Summary and Perspective

Deepak D'Souza

Department of Computer Science and Automation
Indian Institute of Science, Bangalore.

31 May 2021

Outline

Focus of Discussion

- Recap
- Models versus Proof Systems
- Truth in a fixed interpretation of interest
  - How do proof systems help?
- SMT solvers

Overview of what we did in the course: Part I

Proof Systems

- Proof systems for Propositional and First-Order Logic
  - Hilbert-style (Hilbert-Bernays), Resolution for PL
  - Hilbert-Bernays for ZOL (QF fragment of FOL)
  - Hilbert-Bernays for FOL.
- Prenex normal form, Existential, Universal fragments of FOL
- Soundness and Completeness
- Compactness, Lowenheim-Skolem

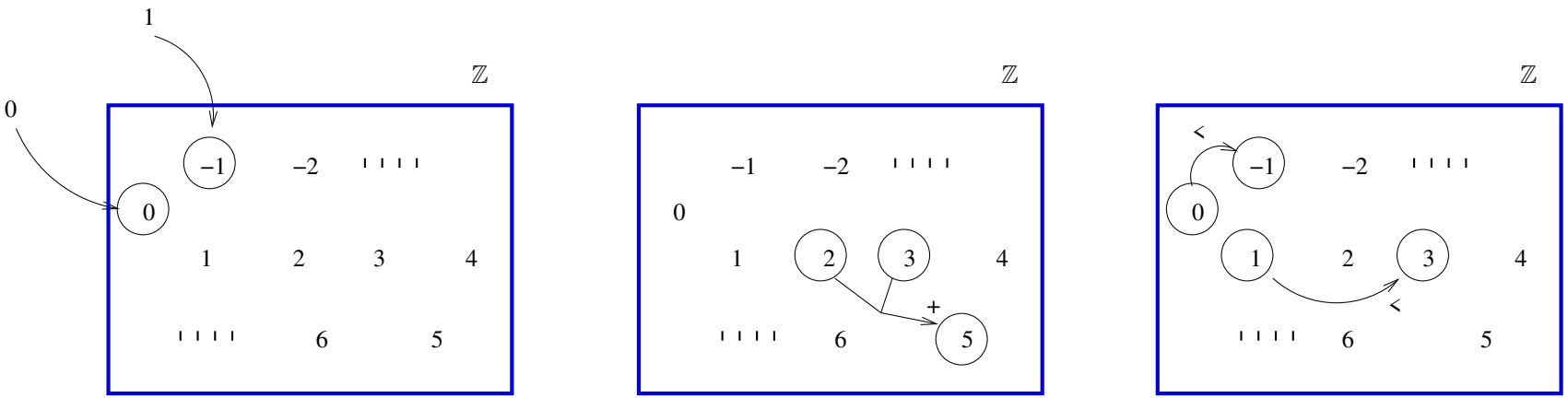
Overview of what we did in the course: Part II

Decision Procedures

- DPLL (or Conflict-Driven Clause Learning)
- Quantifier-Free logic of Equality and Uninterpreted Functions (EUF)
- Quantifier-Free logic of Linear Arithmetic (Reals and Itegers) (LA, LIA)
- Logic of Arrays (Array Property Fragment)
- Constrained Horn Clauses (CHCs)
- Model-Based Projection

Semantics of FOL

- Signature $\Sigma = (+, <, 0, 1)$
- What is a model for this signature? $M = (D, I)$.



- Need assignment or valuation for variables v, to give meaning to formulas.

$$(D, I), v \vDash \varphi$$

- Satisfiable?
- Valid?

Completeness

Two key notions:

- φ is a logical consequence of a set of sentences X: $X \models \varphi$, and validity: $\models \varphi$.
- φ is provable in a proof system (like HB) from a set of formulas X: $X \vdash \varphi$, and provability: $\vdash \varphi$.

Theorem (Completeness)

The Hilbert-Bernays proof system for FOL is complete: If $\models \varphi$ (i.e. φ is valid) then $\vdash \varphi$ (i.e. φ is provable in HB proof system).

Theorem (Strong Completeness)

The Hilbert-Bernays proof system for FOL is strongly complete: If $X \models \varphi$ (i.e. φ is logical consequence of a set of sentences X) then $X \vdash \varphi$ (i.e. φ is provable from X in HB proof system).

Satisfiability and Consistency

- φ is satisfiable if there exists a model M satisfying φ.
- φ is consistent if $\{\varphi\} \nvdash \mathit{false}$.

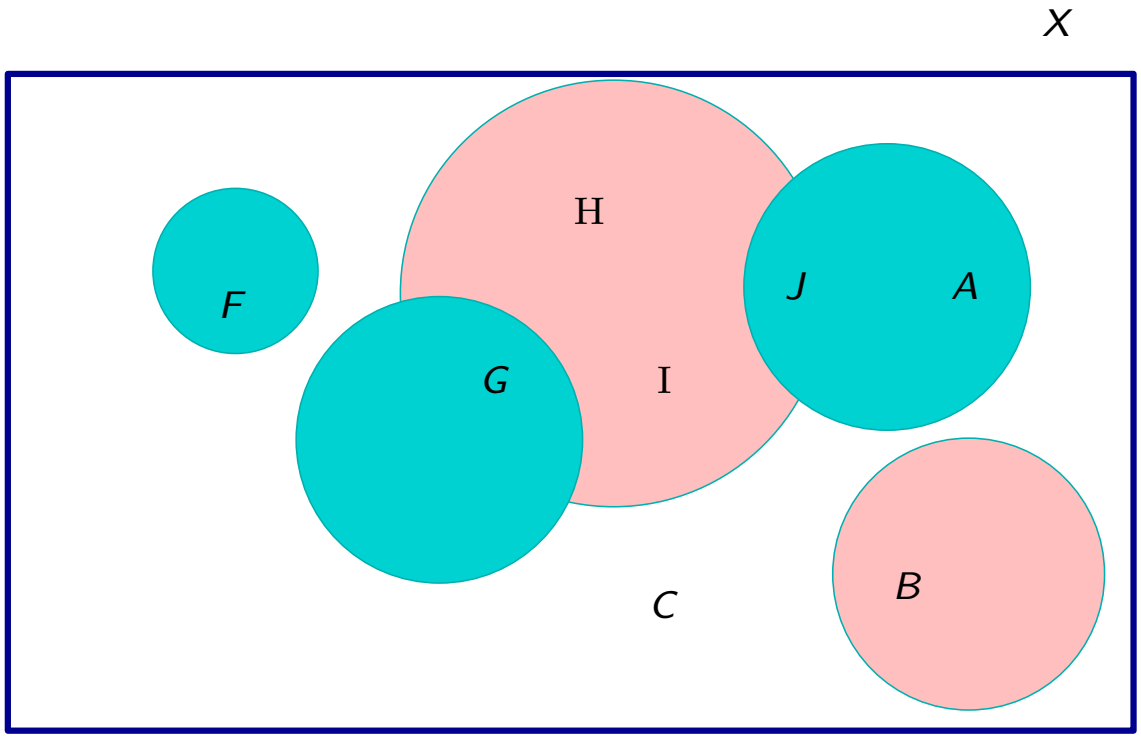
Theorem

φ is satisfiable iff φ is consistent

Compactness

Theorem

A (possibly infinite) set of FO formulas X is (simultaneously) satisfiable iff every finite subset of X is satisfiable.



An application of Compactness

If a set of FO formulas S is satisfiable in arbitrarily large finite models, it must be satisfiable in an infinite model.

- Construct FO formulas A_k which say that "there are at least k elements in the domain."
- Consider $S^* = S \cup \{A_1, A_2, \ldots\}$
- Every finite subset of S^* is satisfiable.
- By compactness, S^* is satisfiable in a model $M = (D, I)$.
- But clearly D must be infinite.

Corollary: There does not exist a set of FO sentences that characterize *finiteness* of the domain.

Proving Compactness using Proof Systems

Theorem

A (possibly infinite) set of FO formulas X is (simultaneously) satisfiable iff every finite subset of X is satisfiable.

- Suppose X were not satisfiable.
- Then X must be inconsistent (Using X consistent iff satisfiable).
- So $X \vdash \mathit{false}$ in the proof system (meaning of inconsistent).
- But then we should be able to derive *false* using a finite subset X_0 of X (proof is a finite sequence of formulas)
- Hence $X_0 \vdash \mathit{false}$.
- Hence X_0 is unsatisfiable (using X_0 inconsistent, and consistent iff sat).

Lowenheim-Skolem Theorems

Theorem (Lowenheim)

If a formula F is satisfiable, it is satisfiable in a countable model.

Exercise: Give a countable model for the formula which expresses "denseness" of the $<$-ordering:

$$\forall x \forall y (x < y \implies \exists z (x < z < y))$$

Theorem (Lowenheim-Skolem)

If a set of sentences S is satisfiable, it is satisfiable in a countable model.

An application: There does not exist a set of FO sentences S which characterize the domain of real numbers (i.e. S is satisfied in a model $M = (D, I)$ iff $D = \mathbb{R}$).

Fixed Interpretations

We are often interested in satisfiability and validity in a fixed model (or a fixed class of models) of interpretation:

- Equality Logic (models with interpretation of "$=$" fixed)
- FOL of Groups (models with interpretation of $\circ$ satisfying group axioms)
- FOL of linear arithmetic (single model with domain $\mathbb{R}$)
- FOL of arithmetic (single model with domain $\mathbb{Z}$)

Theories

- The FO theory of linear arithmetic is the set of all sentences of $\Sigma_{LA} = (+^{(2)}, -^{(2)}, <^{(2)}, 0, 1)$ that are true when interpreted in the intended model of $D = \mathbb{R}$, $+$, $-$, $<$ and 0, 1 as intended.
- The FO theory of groups is the set of all sentences over $\Sigma_G = (=^{(2)}, \circ^{(2)}, e)$, that are valid across the class of models where the interpretation of $\circ$ satisfies the group axioms.

A possible way to use proof systems: Try to capture the characteristics of a fixed class of models by a set of axioms $\mathcal{A}$.

Equality Logic

$\Sigma_E = (=^{(2)}, f^{(2)}, p^{(2)}, \ldots)$.

T_E is:

$$\forall x(x = x) \tag{1}$$

$$\forall x \forall y((x = y) \implies (y = x)) \tag{2}$$

$$\forall x \forall y((x = y) \wedge (y = z) \implies (x = z)) \tag{3}$$

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2((x_1 = y_1 \wedge x_2 = y_2) \implies f(x_1, x_2) = f(y_1, y_2)) \tag{4}$$

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2((x_1 = y_1 \wedge x_2 = y_2) \implies (p(x_1, x_2) \Leftrightarrow p(y_1, y_2))) \tag{5}$$

Groups

$\Sigma_G = (=^{(2)}, \circ^{(2)}, e)$.

T_G is:

$$\forall x \forall y \forall z((x \circ y) \circ z = x \circ (y \circ z)) \quad (1)$$

$$\forall x(x \circ e = x = e \circ x) \quad (2)$$

$$\forall x \exists x'(x \circ x' = e = x' \circ x) \quad (3)$$

Peano's Proof System for Arithmetic (1889)

$\Sigma_{PA} = (+^{(2)}, .^{(2)}, <^{(2)}, 0, 1)$.

T_{PA} is:

$$\forall x \neg(0 = x + 1) \tag{1}$$
$$\forall x \forall y (x + 1 = y + 1 \implies x = y) \tag{2}$$
$$\forall x (x + 0 = x) \tag{3}$$
$$\forall x \forall y \forall z (x + (y + z) = (x + y) + z) \tag{4}$$
$$\forall x (x \cdot 0 = 0) \tag{5}$$
$$\forall x \forall y \forall z (x \cdot (y + z) = ((x \cdot y) + (x \cdot z))) \tag{6}$$
$$(\varphi(0) \wedge \forall x (\varphi(x) \implies \varphi(x + 1))) \implies \forall x \varphi(x). \tag{7}$$

Using Proof Systems

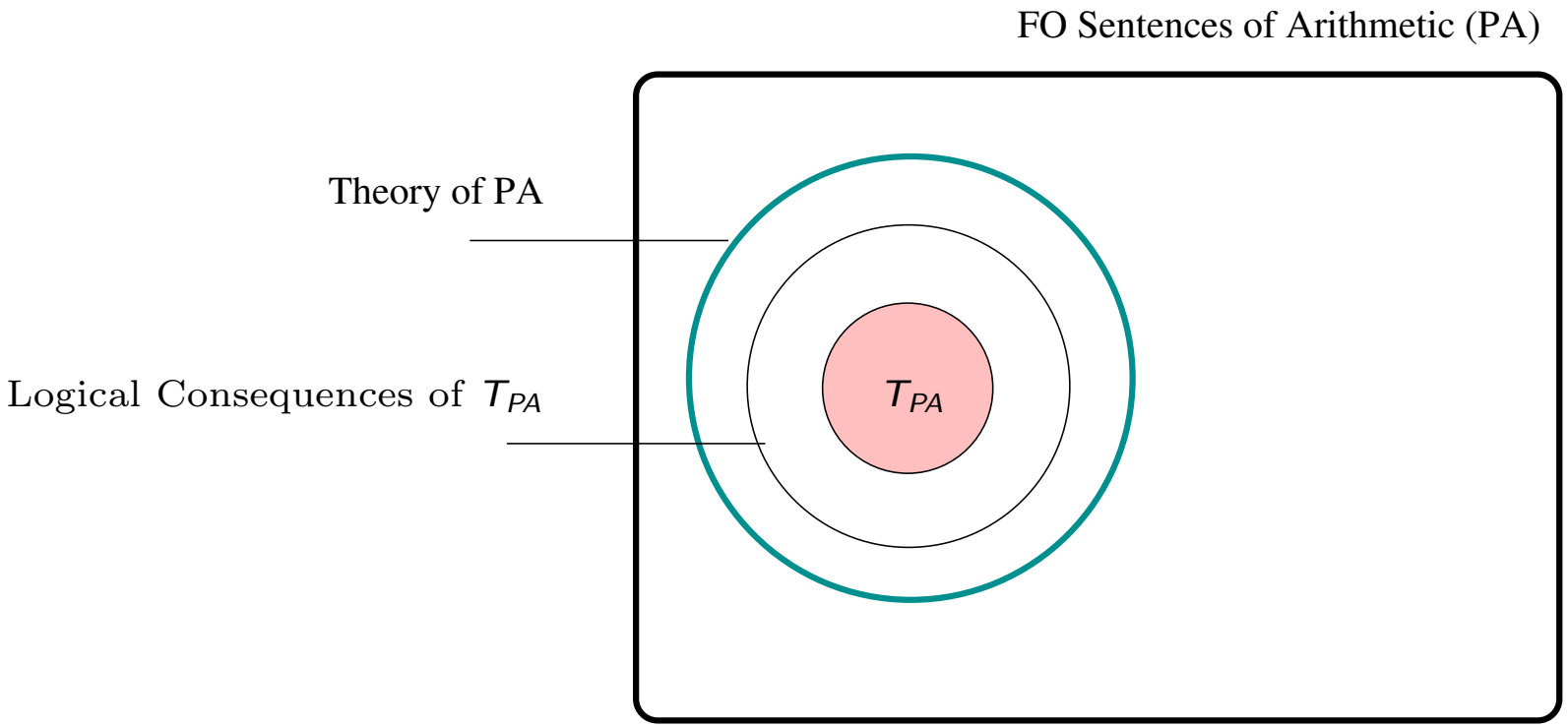
- Suppose we (magically!) knew that the set of logical consequences of a set of axioms $T_{\mathcal{C}}$ was exactly the set of $\mathcal{C}$-valid sentences.
- To check if φ is valid for $\mathcal{C}$, we could ask if

$$\mathcal{A} \vdash \varphi.$$

- By Strong Completeness of the proof system, this is equivalent to $\mathcal{A} \models \varphi$.
- This gives us a semi-decision procedure for $\mathcal{C}$-validity.

Some Problems with doing this

The inherent gap between theory of arithmetic and logical consequencs of T_{PA} (or any other "finitely described" sound set of axioms), from Gödel's Incompleteness Theorem:



SMT Solvers

SMT = Satisfiability Modulo Theories = DPLL(T).