SMT (Satisfiability modulo a theory T)

Theory T: set of closed formulas closed under implication ($\models$)

φ T-valid iff for all T-interpretations I, $\varphi \in I$ iff $\varphi \in T$
($\forall \varphi \in T.\ I \models \varphi$)

φ T-satisfiable iff exists T-interpretation I s.t. $I \models \varphi$

Note: φ T-valid iff $\neg\varphi$ not T-satisfiable

φ_1, φ_2 T-equivalent iff for all T-interpretations I, $I \models \varphi_1$ iff $I \models \varphi_2$

Note: φ_1, φ_2 T-equivalent iff $\varphi_1 \Leftrightarrow \varphi_2$ T-valid.

Semantic def of T: $T = \{\varphi \mid I \models \varphi\}$ for a specified model I (e.g. $I = (\mathbb{N}, 0, S, +, \ldots)$)

Syntactic def of T: $T = \{\varphi \mid A \models \varphi\}$ for a specified recursive set A of axioms

In case (b), we have sound + complete proof systems for T (proof system for FO + axioms A)

T consistent if exists I s.t. $I \models T$ (note the theory T_I = set of all Σ-formulas is the only inconsistent theory)
("largest theory")

("smallest theory" $T_\emptyset$ = valid formulas of FO) (given Σ, empty set of axioms)

T complete if for all Σ-formulas φ, either $\varphi \in T$ or $\neg\varphi \in T$.
$\Sigma = \{P\}$

$\forall x\, P(x) \notin T_\emptyset$
$\neg \forall x\, P(x) \notin T_\emptyset$

In case (a), T is always complete.
In case (b), if T is complete, then T is decidable.

theories of equality = bina... symbol ("interpret...

Theories of equality $=$ binary predicate symbol ("interpreted"), F other function + P predicate symbols ("uninterpreted")

Axioms (1) $=$ is an equivalence relation
$\forall x.\ x=x$
$\forall xy.\ x=y \Rightarrow y=x$
$\forall xyz\ x=y \Rightarrow y=z \Rightarrow x=z$

(2) $=$ is a congruence wrt all functions + pred symbols: for all $f\in F$, $\forall x_1,\dots x_n, y_1,\dots y_n\ \ x_1=y_1 \wedge \dots \wedge x_n=y_n \Rightarrow f(x_1,\dots x_n)=f(y_1,\dots y_n)$
for all $p\in P$, $\forall x_1,\dots x_n, y_1,\dots y_n\ \ "\ \ \wedge p(x_1,\dots x_n) \Rightarrow p(y_1,\dots y_n)$

- undecidable (like FOL)
- quantifier-free fragment decidable
  - in general satisfiability NP-complete
  - conjunctive of literals $O(n \cdot \log n)$ (vs. $O(n)$ in prop logic)

$O(n\cdot\log n)$ ← congruence closure: check satisfiability of conj of formulas of form $s=t$ and $s\neq t$ (2 terms)

Example $f^3(a)=a \wedge f^5(a)=a \wedge f(a)\neq a$

Congruence closure
- set of subterms $\{a\}, \{fa\}, \{f^2a\}, \{f^3a\}, \{f^4a\}, \{f^5a\}$
- (1) put all into different equiv classes
- (2) iteratively merge equiv classes if required by a equality conjunct

$\{a, f^3a\}, \{fa, f^4a\}, \{f^2a, f^5a\}$
$\{a, f^2a, f^3a, f^5a\}, \{fa, f^4a\}$

Thm: write this alg precisely and argue its $O(n\log n)$ (use "union-find" data structure)

Theories of equality = binary predicate symbol $=$ ("interpreted"), any other function F + predicate symbols P ("uninterpreted")

Axioms (1) $=$ is an equivalence relation
$\forall x.\ x=x$
$\forall xy.\ x=y \Rightarrow y=x$
$\forall xyz\ x=y \Rightarrow y=z \Rightarrow x=z$

(2) $=$ is a congruence wrt all function + pred symbols: for all $f \in F$, $\forall x_1,\dots x_n, y_1,\dots y_n \quad x_1=y_1 \wedge \dots \wedge x_n=y_n \Rightarrow f(x_1,\dots x_n)=f(y_1,\dots y_n)$
for all $p \in P$, $\forall x_1,\dots x_n, y_1,\dots y_n$. "

- undecidable (like FOL)

Congruence closure — set of subterms $\{a\}, \{fa\}, \{f^2a\}, \{f^3a\}, \{f^4a\}, \{f^5a\}$
(1) Put all into different equiv classes
(2) iteratively merge equiv classes if required by a equality conjunct
$\{a, f^3a\}, \{fa, f^4a\}, \{f^2a, f^5a\}$
$\{a, f^2a, f^3a, f^5a\}, \{fa, f^4a\}$

Arithmetic: theories over $\mathbb{N}$
Signature: $(0, S, =, +, \cdot)$

Presburger arithmetic (T_A) is given by the axioms: + axioms for $=$ (PR)

$\forall x.\ S(x) \neq 0$
$\forall xy.\ S(x)=S(y) \Rightarrow x=y$
induction axioms → $\varphi(0) \wedge \forall x.\ (\varphi(x) \Rightarrow \varphi(S(x))) \Rightarrow \forall x.\ \varphi(x)$

$\forall x.\ x+0=x$
$\forall xy.\ x+S(y)=S(x+y)$
$\forall x.\ x \cdot 0 = 0$
$\forall xy.\ x \cdot S(y) = x \cdot y + x$

PR = decidable and complete = $\{\varphi \mid (\mathbb{N}, 0, S, =, +) \models \varphi\}$
(between 2EXPSPACE and 3EXP)

Gödel's incompleteness thm There is no set A of axioms that s.t. T_A is complete
For every (recursive) set A of axioms, there exists a formula φ that is true in $(\mathbb{N}, 0, S, =, +, \cdot)$ but cannot be proved / equivalently does not follow from the axioms.

$T_A = \{\varphi \mid (\mathbb{N}, \dots) \models \varphi\}$

$\varphi =$ "$\forall \varphi$"

need rich enough theory to encode proofs (sequences of wffs) in particular, in $(\mathbb{N}, \dots +, \cdot)$ you can encode this by prime factorization (use Gödel numbers)

need multiplication