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 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

QUESTIONS

- 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
    - $T \vDash F$ or $T \vDash \neg F$
- 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 $T \vDash F$ is decidable for every formula F.
- Even though FOL (or empty theory) is undecidable, various useful theories are actually decidable.

THEORY OF EQUALITY ($T_=$)

- One of the simplest first-order theories
  - $\Sigma_=$: All symbols used in FOL and the special symbol $=$
  - Allows uninterpreted functions and predicates, but $=$ is interpreted.
- Axioms of Equality:

1. $\forall x.\ x = x$	(reflexivity)
2. $\forall x, y.\ x = y \ \rightarrow\ y = x$	(symmetry)
3. $\forall x, y, z.\ x = y \ \wedge\ y = z \ \rightarrow\ x = z$	(transitivity)

AXIOMS OF EQUALITY

- Function Congruence: For a n-ary function f, two terms $f(\overrightarrow{x})$ and $f(\overrightarrow{y})$ are equal if $\overrightarrow{x}$ and $\overrightarrow{y}$ are equal:

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow f(\overline{x}) = f(\overline{y})$$

- Predicate Congruence: For a n-ary predicate p, two formulas $p(\overrightarrow{x})$ and $p(\overrightarrow{y})$ are equivalent if $\overrightarrow{x}$ and $\overrightarrow{y}$ are equal:

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow (p(\overline{x}) \leftrightarrow p(\overline{y}))$$

AXIOMS OF EQUALITY

- Function Congruence and Predicate Congruence are actually Axiom Schemes, which can be instantiated with any function or predicate to get axioms.
- For example, for a unary function g, the function congruence axiom is:
  - $\forall x, y \,.\, x = y \rightarrow g(x) = g(y)$