Formalisms
Every Computer Scientist Should Know

Thomas A. Henzinger

November 20, 2024

# 1 Preliminaries

An *alphabet* is a recursive set. A *preorder* is a binary relation that is reflexive and transitive. Given a function $f : A \to B$ and two elements $a \in A$ and $b \in B$, we write $f[a \mapsto b]$ for the function from $A$ to $B$ that agrees with $f$ except that $a$ is mapped to $b$. We write "iff" for "if and only if." Let $\mathbb{B} = \{\mathbf{true}, \mathbf{false}\}$.

# 2 Logic

## 2.1 Propositional Logic

### Syntax

Let $P_0$ be an alphabet of *propositions* not containing the special symbol $\bot$. The *propositional sentences* $\Phi$ are defined inductively:

$P_0 \subseteq \Phi$
$\bot \in \Phi$
$\Phi \times \{\Rightarrow\} \times \Phi \subseteq \Phi$

We write $(\varphi_1 \Rightarrow \varphi_2)$ for $(\varphi_1, \Rightarrow, \varphi_2)$ and use the following abbreviations in sentences:

$\neg\varphi$ for $\varphi \Rightarrow \bot$
$\varphi_1 \vee \varphi_2$ for $(\neg\varphi_1) \Rightarrow \varphi_2$
$\varphi_1 \wedge \varphi_2$ for $\neg(\varphi_1 \Rightarrow \neg\varphi_2)$
$\varphi_1 \Leftrightarrow \varphi_2$ for $(\varphi_1 \Rightarrow \varphi_2) \wedge (\varphi_2 \Rightarrow \varphi_1)$

When writing sentences, we omit parentheses whenever this can be done without ambiguity. We write $\varphi_1 \Rightarrow \varphi_2 \Rightarrow \varphi_3$ for $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \varphi_3)$.

### Classical semantics

A *boolean interpretation* $\nu : P_0 \to \mathbb{B}$ is a function that maps each proposition to a boolean value. Given a boolean interpretation $\nu$, the semantics of propositional sentences is defined inductively:

$[\![p]\!]_\nu = \nu(p)$ for $p \in P_0$
$[\![\bot]\!]_\nu = \mathbf{false}$
$[\![\varphi_1 \Rightarrow \varphi_2]\!]_\nu =$ if $[\![\varphi_1]\!]_\nu$ then $[\![\varphi_2]\!]_\nu$ else $\mathbf{true}$

Therefore:

$[\![\neg\varphi]\!]_\nu =$ if $[\![\varphi]\!]_\nu$ then $\mathbf{false}$ else $\mathbf{true}$
$[\![\varphi_1 \vee \varphi_2]\!]_\nu =$ if $[\![\varphi_1]\!]_\nu$ then $\mathbf{true}$ else $[\![\varphi_2]\!]_\nu$
$[\![\varphi_1 \wedge \varphi_2]\!]_\nu =$ if $[\![\varphi_1]\!]_\nu$ then $[\![\varphi_2]\!]_\nu$ else $\mathbf{false}$
$[\![\varphi_1 \Leftrightarrow \varphi_2]\!]_\nu =$ if $([\![\varphi_1]\!]_\nu = [\![\varphi_2]\!]_\nu)$ then $\mathbf{true}$ else $\mathbf{false}$

An interpretation $\nu$ is a *model* of a sentence $\varphi$ if $[\![\varphi]\!]_\nu = \mathbf{true}$. A sentence $\varphi$ is *valid* if every interpretation is a model of $\varphi$, and $\varphi$ is *satisfiable* if it has a model. A sentence $\varphi_1$ *implies* a sentence $\varphi_2$ if every model of $\varphi_1$ is a model of $\varphi_2$, and $\varphi_1$ is *equivalent* to $\varphi_2$ if they have the same models. Note that $\varphi$ is valid iff $\neg\varphi$ is not satisfiable (a.k.a. "unsatisfiable"); that $\varphi_1 \Rightarrow \varphi_2$ is valid iff $\varphi_1$ implies $\varphi_2$; and that $\varphi_1 \Leftrightarrow \varphi_2$ is valid iff $\varphi_1$ is equivalent to $\varphi_2$.

### Intuitionistic semantics

A *Kripke interpretation* $\nu = (W, w_0, \leq, [\cdot])$ consists of a set $W$ of worlds, an initial world $w_0 \in W$, a preorder $\leq$ on the worlds $W$, and a function $[\cdot]$ that maps each world $w \in W$ to a boolean interpretation $[w] : P_0 \to \mathbb{B}$ such that for all worlds $w, w' \in W$ and all propositions $p \in P_0$, if $[w](p) = \mathbf{true}$ and $w \leq w'$, then $[w'](p) = \mathbf{true}$. Given a Kripke interpretation $\nu$, the semantics of propositional sentences is defined inductively for each world $w \in W$:

$[\![p]\!]_\nu^w = [w](p)$
$[\![\bot]\!]_\nu^w = \mathbf{false}$
$[\![\varphi_1 \Rightarrow \varphi_2]\!]_\nu^w =$ (for all $w' \in W$ : if $w \leq w'$ then if $[\![\varphi_1]\!]_\nu^{w'}$ then $[\![\varphi_2]\!]_\nu^{w'}$)

The truth value of a sentence $\varphi$ for the Kripke interpretation $\nu$ is $[\![\varphi]\!]_\nu = [\![\varphi]\!]_\nu^{w_0}$. Note that the sentence $p \vee \neg p$ is false for the two-world interpretation

$$(\{w_0, w_1\}, w_0, \{(w_0, w_0), (w_0, w_1)), (w_1, w_1)\}, [\cdot])$$

with $[w_0](p) = \mathbf{false}$ and $[w_1](p) = \mathbf{true}$.

### Decision problems

Validity and satisfiability are complementary questions: validity ("Is a given sentence true for all interpretations?") is universal; satisfiability ("Is a given sentence true for some interpretation?") is existential. The satisfiability problem for the boolean semantics of propositional sentences is NP-complete; the corresponding validity problem is coNP-complete. The satisfiability and validity problems for the Kripke semantics of propositional sentences are PSPACE-complete (note that PSPACE = coPSPACE).

The brute-force procedure for deciding boolean satisfiability evaluates a given sentence $\varphi$ for all boolean interpretations. Let $n = |\varphi|$ be the size of $\varphi$.

While the computation of the truth value $[\![\varphi]\!]_\nu$ can be computed in $O(n)$ time for each boolean interpretation $\nu$, there may be $\Omega(2^n)$ many boolean interpretations to consider. In practice, the resolution procedure is often more efficient. In resolution, we assume that $\varphi$ is given in *conjunctive normal form* (CNF), as a conjunction of disjunctions of propositions and negated propositions. A propositional sentence $\varphi$ can be converted into an equivalent CNF sentence in $O(2^n)$ time. To avoid the duplication and reordering of expressions within a sentence, we write a CNF sentence as a *set* of *clauses*, each representing a disjunctive sentence, and we write a clause as a set of *literals*, each being a proposition or negated proposition.

```
Algorithm PROPOSITIONAL RESOLUTION
Input: propositional sentence φ in CNF
Output: if φ satisfiable then YES else NO
while ∅ ∉ φ and exist γ1, γ2 ∈ φ and α ∈ γ1 such that ¬α ∈ γ2 do
    φ := φ ∪ {γ1 ∪ γ2}\{α, ¬α}
    od
return if ∅ ∈ φ then NO else YES
```

TODO DPLL

### Proof systems

A *proof system* $\mathcal{P} = (\mathcal{J}, \mathcal{R})$ comprises a recursive set $\mathcal{J}$ of *judgments* and a recursive set $\mathcal{R}$ of *rules*; each rule in $\mathcal{R}$ consists of a finite (possibly zero) number of premises in $\mathcal{J}$ and a conclusion in $\mathcal{J}$. A *proof* in $\mathcal{P}$ is a finite sequence $J_0, J_1, \ldots, J_k$ of judgments $J_i \in \mathcal{J}$ such that for all $0 \leq i \leq k$, there is a rule $R_i \in \mathcal{R}$ whose conclusion is $J_i$ and whose premises occur earlier in the sequence. Note that the first judgment of a proof must be the conclusion of a rule without premises. A judgment $J$ is a *theorem* of $\mathcal{P}$ if there is a proof in $\mathcal{P}$ whose last judgment is $J$. Note that the set of theorems of $\mathcal{P}$ is r.e.

A *correctness* criterion $\mathcal{C} \subseteq \mathcal{J}$ identifies a set of correct judgments. A proof system $\mathcal{P}$ is *sound* w.r.t. $\mathcal{C}$ if every theorem is correct, and $\mathcal{P}$ is *complete* w.r.t. $\mathcal{C}$ if every correct judgment is a theorem. Note that the set of correct judgments is r.e. if there is a sound and complete proof system.

We present four proof systems for propositional logic, each with a different set of judgments and correctness criterion.

**Hilbert systems.** A *Hilbert* system has judgments of the form $\vdash \varphi$ for sentences $\varphi$. A judgment $\vdash \varphi$ is correct if the sentence $\varphi$ is valid. The Hilbert system HJ with the three rule schemata K, S, and MP ("modus ponens") is sound and complete for the Kripke semantics of propositional sentences:

$$\frac{}{\vdash \psi \Rightarrow \varphi \Rightarrow \psi}\ \mathrm{K}$$

$$\frac{}{\vdash (\psi \Rightarrow \varphi \Rightarrow \chi) \Rightarrow ((\psi \Rightarrow \varphi) \Rightarrow \psi \Rightarrow \chi)}\ \mathrm{S}$$

$$\frac{\vdash \varphi \quad \vdash \varphi \Rightarrow \psi}{\vdash \psi}\ \mathrm{MP}$$

We write the premises of a rule schema above a line, and the conclusion below; the schemata K and S have no premises, the schema MP has two premises. Each rule schema represents infinitely many rules that are obtained from the schema by substituting sentences for metavariables such as $\varphi$, $\psi$, and $\chi$. The Hilbert system HK = HJ+HX has in addition the rule schema HX ("excluded middle"):

$$\frac{}{\vdash ((\varphi \Rightarrow \bot) \Rightarrow \psi \Rightarrow \bot) \Rightarrow \psi \Rightarrow \varphi}\ \mathrm{HX}$$

The system HK is sound and complete for the boolean semantics of propositional sentences.

**Natural deduction.** A *Natural-Deduction* system has judgments of the form $\Gamma \vdash \varphi$, where $\Gamma$ is a finite set of sentences and $\varphi$ is a sentence. A judgment $\Gamma \vdash \varphi$ is correct if the conjunction of the sentences in $\Gamma$ implies $\varphi$. The Natural-Deduction system NJ, with the following rule schemata, is sound and complete for the Kripke semantics of propositional sentences:

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ \text{axiom}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ \bot\ \text{elimination} \qquad \frac{}{\Gamma \vdash \bot}\ \bot\ \text{introduction}$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \varphi \Rightarrow \psi}{\Gamma \vdash \psi}\ \Rightarrow\ \text{elimination} \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \Rightarrow \psi}\ \Rightarrow \text{introduction}$$

$$\frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ \wedge\mathrm{e} \qquad \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ \wedge\mathrm{i}$$

$$\frac{\Gamma \vdash \varphi_1 \vee \varphi_2 \quad \Gamma, \varphi_1 \vdash \psi \quad \Gamma, \varphi_2 \vdash \psi}{\Gamma \vdash \psi}\ \vee\mathrm{e} \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ \vee\mathrm{i}$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \neg\varphi}{\Gamma \vdash \bot}\ \neg\mathrm{e} \qquad \frac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi}\ \neg\mathrm{i}$$

The Natural-Deduction system NK = NJ+NX, with the additional excluded-middle schema NX, is sound and complete for the boolean semantics of propositional sentences:

$$\frac{}{\Gamma \vdash \varphi \vee \neg\varphi}\ \mathrm{NX}$$

**Gentzen systems.** A *Gentzen* system has judgments of the form $\Gamma \vdash \Delta$, where $\Gamma$ and $\Delta$ are finite sets of sentences. The sentences in $\Gamma$ and $\Delta$ are called *assertions* and *goals*, respectively; the judgment $\Gamma \vdash \Delta$, a *sequent*. A sequent $\Gamma \vdash \Delta$ is correct if the conjunction of the assertions implies the disjunction of the goals. Note that in natural deduction, all sequents have a single goal; moreover in Hilbert systems, there are no assertions. The Gentzen system LK, with the following rule schemata, is sound and complete for the boolean semantics of propositional sentences:

$$\frac{}{\Gamma, \varphi \vdash \varphi, \Delta}\ \text{axiom}$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot\text{e} \qquad \frac{}{\Gamma \vdash \top, \Delta}\ \top\text{i}$$

$$\frac{\Gamma \vdash \varphi, \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \Rightarrow \psi \vdash \Delta} \Rightarrow \text{e} \qquad \frac{\Gamma, \varphi \vdash \psi, \Delta}{\Gamma \vdash \varphi \Rightarrow \psi, \Delta} \Rightarrow \text{i}$$

$$\frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}\ \wedge\text{e} \qquad \frac{\Gamma \vdash \varphi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \varphi \wedge \psi, \Delta}\ \wedge\text{i}$$

$$\frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}\ \vee\text{e} \qquad \frac{\Gamma \vdash \varphi, \psi, \Delta}{\Gamma \vdash \varphi \vee \psi, \Delta}\ \vee\text{i}$$

$$\frac{\Gamma \vdash \varphi, \Delta}{\Gamma, \neg\varphi \vdash \Delta}\ \neg\text{e} \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \neg\varphi, \Delta}\ \neg\text{i}$$

Note the internal symmetries of LK in all but the $\Rightarrow$ rules.

### Metatheorems

**Deduction.** TODO

**Compactness.** TODO

**Cut elimination.** TODO

**Craig interpolation.** TODO

## 2.2 First-order Logic

### Syntax

Let $X$ be an infinite alphabet of *variables*. A *signature* $\Sigma = (F_i, P_i)_{i \in \mathbb{N}}$ comprises, for each natural number $i$, two alphabets $F_i$ and $P_i$ of *function* and *predicate* symbols of arity $i$. The function symbols of arity 0 are disjoint from $X$ and called *constants*; the predicate symbols of arity 0 are different from $\bot$ and called *propositions*. The $\Sigma$-*terms* $T$ are defined inductively:

$$X \subseteq T$$
$$F_i \times T^i \subseteq T \text{ for all } i \in \mathbb{N}$$

The $\Sigma$-*atoms* $A$ are defined inductively:

$$\bot \in A$$
$$P_i \times T^i \subseteq T \text{ for all } i \in \mathbb{N}$$

The $\Sigma$-*formulas* $\Phi$ are defined inductively:

$$A \subseteq \Phi$$
$$\Phi \times \{\Rightarrow\} \times \Phi \subseteq \Phi$$
$$\{\forall\} \times X \times \Phi \subseteq \Phi$$

We write $(\forall x : \varphi)$ for the universally quantified formula $(\forall, x, \varphi)$ with the *bound* variable $x$. The existentially quantified formula $(\exists x : \varphi)$ is an abbreviation for $\neg(\forall x : \neg\varphi)$. The *free* variables of terms, atoms, and formulas are defined inductively:

$free(x) = \{x\}$ for $x \in X$
$free(f_i, t_1, \ldots, t_i) = free(t_1) \cup \cdots \cup free(t_i)$ for $f_i \in F_i$
$free(\bot) = \emptyset$
$free(p_i, t_1, \ldots, t_i) = free(t_1) \cup \cdots \cup free(t_i)$ for $p_i \in P_i$
$free(\varphi_1 \Rightarrow \varphi_2) = free(\varphi_1) \cup free(\varphi_2)$
$free(\forall x : \varphi) = free(\varphi) \backslash \{x\}$

A $\Sigma$-formula $\varphi$ is a $\Sigma$-*sentence* if $free(\varphi) = \emptyset$. The *universal closure* of $\varphi$ is the $\Sigma$-sentence that results from $\varphi$ by adding outermost $\forall$-quantifiers.

### Semantics

We give only the classical (so-called Tarski) semantics for first-order sentences. A $\Sigma$-*interpretation* $\nu$ is a function with the domain $\{\forall\} \cup X \cup \bigcup_{i \in \mathbb{N}}(F_i \cup P_i)$:

$\nu(\forall) = \mathbf{U}$ for a nonempty set $\mathbf{U}$ called *universe*
$\nu(x) \in \mathbf{U}$ for each variable $x \in X$
$\nu(f_i) : \mathbf{U}^i \rightarrow \mathbf{U}$ for each function symbol $f_i \in F_i$
$\nu(p_i) \subseteq \mathbf{U}^i$ for each predicate symbol $p_i \in P_i$

Given a $\Sigma$-interpretation $\nu$, the semantics of terms, atoms, and formulas is defined inductively:

$[\![x]\!]_\nu = \nu(x)$ for $x \in X$
$[\![f_i, t_1, \ldots, t_i]\!]_\nu = \nu(f_i)([\![t_1]\!]_\nu, \ldots, [\![t_i]\!]_\nu)$ for $f_i \in F_i$;
$[\![\bot]\!]_\nu = \mathbf{false}$
$[\![p_i, t_1, \ldots, t_i]\!]_\nu$ = if $([\![t_1]\!]_\nu, \ldots, [\![t_i]\!]_\nu) \in \nu(p_i)$ then **true** else **false**
for $p_i \in P_i$
$[\![\varphi_1 \Rightarrow \varphi_2]\!]_\nu$ = if $[\![\varphi_1]\!]_\nu$ then $[\![\varphi_2]\!]_\nu$ else **true**
$[\![\forall x : \varphi]\!]_\nu$ = (for all $\mathbf{u} \in \mathbf{U} : [\![\varphi]\!]_{\nu[x \mapsto \mathbf{u}]} = \mathbf{true}$)

It follows that

$[\![\exists x : \varphi]\!]_\nu$ = (for some $\mathbf{u} \in \mathbf{U} : [\![\varphi]\!]_{\nu[x \mapsto \mathbf{u}]} = \mathbf{true}$).

Note that we can rename the bound variables in a formula $\varphi$ to new (so-called "fresh") variables without changing the semantics of $\varphi$. The definitions of model, validity, satisfiability, implication, and equivalence for $\Sigma$-sentences and $\Sigma$-interpretations are the same as for propositional sentences and boolean interpretations.

### Proof systems

First-order Hilbert judgments have the form $\vdash \varphi$ for $\Sigma$-formulas $\varphi$. A first-order judgment $\vdash \varphi$ is correct if the universal closure of $\varphi$ is valid. The Hilbert system HK has three additional rule schemata for first-order quantification:

$$\frac{}{\vdash (\forall x : \phi) \Rightarrow \varphi[x \mapsto t]}$$

$$\frac{}{\vdash \varphi \Rightarrow (\forall x : \varphi)} \text{ if } x \notin \mathit{free}(\varphi)$$

$$\frac{}{\vdash (\forall x : \varphi \Rightarrow \psi) \Rightarrow (\forall x : \varphi) \Rightarrow (\forall x : \psi)}$$

The formula $\varphi[x \mapsto t]$ is obtained as follows: first, all bound variables in $\varphi$ are renamed to variables not in $\mathit{free}(\varphi) \cup \{x\} \cup \mathit{free}(t)$; second, all occurrences of the variable $x$ in $\varphi$ are replaced by the term $t$. The renaming of the bound variables in $\varphi$ prevents the accidental "capturing" of free variables in $t$ by quantifiers in $\varphi$. The proof system HK is sound and complete for $\Sigma$-formulas; the latter is known as Gödel's completeness theorem. TODO NK, LK

### Metatheorems

TODO Löwenhein-Skolem, Craig, resolution

### Theories

We extend some definitions to *sets* of sentences and interpretations. An interpretation $\nu$ is a *model* of a set $T$ of sentences if $\nu$ is a model of every sentence in $T$. A set $T$ of sentences *implies* a sentence $\varphi$, written $T \vDash \varphi$, if every model of $T$ is a model of $\varphi$. A set $V$ of interpretations *models* a sentence $\varphi$, written $V \vDash \varphi$, if every interpretation in $V$ is a model of $\varphi$.

A set $T$ of $\Sigma$-sentences is a $\Sigma$-*theory* if $T$ is closed under implication, that is, for every $\Sigma$-sentence $\varphi$, if $T \vDash \varphi$ then $\varphi \in T$. A theory $T$ can be specified syntactically or semantically: a syntactically defined $T$ is $T_A = \{\varphi : A \vDash \varphi\}$ for a specified recursive set $A$ of $\Sigma$-sentences called *axioms*; a semantically defined $T$ is $T_V = \{\varphi : V \vDash \varphi\}$ for a specified set $V$ of $\Sigma$-interpretations. Note that both $T_A$ and $T_V$ are closed under implication.

Given a theory $T$, we can parametrize many definitions *modulo* $T$. A sentence $\varphi$ is $T$-*satisfiable* if $[\![\varphi]\!]_\nu = \mathbf{true}$ for some model $\nu$ of $T$. A sentence $\varphi_1$ is $T$-*equivalent* to a $\Sigma$-sentence $\varphi_2$ if $[\![\varphi_1]\!]_\nu = [\![\varphi_2]\!]_\nu$ for every model $\nu$ of $T$. Note that $\varphi \in T$ ("$\varphi$ is $T$-*valid*") iff $[\![\varphi]\!]_\nu = \mathbf{true}$ for every model $\nu$ of $T$; that $\neg\varphi \in T$ iff $\varphi$ is not $T$-satisfiable; and that $(\varphi_1 \Leftrightarrow \varphi_2) \in T$ iff $\varphi_1$ is $T$-equivalent to $\varphi_2$.

A $\Sigma$-theory $T$ is *consistent* if $T$ has a model, and *complete* if $T$ contains $\varphi$ or $\neg\varphi$ for every $\Sigma$-sentence $\varphi$. Note that there is only one inconsistent theory, namely, the theory $T_\bot$ that contains all $\Sigma$-sentences. The inconsistent theory $T_\bot$ can be defined syntactically by the single axiom $\bot$, or semantically by the empty set of interpretations. The inconsistent theory is trivially complete. While the inconsistent theory is the largest theory, the smallest theory $T_\emptyset$ contains only the valid $\Sigma$-sentences. The theory $T_\emptyset$ is first-order logic itself; it can be defined syntactically by the empty set of axioms, or semantically by the set of all $\Sigma$-interpretations. Note that $T_\emptyset$ is incomplete. An important class of theories are the theories that are defined semantically by a single interpretation; these theories are consistent and complete.

**Decision problems**

The validity problem for $\Sigma$-sentences is r.e. but not recursive; the satisfiability problem is co-r.e. but not recursive. However, there are interesting $\Sigma$-theories with decidable validity and satisfiability problems.

**Theories with equality.** A theory with equality contains the binary predicate symbol $=$ in $P_2$ and the following *equality axioms*:

> [reflexivity] $(\forall x : x = x)$
> [symmetry] $(\forall x, y : x = y \Rightarrow y = x)$
> [function congruence] $(\forall x_1, y_1, \ldots, x_i, y_i : x_1 = y_1 \wedge \cdots \wedge x_i = y_i \Rightarrow f_i(x_1, \ldots, x_i) = f_i(y_1, \ldots, y_i))$ for each $f_i \in F_i$
> [predicate congruence] $(\forall x_1, x_1, \ldots, x_i, y_i : x_1 = y_1 \wedge \cdots \wedge x_i = y_i \Rightarrow p_i(x_1, \ldots, x_i) \Rightarrow p_i(y_1, \ldots, y_i))$ for each $p_i \in P_i$

Note that the transitivity of $=$ follows from the congruence axiom for the equality predicate. The *theory of uninterpreted function and predicate symbols* $T_=$ has no other axioms. While the first-order theory $T_=$ is undecidable, the satisfiability problem is NP-complete for existentially quantified sentences (where all variables are quantified by outermost $\exists$), and the validity problem is coNP-complete for universally quantified sentences (where all variables are quantified by outermost $\forall$). The critical subroutine checks the $T_=$-satisfiability of a conjunction of the form

$$\varphi = (\bigwedge_{1 \leq j < m} s_j = t_j \wedge \bigwedge_{m \leq j < n} s_j \neq t_j).$$

This is done by computing the *congruence closure* on all subterms of the set $S = \{s_i, t_i : 1 \leq i < n\}$, which can be done in time $O(|\varphi| \cdot \log|\varphi|)$ using a union-find data structure.

**Arithmetic theories.** Consider the signature $\Sigma_{(0,S,+,\times)}$ with the constant 0, the unary function symbol $S$, the binary function symbols $+$ and $\times$, and the equality predicate. Let $\nu_{\mathbb{N}}$ be the $\Sigma_{(0,S,+,\times)}$-interpretation with the universe $\mathbb{N}$ which interprets $S$ as successor function (i.e., $\nu_{\mathbb{N}}(S)(\mathbf{n}) = \mathbf{n+1}$ for all $n \in \mathbb{N}$), and 0, $+$, $\times$ and $=$ are interpreted as zero, addition, multiplication, and equality on $\mathbb{N}$. *Arithmetic* is the theory $T_{\mathbb{N}} = \{\varphi : \{\nu_{\mathbb{N}}\} \vDash \varphi\}$ of $\Sigma_{(0,S,+,\times)}$-sentences that are true for the natural numbers. *Peano arithmetic* PA is an attempt to axiomatize arithmetic. The theory PA has, in addition to the equality axioms, the following axioms:

> [zero] $S0 \neq 0$
> [successor] $(\forall x, y : S(x) = S(y) \Rightarrow x = y)$
> [induction] $\varphi[x \mapsto 0] \Rightarrow (\forall x : \varphi \Rightarrow \varphi[x \mapsto S(x)]) \Rightarrow (\forall x : \varphi)$
> [zero-addition] $(\forall x : x + 0 = x)$
> [successor-addition] $(\forall x, y : x + S(y) = S(x + y))$
> [zero-multiplication] $(\forall x : x \times 0 = 0)$
> [successor-multiplication] $(\forall x, y : x \times S(y) = (x \times y) + x)$

Gödel's celebrated incompleteness theorem shows that for any set $A$ of axioms that are true for the natural numbers, such as PA, there exists a $\Sigma_{(0,S,+,\times)}$-sentence $\varphi_A$ such that neither $\varphi_A$ nor $\neg\varphi_A$ are implied by $A$, that is, the $\Sigma_{(0,S,+,\times)}$-theory $T_A$ is not complete. (Roughly speaking, the Gödel sentence $\varphi_A$ is self-reflexive and encodes the statement "$\nvdash \varphi$" that there is no proof of $\varphi_A$ from the axioms in $A$.) It follows that, while $\nu_{\mathbb{N}}$ is a model of PA, there are also other (so-called "nonstandard") models of PA. TODO Presburger

**Algebraic theories.** TODO

**Theories of data structures.** Bitvectors, arrays, lists. TODO

**Combination of theories.** TODO