessing Theorems show proofs are feasibly constructive

Sentence	Witnessing theorem
$\forall x\, \exists y\, A(x,y)$	S_2^1 : polytime algorithm S_2^i : algorithm in i^{th} level of polyhierarchy T_2^1 : similar to S_2^1 but PLS algorithm

Language of Bounded Arithmetic $\mathcal{L}_{BA}$

Function symbols: $0,\ s,\ +,\ \cdot,\ |x|,\ \lfloor \tfrac{1}{2}x \rfloor,\ \#$

length of $x \in \mathbb{N}$ in binary

$x \# y = 2^{|x|\cdot|y|}$

allows polynomial growth rate of terms

Relation symbols: $=,\ \leq$

Logical Symbols:

PA logical symbols $(\neg, \vee, \wedge, \forall, \exists)$

plus bounded quantifiers: $\forall x \leq t\ A(x,a),\ \exists x \leq t\ A(x,a)$

x runs over all natural numbers of length $\leq$ poly$(|a|)$

and sharply bounded quantifiers: $\forall x \leq |t|\ A(x,a)\quad \exists x \leq |t|\ A(x,a)$

x runs over all numbers $\leq$ poly(a)

Bounded Arithmetic Proofs (formalized in LK)

- Lines are sequents over $\mathcal{L}_{BA}$
- All rules/axioms of LK PLUS
  - A SET OF (~25) BASIC AXIOMS
  - Rules for Bounded Quantifiers

$$\frac{b \le s,\ A(b),\ \Gamma \to \Delta}{\exists x \le s\ A(x),\ \Gamma \to \Delta} \qquad \frac{\Gamma \to \Delta,\ A(t)}{t \le s,\ \Gamma \to \Delta,\ \exists x \le s\ A(x)}$$

$$\frac{A(t),\ \Gamma \to \Delta}{t \le s,\ \forall x \le s\ A(x),\ \Gamma \to \Delta} \qquad \frac{b \le s,\ \Gamma \to \Delta,\ A(b)}{\Gamma \to \Delta,\ \forall x \le s\ A(x)}$$

  - Restricted Induction Rule

T^i_2 has Σ^b_i-IND:

$$\frac{A(b),\ \Gamma \to \Delta,\ A(b+1)}{A(0),\ \Gamma \to \Delta,\ A(t)}$$

S^i_2 has Σ^b_i - PIND:

$$\frac{A(\lfloor \tfrac{1}{2} b \rfloor),\ \Gamma \to \Delta,\ A(b)}{A(0),\ \Gamma \to \Delta,\ A(t)}$$

$A \in \Sigma^b_i$

Σ_i^b and Π_i^b formulas

$$\Sigma_i^b : \underbrace{\exists x_1 \le t_1 \ \forall x_2 \le t_2 \ \exists x_3 \le t_3 \ \cdots}_{i \text{ alternations}} \quad A(a_1, x_1, x_2, \ldots x_k)$$

$$\Pi_i^b : \forall x_1 \le t_1 \ \exists x_2 \le t_2 \ \cdots \quad A(a_1, x_1, \ldots, x_k)$$

Main Witnessing Theorems for S_2^1

Let $A := \forall a \; \exists x \leq t(a) \; B(a,x)$ be a $\forall \Sigma_1^b$ formula provable in S_2^1

Then there is a function $f: \mathbb{N} \to \mathbb{N}$ computable in polynomial time such that $\mathbb{N} \models \forall a \; B(a, f(a))$ (that is, over standard model of $\mathbb{N}$, f finds x such that $B(a,x)$ is true)

Similar witnessing theorems hold for S_2^i, T_2^i, $\forall i \geq 1$

Translation I : From S^1_2 proofs to Extended Frege

It is helpful to think of S^1_2 as uniform proof system, and EF as the corresponding Nonuniform pf system.

Translation : For any $\forall \Sigma^b_1$ formula $A := \forall a\, \exists x \leq t(a)\ B(a, x)$ provable in S^1_2, there is a sequence of propositional statements $[\![A]\!]_n$ (expressing A for all $m \in \mathbb{N}$, $|m| = n$) such that $[\![A]\!]_n$ has polysize EF proofs

Translation II : From Relativized $S_2^i(R)$ proofs to AC_i^0-Frege proofs

$S_2^i(R)$: Just like S_2^i but with a New k-ary relation symbol R.

It is helpful to think of a Σ_i^b formula of $S_2^i(R)$ as corresponding to a predicate in i^{th} level of relativized poly hierarchy

Translation For any $\forall\Sigma_i^b$ formula A^R provable in $S_2^i(R)$, there is a sequence of propositional statements $[\![A^R]\!]_n$ (expressing A^R for all $m \in \mathbb{N}$, $|m| = n$) such that $[\![A^R]\!]_n$ has quasi-poly size AC_i^0-Frege proofs.

Translation II : From Relativized $S^i_2(R)$ proofs to AC^0_i-Frege proofs

Example: PHP(R) = Pigeonhole principle for relation R

$$\forall a \left[\left(\exists x \leq a+1 \ \forall y \leq a \ \neg R(x,y) \right) \vee \left(\exists x_1, x_2 \leq a+1 \ \exists y \leq a \ \left(x_1 \neq x_2 \wedge R(x_1,y) \wedge R(x_2,y) \right) \right) \right]$$

Propositional Translation: $[\![PHP^R]\!]_n$ (set $a := n$, $n \in \mathbb{N}$)

Propositional Variables $R_{i,j}$, $i \leq n+1$, $j \leq n$

$$\bigvee_{i \in [n+1]} \bigwedge_{j \in [n]} \neg R_{i,j} \ \vee \bigvee_{\substack{i_1 \neq i_2 \\ i_1, i_2 \in [n+1]}} \ \bigvee_{j \in [n]} R_{i_1 j} \wedge R_{i_2 j}$$

Main Steps : $S^i_2(R) \longrightarrow AC^0$ - Frege

Roughly similar to reduction from Relativized Poly hierarchy PH^R to quasipoly size AC^0 circuits (but more work)

Step ① Use cut-elimination to show that if $\longrightarrow \overbrace{\forall a\, \exists x \leq t(a)\, B(a,x)}^{A}$ has a $S^i_2(R)$ proof, then there is another $S^i_2(R)$ proof Π of $\rightarrow A$ where all formulas in the proof $\in \Sigma^b_i(R)$

② Fix $n \in \mathbb{N}$

ie consider the restricted statement $\longrightarrow \exists x \leq t(n)\, B(a,x)$

Translate each line in Π to an AC^0-formula

③ Patch together an AC^0-Frege proof from the translated lines. (Main step: unwind induction via repeated cut rule)

Step ① "Free Cut-Free Elimination"

Let $S_2^i(R) \vdash A^R(a)$ $\quad A \in \Sigma_i^b(R)$

Then there is an $S_2^i(R)$ proof Π of $A^R(a)$ with NO "free cuts"

free cut: A cut inference on a formula that is not from an induction axiom/inference or a subformula of A

- also we can assume the only free variables in proof are those occurring in an induction inference, plus a (the free variable in A)

Translating $\Sigma_i^b(R)$ formulas to AC^0 formulas

Let R be binary relation, so $k=2$. (Same idea $\forall k$)

Let $A(a) \in \Sigma_i^b(R)$.

Corresponding propositional variables : $r_{i,j}$ $\quad i,j \in \mathbb{N}$

We define $[\![A(n)]\!]$ inductively:

(1) $A(a)$ quantifier-free, & doesn't contain R

Then $[\![A(n)]\!] = 1$ if $\overset{R}{A}(n)$ is valid, 0 otherwise

(2) $A(a)$ quantifier free, contains R.

Example. $A(a) = R(a, a+1) \vee R(2a, 4a)$

Then $[\![A(n)]\!] = r_{n,n+1} \vee r_{2n,4n}$

Translating $\Sigma_i^b(R)$ formulas to AC^0 formulas

Let R be binary relation, so $k=2$. (Same idea $\forall k$)

Let $A(a) \in \Sigma_i^b(R)$.

(3) $A(a) := \exists x \leq t(a)\ B(a, x)$

then $$[\![A(n)]\!] = \bigvee_{m \leq t(n)} [\![B(m)]\!]$$

(4) $A(a) := \forall x \leq t(a)\ B(a, x)$

then $$[\![A(n)]\!] = \bigwedge_{m \leq t(n)} [\![B(m)]\!]$$