LAST LECTURE

- Semantic Argument-based method for Validity of FOL Formula
  - Can it be directly used for checking satisfiability of FOL Formula? No. Consider the formula $\forall x . \exists y . p(x, y)$. Applying the proof rules will result in an interpretation which is not satisfying.
- Why do we insist on fresh values in some proof rules?
  - Example in class: $\exists x . \exists y . \exists z . p(x, y) \land \neg p(x, z)$.
- Prenex Normal Form
  - Is $\forall x . \exists y . p(x, y) \Leftrightarrow \exists y . \forall x . p(x, y)$?
  - What about $\forall x . \exists y . p(x) \land q(y)$ and $\exists y . \forall x . p(x) \land q(y)$?

SATISFIABILITY MODULO THEORIES (SMT)

SMT - INTRODUCTION

- In FOL, predicates and functions are in general uninterpreted
- In practice, we may have a specific meaning in mind for certain predicates and functions (e.g. $=$, $\leq$, $+$, etc.)
- First-order Theories allow us to formalise the meaning of certain structures.

FIRST-ORDER THEORY

- A First-order Theory (T) is defined by two components:
  - Signature (Σ_T) : Contains constant, predicate and function symbols
  - Axioms (A_T) : Set of closed FOL formulae containing only the symbols in Σ_T
- A Σ_T–formula is a normal FOL formula which only contains symbols from Σ_T

SATISFIABILITY AND VALIDITY

MODULO THEORIES

- An interpretation I is called a $T-$interpretation if it satisfies all the axioms of the theory T
    - For all $A \in A_T$, $I \vDash A$
- A Σ_T-formula F is satisfiable modulo T if there is a $T-$interpretation that satisfies F
- A Σ_T-formula F is valid modulo T if every $T-$interpretation satisfies F
    - Also denoted as $T \vDash F$

ENTAILS

SATISFIABILITY AND VALIDITY

MODULO THEORIES

- Which is of the following holds?
  - F is satisfiable ⇒ F is satisfiable modulo T
  - F is satisfiable modulo T ⇒ F is satisfiable
- Which is of the following holds?
  - F is valid ⇒ F is valid modulo T
  - F is valid modulo T ⇒ F is valid

COMPLETENESS AND DECIDABILITY

- A theory T is complete if for every closed formula F, either F or ¬F is valid modulo T
  - $T \models F$ or $T \models \neg F$
- Is FOL (i.e.'empty' theory) complete?
  - No. Consider $F : \exists x\,.\,p(x)$. Neither F nor $\neg F$ is valid.
- A theory T is decidable if $T \models F$ is decidable for every formula F.
- Even though FOL (or empty theory) is undecidable, various useful theories are actually decidable.

PRESBURGER ARITHMETIC ($T_{\mathbb{N}}$)

THE THEORY OF NATURAL NUMBERS

- Signature, $\Sigma_{\mathbb{N}} : 0{,}1, + \, , =$
  - $0{,}1$ are constants
  - + is a binary function
  - = is a binary predicate.
- Axioms:

1.	$\forall x.\ \neg(x + 1 = 0)$	(zero)
2.	$\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$	(successor)
3.	$F[0] \ \wedge\ (\forall x.\ F[x] \rightarrow F[x + 1]) \ \rightarrow\ \forall x.\ F[x]$	(induction)
4.	$\forall x.\ x + 0 = x$	(plus zero)
5.	$\forall x, y.\ x + (y + 1) = (x + y) + 1$	(plus successor)

PRESBURGER ARITHMETIC

INTERPRETATION

1. $\forall x.\ \neg(x + 1 = 0)$	(zero)
2. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow \ x = y$	(successor)
3. $F[0] \ \wedge \ (\forall x.\ F[x] \rightarrow F[x + 1]) \ \rightarrow \ \forall x.\ F[x]$	(induction)
4. $\forall x.\ x + 0 = x$	(plus zero)
5. $\forall x, y.\ x + (y + 1) = (x + y) + 1$	(plus successor)

- The intended $T_{\mathbb{N}}$−interpretation is $\mathbb{N}$, the set of natural numbers
- Does there exist a finite subset of $\mathbb{N}$ which is also a $T_{\mathbb{N}}$−interpretation?
  - Which axiom will be violated by any finite subset?
- Are negative numbers allowed by the axioms?