Computer-Aided Program Design

Spring 2015, Rice University

Unit 5

Swarat Chaudhuri

March 20, 2015

First-Order Logic (FOL): Syntax

variables	$x, y, z, \cdots$
constants	$a, b, c, \cdots$
functions	$f, g, h, \cdots$
terms	variables, constants or n-ary function applied to n terms as arguments $a, x, f(a), g(x, b), f(g(x, g(b)))$
predicates	$p, q, r, \cdots$
atom	$\top$, $\bot$, or an n-ary predicate applied to n terms
literal	atom or its negation $p(f(x), g(x, f(x))), \quad \neg p(f(x), g(x, f(x)))$

Note: 0-ary functions: constant
0-ary predicates: $P, Q, R, \ldots$

FOL syntax: continued

quantifiers

existential quantifier $\exists x. F[x]$
"there exists an x such that $F[x]$"

universal quantifier $\forall x. F[x]$
"for all x, $F[x]$"

FOL formula literal, application of logical connectives ($\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$) to formulae,
or application of a quantifier to a formula

Example

FOL formula

$$\underbrace{\forall x.\ p(f(x), x)\ \rightarrow\ (\exists y.\ \underbrace{p(f(g(x,y)), g(x,y))}_{G})\ \wedge\ q(x, f(x))}_{F}$$

The scope of $\forall x$ is F. We say that x is *bound* by the quantifier.
The scope of $\exists y$ is G. We say that y is *bound* by the quantifier.
The formula reads:

“for all x,
if $p(f(x), x)$
then there exists a y such that
$p(f(g(x,y)), g(x,y))$ and $q(x, f(x))$”

Translations of English Sentences into FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

  $$\forall x, y, z.\ triangle(x, y, z) \rightarrow length(x) < length(y) + length(z)$$

Translations of English Sentences into FOL

- The length of one side of a triangle is less than the sum of the lengths of the other two sides

$$\forall x, y, z.\ triangle(x, y, z) \rightarrow length(x) < length(y) + length(z)$$

- Fermat's Last Theorem.

$$\begin{array}{l} \forall n.\ integer(n) \ \wedge \ n > 2 \\ \quad \rightarrow \ \forall x, y, z. \\ \qquad integer(x) \ \wedge \ integer(y) \ \wedge \ integer(z) \\ \qquad \wedge \ x > 0 \ \wedge \ y > 0 \ \wedge \ z > 0 \\ \qquad\quad \rightarrow \ x^n + y^n \neq z^n \end{array}$$

FOL Semantics

An interpretation $I : (D_I, \alpha_I)$ consists of:

- Domain D_I
  non-empty set of values or objects
  cardinality $|D_I|$ finite (eg, 52 cards),
  countably infinite (eg, integers), or
  uncountably infinite (eg, reals)
- Assignment α_I
  - each variable x assigned value $x_I \in D_I$
  - each n-ary function f assigned $f_I : D_I^n \rightarrow D_I$.
    In particular, each constant a (0-ary function) assigned value $a_I \in D_I$
  - each n-ary predicate p assigned $p_I : D_I^n \rightarrow \{\underline{\text{true}}, \underline{\text{false}}\}$.
    In particular, each propositional variable P (0-ary predicate) assigned truth value (<u>true</u>, <u>false</u>)

Example

$$F: \; p(f(x,y),z) \;\rightarrow\; p(y,g(z,x))$$

Interpretation $I : (D_I, \alpha_I)$:

- $D_I = \mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ integers
- $\alpha_I : \{f \mapsto +, g \mapsto -, p \mapsto >, x \mapsto 13, y \mapsto 42, z \mapsto 1\}$
- Let $F : x + y > z \;\rightarrow\; y > z - x$. Compute the truth value of F under I:

1.	I	$\models$	$x + y > z$	since $13 + 42 > 1$
2.	I	$\models$	$y > z - x$	since $42 > 1 - 13$
3.	I	$\models$	F	by 1, 2, and $\rightarrow$

F is <u>true</u> under I.

Semantics: Quantifiers

x variable.

<u>x-variant</u> of interpretation I is an interpretation $J : (D_J, \alpha_J)$ such that

- $D_I = D_J$
- $\alpha_I[y] = \alpha_J[y]$ for all symbols y, except possibly x

That is, I and J agree on everything except possibly the value of x

Denote $J : \ I \triangleleft \{x \mapsto \mathsf{v}\}$ the x-variant of I in which $\alpha_J[x] = \mathsf{v}$ for some $\mathsf{v} \in D_I$. Then

- $I \ \models \ \forall x.\ F$ iff for all $\mathsf{v} \in D_I$, $I \triangleleft \{x \mapsto \mathsf{v}\} \ \models \ F$
- $I \ \models \ \exists x.\ F$ iff there exists $\mathsf{v} \in D_I$ s.t. $I \triangleleft \{x \mapsto \mathsf{v}\} \ \models \ F$

Normal Forms

Negation Normal Forms (NNF)

Augment the equivalence with (left-to-right)

$$\neg \forall x.\ F[x] \ \Leftrightarrow\ \exists x.\ \neg F[x]$$

$$\neg \exists x.\ F[x] \ \Leftrightarrow\ \forall x.\ \neg F[x]$$

Prenex Normal Form (PNF)

All quantifiers appear at the beginning of the formula

$$Q_1 x_1 \cdots Q_n x_n.\ F[x_1, \cdots, x_n]$$

where $Q_i \in \{\forall,\ \exists\}$ and F is quantifier-free.

Every FOL formula F can be transformed to equivalent formula F' in PNF.

Example: Find equivalent PNF of

$$F:\ \forall x.\ \neg(\exists y.\ p(x, y)\ \wedge\ p(x, z))\ \vee\ \exists y.\ p(x, y)$$

Satisfiability and Validity

F is <u>satisfiable</u> iff there exists I s.t. $I \models F$
F is <u>valid</u> iff for all I, $I \models F$

$$F \text{ is valid iff } \neg F \text{ is unsatisfiable}$$

Proving validity: semantic argument method

$$F : \; (\forall x.\; p(x)) \;\leftrightarrow\; (\neg\exists x.\; \neg p(x)) \quad \text{valid?}$$

Suppose not. Then there is I s.t.

$$\begin{array}{lccc} 0. & I & \not\models & (\forall x.\; p(x)) \;\leftrightarrow\; (\neg\exists x.\; \neg p(x)) \end{array}$$

First case:

$$\begin{array}{lrcll}
1. & I & \models & \forall x.\; p(x) & \text{assumption} \\
2. & I & \not\models & \neg\exists x.\; \neg p(x) & \text{assumption} \\
3. & I & \models & \exists x.\; \neg p(x) & \text{2 and } \neg \\
4. & I \triangleleft \{x \mapsto \mathsf{v}\} & \models & \neg p(x) & \text{3 and } \exists\text{, for some } \mathsf{v} \in D_I \\
5. & I \triangleleft \{x \mapsto \mathsf{v}\} & \models & p(x) & \text{1 and } \forall
\end{array}$$

4 and 5 are contradictory.

Proving validity: semantic argument method

Second case:

1.	I	$\not\models$	$\forall x.\ p(x)$	assumption
2.	I	$\models$	$\neg\exists x.\ \neg p(x)$	assumption
3.	$I \triangleleft \{x \mapsto \mathsf{v}\}$	$\not\models$	$p(x)$	1 and $\forall$, for some $\mathsf{v} \in D_I$
4.	I	$\not\models$	$\exists x.\ \neg p(x)$	2 and $\neg$
5.	$I \triangleleft \{x \mapsto \mathsf{v}\}$	$\not\models$	$\neg p(x)$	4 and $\exists$
6.	$I \triangleleft \{x \mapsto \mathsf{v}\}$	$\models$	$p(x)$	5 and $\neg$

3 and 6 are contradictory.

Both cases end in contradictions for arbitrary I.

Therefore, F is valid.

Example: Show

$$F: \ (\forall x.\ p(x,x)) \ \rightarrow \ (\exists x.\ \forall y.\ p(x,y)) \quad \text{is invalid.}$$

Find interpretation I such that

$$I \ \models \ \neg[(\forall x.\ p(x,x)) \ \rightarrow \ (\exists x.\ \forall y.\ p(x,y))]$$

i.e.

$$I \ \models \ (\forall x.\ p(x,x)) \ \wedge \ \neg(\exists x.\ \forall y.\ p(x,y))$$

Choose $D_I = \{0,1\}$

$p_I = \{(0,0),\ (1,1)\}$ i.e. $p_I(0,0)$ and $p_I(1,1)$ are true

$p_I(1,0)$ and $p_I(1,0)$ are false

I falsifying interpretation $\Rightarrow$ F is invalid.

Decidability of FOL

- FOL is undecidable (Turing & Church)
  There does not exist an algorithm for deciding if a FOL formula F is valid, i.e. always halt and says "yes" if F is valid or say "no" if F is invalid.
- FOL is semi-decidable
  There is a procedure that always halts and says "yes" if F is valid, but may not halt if F is invalid.
  Or alternately, there is a procedure that always halts and says "yes" is F is unsatisfiable, but may not halt if F is satisfiable.

Why is satisfiability not detectable? Consider the formula

$$\forall x, y, z. \exists w. \quad \neg P(x,x) \wedge (P(x,y) \wedge P(y,z) \rightarrow P(x,z)) \wedge P(x,w).$$

A satisfiable formula of FOL may not have a finite model.

Semantic Argument Proof

To show FOL formula F is valid, assume $I \not\models F$ and derive a contradiction $I \models \bot$ in all branches

- Soundness
  If every branch of a semantic argument proof reaches $I \models \bot$, then F is valid
- Completeness
  Each valid formula F has a semantic argument proof in which every branch reaches $I \models \bot$

First-Order Theories

First-order theory T defined by

- Signature Σ - set of constant, function, and predicate symbols
- Set of axioms A_T - set of closed (no free variables) Σ-formulae

Σ-formula constructed of constants, functions, and predicate symbols from Σ, and variables, logical connectives, and quantifiers

The symbols of Σ are just symbols without prior meaning — the axioms of T provide their meaning.

Satisfiability and validity

- A Σ-formula F is valid in theory T (T-valid, also $T \models F$), if every interpretation I that satisfies the axioms of T,
  i.e. $I \models A$ for every $A \in A_T$ (T-interpretation)
  also satisfies F. In other words, $I \models F$
- A Σ-formula F is satisfiable in T (T-satisfiable), if there is a T-interpretation (i.e. satisfies all the axioms of T) that satisfies F
- Two formulae F_1 and F_2 are equivalent in T (T-equivalent), if $T \models F_1 \leftrightarrow F_2$,
  i.e. if for every T-interpretation I, $I \models F_1$ iff $I \models F_2$
- A fragment of theory T is a syntactically-restricted subset of formulae of the theory.
  Example: quantifier-free segment of theory T is the set of quantifier-free formulae in T.

Decidability

A theory T is <u>decidable</u> if $T \models F$ (T-validity) is decidable for every Σ-formula F,

i.e., there is an algorithm that always terminate with "yes", if F is T-valid, and "no", if F is T-invalid.

A fragment of T is <u>decidable</u> if $T \models F$ is decidable for every Σ-formula F in the fragment.

Theory of Equality T_E

Signature

$$\Sigma_{=} : \{=, a, b, c, \cdots, f, g, h, \cdots, p, q, r, \cdots\}$$

consists of

- $=$, a binary predicate, interpreted by axioms.
- all constant, function, and predicate symbols.

Theory of Equality T_E

Axioms of T_E

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)
4. for each positive integer n and n-ary function symbol f, $\forall x_1, \ldots, x_n, y_1, \ldots, y_n.\ \bigwedge_i x_i = y_i \ \rightarrow\ f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ (congruence)
5. for each positive integer n and n-ary predicate symbol p, $\forall x_1, \ldots, x_n, y_1, \ldots, y_n.\ \bigwedge_i x_i = y_i \ \rightarrow\ (p(x_1, \ldots, x_n) \leftrightarrow p(y_1, \ldots, y_n))$ (equivalence)

Congruence and Equivalence are axiom schemata. For example, Congruence for binary function f_2 for $n = 2$:

$$\forall x_1, x_2, y_1, y_2.\ x_1 = y_1 \ \wedge\ x_2 = y_2 \ \rightarrow\ f_2(x_1, x_2) = f_2(y_1, y_2)$$

Satisfiability

Example:

$x = y \ \wedge \ f(x) \neq f(y)$ $\qquad$ T_E-unsatisfiable

$f(x) = f(y) \ \wedge \ x \neq y$ $\qquad$ T_E-unsatisfiable

$f(f(f(a))) = a \ \wedge \ f(f(f(f(f(a))))) = a \ \wedge \ f(a) \neq a$

T_E-unsatisfiable

Decidability

- T_E is undecidable.
- The quantifier-free fragment of T_E is decidable. Very efficient algorithm.

(Remember: in quantifier-free fragment, all constants are, implicitly, universally quantified!)

We discuss T_E-formulae without predicates

For example, for Σ_E-formula

$$F: \; p(x) \; \wedge \; q(x,y) \; \wedge \; q(y,z) \; \rightarrow \; \neg q(x,z)$$

introduce fresh constant $\bullet$ and fresh functions f_p and f_g, and transform F to

$$G: \; f_p(x) = \bullet \; \wedge \; f_q(x,y) = \bullet \; \wedge \; f_q(y,z) = \bullet \; \rightarrow \; f_q(x,z) \neq \bullet \; .$$

Equivalence and Congruence Relations: Basics

Binary relation R over set S

- is an equivalence relation if
  - reflexive: $\forall s \in S.\ sRs$;
  - symmetric: $\forall s_1, s_2 \in S.\ s_1 R s_2 \ \rightarrow\ s_2 R s_1$;
  - transitive: $\forall s_1, s_2, s_3 \in S.\ s_1 R s_2 \ \wedge\ s_2 R s_3 \ \rightarrow\ s_1 R s_3$.

Example:
Define the binary relation $\equiv_2$ over the set $\mathbb{Z}$ of integers

$$m \equiv_2 n \quad \text{iff} \quad (m \bmod 2) = (n \bmod 2)$$

That is, $m, n \in \mathbb{Z}$ are related iff they are both even or both odd.
$\equiv_2$ is an equivalence relation

- is a congruence relation if in addition

$$\forall \overline{s}, \overline{t}.\ \bigwedge_{i=1}^{n} s_i R t_i \ \rightarrow\ f(\overline{s}) R f(\overline{t})\ .$$

Classes

For $\left\{ \begin{array}{c} \text{equivalence} \\ \text{congruence} \end{array} \right\}$ relation R over set S,

The $\left\{ \begin{array}{c} \underline{\text{equivalence}} \\ \underline{\text{congruence}} \end{array} \right\}$ class of $s \in S$ under R is

$$[s]_R \stackrel{\text{def}}{=} \{s' \in S \ : \ sRs'\} \ .$$

Example:

The equivalence class of 3 under $\equiv_2$ over $\mathbb{Z}$ is

$$[3]_{\equiv_2} = \{n \in \mathbb{Z} \ : \ n \text{ is odd}\} \ .$$

Closures

Given binary relation R over S.
The equivalence closure R^E of R is the equivalence relation s.t.

- R refines R^E, i.e. $R \prec R^E$;
- for all other equivalence relations R' s.t. $R \prec R'$,
  either $R' = R^E$ or $R^E \prec R'$

That is, R^E is the "smallest" equivalence relation that "covers" R.

Closures

Example: If $S = \{a, b, c, d\}$ and $R = \{aRb, bRc, dRd\}$, then

- $aRb, bRc, dRd \in R^E$ since $R \subseteq R^E$;
- $aRa, bRb, cRc \in R^E$ by reflexivity;
- $bRa, cRb \in R^E$ by symmetry;
- $aRc \in R^E$ by transitivity;
- $cRa \in R^E$ by symmetry.

Hence,

$$R^E = \{aRb, bRa, aRa, bRb, bRc, cRb, cRc, aRc, cRa, dRd\} .$$

Similarly, the congruence closure R^C of R is the "smallest" congruence relation that "covers" R.

Congruence Closure Algorithm

Given Σ_E-formula

$$F : \; s_1 = t_1 \;\wedge\; \cdots \;\wedge\; s_m = t_m \;\wedge\; s_{m+1} \neq t_{m+1} \;\wedge\; \cdots \;\wedge\; s_n \neq t_n$$

decide if F is Σ_E-satisfiable.

Consider the set of *subterms* of F.

Example: The subterm set of

$$F : \; f(a, b) = a \;\wedge\; f(f(a, b), b) \neq a$$

is

$$S_F = \{a,\; b,\; f(a, b),\; f(f(a, b), b)\} \; .$$

The Algorithm

Given Σ_E-formula F

$$F : s_1 = t_1 \wedge \cdots \wedge s_m = t_m \wedge s_{m+1} \neq t_{m+1} \wedge \cdots \wedge s_n \neq t_n$$

with subterm set S_F, F is T_E-satisfiable iff there exists a congruence relation $\sim$ over S_F such that

- for each $i \in \{1, \ldots, m\}$, $s_i \sim t_i$;
- for each $i \in \{m+1, \ldots, n\}$, $s_i \not\sim t_i$.

Goal: construct the congruence relation of S_F, or to prove that no congruence relation exists.

The algorithm

$$F: \underbrace{s_1 = t_1 \ \wedge \ \cdots \ \wedge \ s_m = t_m}_{\text{generate congruence closure}} \ \wedge \ \underbrace{s_{m+1} \neq t_{m+1} \ \wedge \ \cdots \ \wedge \ s_n \neq t_n}_{\text{search for contradiction}}$$

1. Construct the congruence closure $\sim$ of

   $$\{s_1 = t_1, \ldots, s_m = t_m\}$$

   over the subterm set S_F. Then

   $$\sim \models \ s_1 = t_1 \ \wedge \ \cdots \ \wedge \ s_m = t_m \ .$$

2. If for any $i \in \{m+1, \ldots, n\}$, $s_i \sim t_i$, return unsatisfiable.
3. Otherwise, $\sim \models F$, so return satisfiable.

Constructing the closure

1. Initially, begin with the finest congruence relation $\sim_0$ given by the partition
$$\{\{s\} \ : \ s \in S_F\} \ .$$
That is, let each term of S_F be its own congruence class.
2. Then, for each $i \in \{1, \dots, m\}$, impose $s_i = t_i$ by merging the congruence classes
$$[s_i]_{\sim_{i-1}} \quad \text{and} \quad [t_i]_{\sim_{i-1}}$$
to form a new congruence relation $\sim_i$. To accomplish this merging,
   - form the union of $[s_i]_{\sim_{i-1}}$ and $[t_i]_{\sim_{i-1}}$
   - propagate any new congruences that arise within this union.

Examples

1. $F: \; f(a,b) = a \;\wedge\; f(f(a,b),b) \neq a$

Examples

1. $F: \; f(a,b) = a \;\wedge\; f(f(a,b),b) \neq a$
2. $F: \; f(f(f(a))) = a \;\wedge\; f(f(f(f(f(a))))) = a \;\wedge\; f(a) \neq a.$

Theorem (Sound and Complete)

Quantifier-free conjunctive Σ_E-formula F is T_E-satisfiable iff the congruence closure algorithm returns satisfiable.

Natural Numbers and Integers

Natural numbers	$\mathbb{N} = \{0, 1, 2, \cdots\}$
Integers	$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$

Three variations:

- Peano arithmetic T_{PA}: natural numbers with addition and multiplication
- Presburger arithmetic $T_{\mathbb{N}}$: natural numbers with addtion
- Theory of integers $T_{\mathbb{Z}}$: integers with $+, -, >$

Peano Arithmetic T_{PA} (first-order arithmetic)

$$\Sigma_{\mathrm{PA}} : \ \{0,\ 1,\ +,\ \cdot,\ =\}$$

The 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)
6. $\forall x.\ x \cdot 0 = 0$ (times zero)
7. $\forall x, y.\ x \cdot (y + 1) = x \cdot y + x$ (times successor)

Line 3 is an axiom schema.

Example: $3x + 5 = 2y$ can be written using Σ_{PA} as

$$x + x + x + 1 + 1 + 1 + 1 + 1 = y + y$$

We have $>$ and $\geq$ since

$$3x + 5 > 2y \quad \text{write as} \quad \exists z.\ z \neq 0 \ \wedge \ 3x + 5 = 2y + z$$
$$3x + 5 \geq 2y \quad \text{write as} \quad \exists z.\ 3x + 5 = 2y + z$$

Example:

- Pythagorean Theorem is T_{PA}-valid
$$\exists x, y, z.\ x \neq 0 \ \wedge \ y \neq 0 \ \wedge \ z \neq 0 \ \wedge \ xx + yy = zz$$
- Every formula in the following set is T_{PA}-valid (Andrew Wiles, 1994).
$\{\forall x, y, z.\, x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \rightarrow x^n + y^n = z^n\}$

Satisfiability and validity in T_{PA} is undecidable, even in quantifier-free case. Therefore, we want a restricted theory – no multiplication

Presburger Arithmetic $T_{\mathbb{N}}$

$\Sigma_{\mathbb{N}} : \{0,\ 1,\ +,\ =\}$ no multiplication!

Axioms $T_{\mathbb{N}}$:

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)

3 is an axiom schema.

$T_{\mathbb{N}}$-satisfiability and $T_{\mathbb{N}}$-validity are decidable (Presburger, 1929)

Theory of Integers $T_{\mathbb{Z}}$

$\Sigma_{\mathbb{Z}}: \{\ldots, -2, -1, 0,\ 1,\ 2,\ \ldots, -3\cdot, -2\cdot,\ 2\cdot,\ 3\cdot,\ \ldots,\ +,\ -,\ =,\ >\}$

where

- $\ldots, -2, -1, 0,\ 1,\ 2,\ \ldots$ are constants
- $\ldots, -3\cdot, -2\cdot, 2\cdot,\ 3\cdot,\ \ldots$ are unary functions
  (intended $2 \cdot x$ is $2x$)
- $+, -, =, >$

$\boxed{T_{\mathbb{Z}} \text{ and } T_{\mathbb{N}} \text{ have the same expressiveness}}$

Equivalence

- Every $T_{\mathbb{Z}}$-formula can be reduced to $\Sigma_{\mathbb{N}}$-formula.
- Every $T_{\mathbb{N}}$-formula can be reduced to $\Sigma_{\mathbb{Z}}$-formula.

$\boxed{T_{\mathbb{Z}}\text{-satisfiability and } T_{\mathbb{N}}\text{-validity is decidable}}$

Rationals and Reals

$$\Sigma = \{0,\ 1,\ +,\ -,\ =,\ \geq\}$$

- Theory of Reals $T_{\mathbb{R}}$ (with multiplication)

$$x^2 = 2 \quad \Rightarrow \quad x = \pm\sqrt{2}$$

- Theory of Rationals $T_{\mathbb{Q}}$ (no multiplication)

$$\underbrace{2x}_{x+x} = 7 \quad \Rightarrow \quad x = \frac{2}{7}$$

<u>Note</u>: Strict inequality OK

$$\forall x, y.\ \exists z.\ x + y > z$$

rewrite as

$$\forall x, y.\ \exists z.\ \neg(x + y = z)\ \land\ x + y \geq z$$

Theory of Reals $T_{\mathbb{R}}$

$$\Sigma_{\mathbb{R}} : \ \{0, \ 1, \ +, \ -, \ \cdot, \ =, \ \geq\}$$

with multiplication.
Axioms in "The Calculus of Computation".

Example:

$$\forall a, b, c. \ b^2 - 4ac \geq 0 \ \leftrightarrow \ \exists x. \ ax^2 + bx + c = 0$$

is $T_{\mathbb{R}}$-valid.

$T_{\mathbb{R}}$ is decidable (Tarski, 1930)
High time complexity

Theory of Rationals $T_{\mathbb{Q}}$

$$\Sigma_{\mathbb{Q}} : \ \{0,\ 1,\ +,\ -,\ =,\ \geq\}$$

without multiplication.
Axioms in "The calculus of computation".

Rational coefficients are simple to express in $T_{\mathbb{Q}}$

Example: Rewrite

$$\frac{1}{2}x + \frac{2}{3}y \geq 4$$

as the $\Sigma_{\mathbb{Q}}$-formula

$$3x + 4y \geq 24$$

$T_{\mathbb{Q}}$ is decidable
Quantifier-free fragment of $T_{\mathbb{Q}}$ is efficiently decidable

Recursive Data Structures (T_{cons})

$$\Sigma_{\text{cons}}: \{\text{cons}, \text{car}, \text{cdr}, \text{atom}, =\}$$

where

- $\text{cons}(a, b)$ – list constructed by concatenating a and b
- $\text{car}(x)$ – left projector of x: $\text{car}(\text{cons}(a, b)) = a$
- $\text{cdr}(x)$ – right projector of x: $\text{cdr}(\text{cons}(a, b)) = b$
- $\text{atom}(x)$ – true iff x is a single-element list

Axioms:

1. The axioms of reflexivity, symmetry, and transitivity of $=$
2. Congruence axioms

$$\forall x_1, x_2, y_1, y_2.\ x_1 = x_2 \ \wedge\ y_1 = y_2 \ \rightarrow\ \mathsf{cons}(x_1, y_1) = \mathsf{cons}(x_2, y_2)$$
$$\forall x, y.\ x = y \ \rightarrow\ \mathsf{car}(x) = \mathsf{car}(y)$$
$$\forall x, y.\ x = y \ \rightarrow\ \mathsf{cdr}(x) = \mathsf{cdr}(y)$$

3. Equivalence axiom

$$\forall x, y.\ x = y \ \rightarrow\ (\mathsf{atom}(x) \ \leftrightarrow\ \mathsf{atom}(y))$$

4. $\forall x, y.\ \mathsf{car}(\mathsf{cons}(x, y)) = x$ (left projection)
5. $\forall x, y.\ \mathsf{cdr}(\mathsf{cons}(x, y)) = y$ (right projection)
6. $\forall x.\ \neg\mathsf{atom}(x) \ \rightarrow\ \mathsf{cons}(\mathsf{car}(x), \mathsf{cdr}(x)) = x$ (construction)
7. $\forall x, y.\ \neg\mathsf{atom}(\mathsf{cons}(x, y))$ (atom)

T_{cons} is undecidable
Quantifier-free fragment of T_{cons} is efficiently decidable

Lists + equality

$$T_{\text{cons}}^{=} \quad = \quad T_{\text{E}} \ \cup \ T_{\text{cons}}$$

Signature: $\Sigma_{\text{E}} \ \cup \ \Sigma_{\text{cons}}$

(this includes uninterpreted constants, functions, and predicates)

Axioms: union of the axioms of T_{E} and T_{cons}

$T_{\text{cons}}^{=}$ is undecidable
Quantifier-free fragment of $T_{\text{cons}}^{=}$ is efficiently decidable

Example: Is the $\Sigma_{\text{cons}}^{=}$-formula

$$F: \quad \begin{array}{l} \text{car}(a) = \text{car}(b) \ \wedge \ \text{cdr}(a) = \text{cdr}(b) \ \wedge \ \neg\text{atom}(a) \ \wedge \ \neg\text{atom}(b) \\ \quad \rightarrow \ f(a) = f(b) \end{array}$$

$T_{\text{cons}}^{=}$-valid?

Theory of Arrays (T_A)

$$\Sigma_A : \{\cdot[\cdot],\ \cdot\langle\cdot \triangleleft \cdot\rangle,\ =\}$$

where

- $a[i]$ binary function –
  read array a at index i ("read(a,i)")
- $a\langle i \triangleleft v\rangle$ ternary function –
  write value v to index i of array a ("write(a,i,e)")

Axioms

1. the axioms of (reflexivity), (symmetry), and (transitivity) of T_E
2. $\forall a, i, j.\ i = j \ \rightarrow\ a[i] = a[j]$ (array congruence)
3. $\forall a, v, i, j.\ i = j \ \rightarrow\ a\langle i \triangleleft v\rangle[j] = v$ (read-over-write 1)
4. $\forall a, v, i, j.\ i \neq j \ \rightarrow\ a\langle i \triangleleft v\rangle[j] = a[j]$ (read-over-write 2)

Note: $=$ is only defined for array elements

$$F: \; a[i] = e \;\rightarrow\; a\langle i \triangleleft e\rangle = a$$

not T_{A}-valid, but

$$F': \; a[i] = e \;\rightarrow\; \forall j.\; a\langle i \triangleleft e\rangle[j] = a[j] \;,$$

is T_{A}-valid.

$\boxed{\begin{array}{l} T_{\mathsf{A}} \text{ is undecidable} \\ \text{Quantifier-free fragment of } T_{\mathsf{A}} \text{ is decidable} \end{array}}$

Theory of Arrays with extensionality ($T_A^=$)

Signature and axioms of $T_A^=$ are the same as T_A, with one additional axiom

$$\forall a, b.\ (\forall i.\ a[i] = b[i]) \ \leftrightarrow\ a = b \quad \text{(extensionality)}$$

Example:

$$F:\ a[i] = e \ \rightarrow\ a\langle i \triangleleft e\rangle = a$$

is $T_A^=$-valid.

$T_A^=$ is undecidable
Quantifier-free fragment of $T_A^=$ is decidable

Combination of Theories

How do we show that

$$1 \leq x \;\wedge\; x \leq 2 \;\wedge\; f(x) \neq f(1) \;\wedge\; f(x) \neq f(2)$$

is $(T_{\mathsf{E}} \;\cup\; T_{\mathbb{Z}})$-unsatisfiable?

Or how do we prove properties about

an array of integers, or

a list of reals . . . ?

Given theories T_1 and T_2 such that

$$\Sigma_1 \;\cap\; \Sigma_2 \quad = \quad \{=\}$$

The combined theory $T_1 \;\cup\; T_2$ has

- signature $\Sigma_1 \;\cup\; \Sigma_2$
- axioms $A_1 \;\cup\; A_2$

Nelson & Oppen showed that

if satisfiability of quantifier-free fragment (qff) of T_1 is decidable,

satisfiability of qff of T_2 is decidable, and

certain technical simple requirements are met

then satisfiability of qff of $T_1 \cup T_2$ is decidable.

Combining Decision Procedures

Σ_1-theory T_1 $\quad\quad\quad\quad$ Σ_2-theory T_2

$\boxed{P_1}$ for T_1-satisfiability $\quad\quad\quad\quad$ $\boxed{P_2}$ for T_2-satisfiability

?

$\boxed{P}$ for $(T_1 \cup T_2)$-satisfiability

Problem:

Decision procedures are domain specific.

How do we combine them?

Nelson-Oppen Combination Method (N-O Method)

$$\Sigma_1 \cap \Sigma_2 = \{=\}$$

Σ_1-theory T_1
stably infinite

Σ_2-theory T_2
stably infinite

$\boxed{P_1}$ for T_1-satisfiability
of quantifier-free Σ_1-formulae

$\boxed{P_2}$ for T_2-satisfiability
of quantifier-free Σ_2-formulae

$\boxed{P}$ for $(T_1 \cup T_2)$-satisfiability
of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae

Nelson-Oppen: Limitations

Given formula F in theory $T_1 \cup T_2$.

1. F must be quantifier-free.
2. Signatures Σ_i of the combined theory only share $=$, i.e.,

$$\Sigma_1 \cap \Sigma_2 = \{=\}$$

3. Theories must be stably infinite.

Note:

- Algorithm can be extended to combine arbitrary number of theories T_i — combine two, then combine with another, and so on.
- We restrict F to be conjunctive formula — otherwise convert to DNF and check each disjunct.

Stably Infinite Theories

A Σ-theory T is *stably infinite* iff
for every quantifier-free Σ-formula F:
if F is T-satisfiable
then there exists some T-interpretation with an infinite domain that satisfies F.

Stably Infinite Theories

A Σ-theory T is *stably infinite* iff
for every quantifier-free Σ-formula F:
if F is T-satisfiable
then there exists some T-interpretation with an infinite domain that satisfies F.

Example: Σ-theory T

$$\Sigma : \{a, b, =\}$$

Axiom: $\forall x.\ x = a \ \vee \ x = b$

For every T-interpretation I, $|D_I| \leq 2$ (at most two elements).
Hence, T is *not* stably infinite.

All the other theories mentioned so far are stably infinite.

Example: Theory of partial orders

Σ-theory $T_{\preceq}$

$$\Sigma_{\preceq} : \ \{\preceq, \ =\}$$

where $\preceq$ is a binary predicate.

Axioms

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

Prove that this theory is stably infinite.

Example: $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$-formula

$$F : \ 1 \leq x \ \wedge \ x \leq 2 \ \wedge \ f(x) \neq f(1) \ \wedge \ f(x) \neq f(2) \ .$$

The signatures of T_E and $T_{\mathbb{Z}}$ only share $=$. Also, both theories are stably infinite. Hence, the N-O combination of the decision procedures for T_E and $T_{\mathbb{Z}}$ decides the $(T_E \cup T_{\mathbb{Z}})$-satisfiability of F.

Nelson-Oppen Method: Overview

Phase 1: Variable Abstraction

- Given conjunction Γ in theory $T_1 \cup T_2$.
- Convert to conjunction $\Gamma_1 \cup \Gamma_2$ s.t.
  - Γ_i in theory T_i
  - $\Gamma_1 \cup \Gamma_2$ satisfiable iff Γ satisfiable.

Phase 2: Check

- If there is some set S of equalities and disequalities between the shared variables of Γ_1 and Γ_2
  $\text{shared}(\Gamma_1, \Gamma_2) = \text{free}(\Gamma_1) \cap \text{free}(\Gamma_2)$
  s.t. $S \cup \Gamma_i$ are T_i-satisfiable for all i,
  then Γ is **satisfiable**.
- Otherwise, **unsatisfiable**.

Nelson-Oppen Method: Overview

Consider quantifier-free conjunctive $(\Sigma_1 \cup \Sigma_2)$-formula F.

Two versions:

- nondeterministic — simple to present, but high complexity
- deterministic — efficient

Nelson-Oppen (N-O) method proceeds in two steps:

- Phase 1 (variable abstraction)
  — same for both versions
- Phase 2
  nondeterministic: guess equalities/disequalities and check
  deterministic: generate equalities/disequalities by equality propagation

Phase 1: Variable abstraction

Given quantifier-free conjunctive $(\Sigma_1 \cup \Sigma_2)$-formula F.
Transform F into two quantifier-free conjunctive formulae

$$\Sigma_1\text{-formula } F_1 \qquad \text{and} \qquad \Sigma_2\text{-formula } F_2$$

s.t. F is $(T_1 \cup T_2)$-satisfiable iff $F_1 \wedge F_2$ is $(T_1 \cup T_2)$-satisfiable
F_1 and F_2 are linked via a set of shared variables.

For term t, let $\text{hd}(t)$ be the root symbol, e.g. $\text{hd}(f(x)) = f$.

Generation of F_1 and F_2

For $i, j \in \{1, 2\}$ and $i \neq j$, repeat the transformations

(1) if function $f \in \Sigma_i$ and $\mathrm{hd}(t) \in \Sigma_j$,

$$F[f(t_1, \ldots, t, \ldots, t_n)] \quad \Rightarrow \quad F[f(t_1, \ldots, w, \ldots, t_n)] \land w = t$$

(2) if predicate $p \in \Sigma_i$ and $\mathrm{hd}(t) \in \Sigma_j$,

$$F[p(t_1, \ldots, t, \ldots, t_n)] \quad \Rightarrow \quad F[p(t_1, \ldots, w, \ldots, t_n)] \land w = t$$

(3) if $\mathrm{hd}(s) \in \Sigma_i$ and $\mathrm{hd}(t) \in \Sigma_j$,

$$F[s = t] \quad \Rightarrow \quad F[\top] \ \land \ w = s \ \land \ w = t$$

(4) if $\mathrm{hd}(s) \in \Sigma_i$ and $\mathrm{hd}(t) \in \Sigma_j$,

$$F[s \neq t] \quad \Rightarrow \quad F[w_1 \neq w_2] \ \land \ w_1 = s \ \land \ w_2 = t$$

where w, w_1, and w_2 are fresh variables.

Example: Consider $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$-formula

$$F:\ 1 \leq x\ \wedge\ x \leq 2\ \wedge\ f(x) \neq f(1)\ \wedge\ f(x) \neq f(2)\ .$$

- Since $f \in \Sigma_E$ and $1 \in \Sigma_{\mathbb{Z}}$, replace $f(1)$ by $f(w_1)$ and add $w_1 = 1$.
- Replace $f(2)$ by $f(w_2)$ and add $w_2 = 2$.

Construct the $\Sigma_{\mathbb{Z}}$-formula

$$F_1:\ 1 \leq x\ \wedge\ x \leq 2\ \wedge\ w_1 = 1\ \wedge\ w_2 = 2$$

and the Σ_E-formula

$$F_2:\ f(x) \neq f(w_1)\ \wedge\ f(x) \neq f(w_2)\ .$$

F_1 and F_2 share the variables $\{x, w_1, w_2\}$.
$F_1\ \wedge\ F_2$ is $(T_E \cup T_{\mathbb{Z}})$-equisatisfiable to F.

Example: Consider $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$-formula

$$F : \; f(x) = x + y \land x \leq y + z \land x + z \leq y \land y = 1 \land f(x) \neq f(2) \, .$$

Show how to do variable abstraction.

Nondeterministic Version

Phase 2: Guess and Check

- Phase 1 separated $(\Sigma_1 \cup \Sigma_2)$-formula F into two formulae:
  Σ_1-formula F_1 and Σ_2-formula F_2
- F_1 and F_2 are linked by a set of shared variables:
  $V = \text{shared}(F_1, F_2) = \text{free}(F_1) \cap \text{free}(F_2)$
- Let E be an equivalence relation over V.
- The arrangement $\alpha(V, E)$ of V induced by E is:

$$\alpha(V, E) : \bigwedge_{u,v \,\in\, V.\ uEv} u = v \ \wedge \bigwedge_{u,v \,\in\, V.\ \neg(uEv)} u \neq v$$

Then,
the original formula F is $(T_1 \cup T_2)$-satisfiable iff
there exists an equivalence relation E of V s.t.
(1) $F_1 \ \wedge\ \alpha(V, E)$ is T_1-satisfiable, and
(2) $F_2 \ \wedge\ \alpha(V, E)$ is T_2-satisfiable.
Otherwise, F is $(T_1 \cup T_2)$-unsatisfiable.

Example: Consider $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$-formula

$$F:\ 1 \leq x \ \wedge\ x \leq 2 \ \wedge\ f(x) \neq f(1) \ \wedge\ f(x) \neq f(2)$$

Phase 1 separates this formula into the $\Sigma_{\mathbb{Z}}$-formula

$$F_1:\ 1 \leq x \ \wedge\ x \leq 2 \ \wedge\ w_1 = 1 \ \wedge\ w_2 = 2$$

and the Σ_E-formula

$$F_2:\ f(x) \neq f(w_1) \ \wedge\ f(x) \neq f(w_2)$$

with

$$V = \text{shared}(F_1, F_2) = \{x, w_1, w_2\}$$

In Phase 2, there are 5 equivalence relations to consider:

1. $\{\{x, w_1, w_2\}\}$, *i.e.*, $x = w_1 = w_2$:
   $x = w_1$ and $f(x) \neq f(w_1) \;\Rightarrow\; F_2 \;\wedge\; \alpha(V, E)$ is T_E-unsatisfiable.
2. $\{\{x, w_1\}, \{w_2\}\}$, *i.e.*, $x = w_1$, $x \neq w_2$:
   $x = w_1$ and $f(x) \neq f(w_1) \;\Rightarrow\; F_2 \;\wedge\; \alpha(V, E)$ is T_E-unsatisfiable.
3. $\{\{x, w_2\}, \{w_1\}\}$, *i.e.*, $x = w_2$, $x \neq w_1$:
   $x = w_2$ and $f(x) \neq f(w_2) \;\Rightarrow\; F_2 \;\wedge\; \alpha(V, E)$ is T_E-unsatisfiable.
4. $\{\{x\}, \{w_1, w_2\}\}$, *i.e.*, $x \neq w_1$, $w_1 = w_2$:
   $w_1 = w_2$ and $w_1 = 1 \;\wedge\; w_2 = 2$
   $\Rightarrow\; F_1 \;\wedge\; \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable.
5. $\{\{x\}, \{w_1\}, \{w_2\}\}$, *i.e.*, $x \neq w_1$, $x \neq w_2$, $w_1 \neq w_2$:
   $x \neq w_1 \;\wedge\; x \neq w_2$ and $x = w_1 = 1 \;\vee\; x = w_2 = 2$
   (since $1 \leq x \leq 2$ implies that $x = 1 \;\vee\; x = 2$ in $T_{\mathbb{Z}}$)
   $\Rightarrow\; F_1 \;\wedge\; \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable.

Hence, F is $(T_E \cup T_{\mathbb{Z}})$-unsatisfiable.

Example: Consider the $(\Sigma_{\text{cons}} \cup \Sigma_{\mathbb{Z}})$-formula

$$F : \ \text{car}(x) + \text{car}(y) = z \ \wedge \ \text{cons}(x, z) \neq \text{cons}(y, z) \ .$$

After two applications of (1), Phase 1 separates F into the Σ_{cons}-formula

$$F_1 : \ w_1 = \text{car}(x) \ \wedge \ w_2 = \text{car}(y) \ \wedge \ \text{cons}(x, z) \neq \text{cons}(y, z)$$

and the $\Sigma_{\mathbb{Z}}$-formula

$$F_2 : \ w_1 + w_2 = z \ ,$$

with

$$V = \text{shared}(F_1, F_2) = \{z, w_1, w_2\} \ .$$

Consider the equivalence relation E given by the partition

$$\{\{z\}, \{w_1\}, \{w_2\}\} \ .$$

The arrangement

$$\alpha(V, E) : \ z \neq w_1 \ \wedge \ z \neq w_2 \ \wedge \ w_1 \neq w_2$$

satisfies both F_1 and F_2: $F_1 \ \wedge \ \alpha(V, E)$ is T_{cons}-satisfiable, and $F_2 \ \wedge \ \alpha(V, E)$ is $T_{\mathbb{Z}}$-satisfiable.
Hence, F is $(T_{\text{cons}} \cup T_{\mathbb{Z}})$-satisfiable.

Practical Efficiency

Phase 2 was formulated as "guess and check":
First, guess an equivalence relation E,
then check the induced arrangement.

The number of equivalence relations grows super-exponentially with the # of shared variables. It is given by Bell numbers.
e.g., 12 shared variables $\Rightarrow$ over four million equivalence relations.

Solution: Deterministic Version

Deterministic Version

Phase 1 as before
Phase 2 asks the decision procedures P_1 and P_2 to propagate new equalities.

Example 1:

Real linear arithmethic $T_{\mathbb{R}}$ $\boxed{P_{\mathbb{R}}}$

Theory of equality T_E $\boxed{P_E}$

$$F: \quad f(f(x)-f(y)) \neq f(z) \ \wedge \ x \leq y \ \wedge \ y+z \leq x \ \wedge \ 0 \leq z$$

$$(T_{\mathbb{R}} \cup T_E)\text{-unsatisfiable}$$

Intuitively,
last 3 conjuncts $\Rightarrow$ $x = y \ \wedge \ z = 0$
contradicts 1st conjunct

Phase 1: Variable Abstraction

$$F : \; f(f(x) - f(y)) \neq f(z) \;\wedge\; x \leq y \;\wedge\; y + z \leq x \;\wedge\; 0 \leq z$$

$$f(x) \;\Rightarrow\; u \qquad f(y) \;\Rightarrow\; v \qquad u - v \;\Rightarrow\; w$$

$$\Gamma_E : \quad \{f(w) \neq f(z),\; u = f(x),\; v = f(y)\} \qquad \ldots\, T_E\text{-formula}$$

$$\Gamma_{\mathbb{R}} : \quad \{x \leq y,\; y + z \leq x,\; 0 \leq z,\; w = u - v\} \quad \ldots\, T_{\mathbb{R}}\text{-formula}$$

$$\text{shared}(\Gamma_{\mathbb{R}}, \Gamma_E) = \{x, y, z, u, v, w\}$$

Nondeterministic version — too expensive!
Let's try the deterministic version.

Phase 2: Equality Propagation

$\boxed{P_{\mathbb{R}}}$ $\boxed{P_E}$

$$s_0 : \langle \Gamma_{\mathbb{R}}, \Gamma_E, \{\} \rangle$$

$\Gamma_{\mathbb{R}} \models x = y$

$$s_1 : \langle \Gamma_{\mathbb{R}}, \Gamma_E, \{x = y\} \rangle$$

$\Gamma_E \cup \{x = y\} \models u = v$

$$s_2 : \langle \Gamma_{\mathbb{R}}, \Gamma_E, \{x = y, u = v\} \rangle$$

$\Gamma_{\mathbb{R}} \cup \{u = v\} \models z = w$

$$s_3 : \langle \Gamma_{\mathbb{R}}, \Gamma_E, \{x = y, u = v, z = w\} \rangle$$

$\Gamma_E \cup \{z = w\} \models \text{false}$

$$s_4 : \text{false}$$

Contradiction. Thus, F is $(T_{\mathbb{R}} \cup T_E)$-unsatisfiable.
If there were no contradiction, F would be $(T_{\mathbb{R}} \cup T_E)$-satisfiable.

Convex Theories

Claim:
Equality propagation is a decision procedure for convex theories.

Def. A Σ-theory T is *convex* iff
for every quantifier-free conjunctive Σ-formula F
and for every disjunction $\bigvee_{i=1}^{n}(u_i = v_i)$

$$\text{if } F \;\Rightarrow\; \bigvee_{i=1}^{n}(u_i = v_i)$$

$$\text{then } F \;\Rightarrow\; u_i = v_i, \;\text{ for some } i \in \{1, \ldots, n\}$$

Convex Theories

- T_E, $T_{\mathbb{R}}$, $T_{\mathbb{Q}}$, T_{cons} are convex
- $T_{\mathbb{Z}}$, T_{A} are not convex

Example: $T_{\mathbb{Z}}$ is not convex

Consider quantifier-free conjunctive

$$F: \quad 1 \le z \;\wedge\; z \le 2 \;\wedge\; u = 1 \;\wedge\; v = 2$$

Then

$$F \;\Rightarrow\; z = u \vee z = v$$

but

$$F \;\not\Rightarrow\; z = u$$
$$F \;\not\Rightarrow\; z = v$$

Example:

The theory of arrays T_{A} is not convex.
Consider the quantifier-free conjunctive Σ_{A}-formula

$$F: \ a\langle i \triangleleft v\rangle[j] = v \ .$$

Then

$$F \ \Rightarrow \ i = j \ \lor \ a[j] = v \ ,$$

but

$$\begin{array}{l} F \not\Rightarrow i = j \\ F \not\Rightarrow a[j] = v \ . \end{array}$$

What if T is Not Convex?

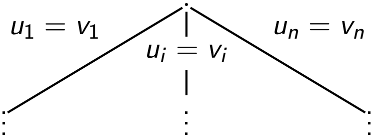
Case split when:

$$\Gamma \models \bigvee_{i=1}^{n} (u_i = v_i)$$

but

$$\Gamma \not\models u_i = v_i \qquad \text{for all } i = 1, \dots, n$$

- For each $i = 1, \dots, n$, construct a branch on which $u_i = v_i$ is assumed.
- If all branches are contradictory, then **unsatisfiable**. Otherwise, **satisfiable**.



Example 2: Non-Convex Theory

$T_{\mathbb{Z}}$ not convex! $\boxed{P_{\mathbb{Z}}}$

T_E convex $\boxed{P_E}$

$$\Gamma : \left\{ \begin{array}{ll} 1 \leq x, & x \leq 2, \\ f(x) \neq f(1), & f(x) \neq f(2) \end{array} \right\} \quad \text{in } T_{\mathbb{Z}} \cup T_E$$

- Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.

Result:

$$\Gamma_{\mathbb{Z}} = \left\{ \begin{array}{l} 1 \leq x, \\ x \leq 2, \\ w_1 = 1, \\ w_2 = 2 \end{array} \right\} \quad \text{and} \quad \Gamma_E = \left\{ \begin{array}{l} f(x) \neq f(w_1), \\ f(x) \neq f(w_2) \end{array} \right\}$$

$\text{shared}(\Gamma_{\mathbb{Z}}, \Gamma_E) = \{x, w_1, w_2\}$

Example 2: Non-Convex Theory

$s_0 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{\} \rangle$

$x = w_1$ $\star$ $x = w_2$

$s_1 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{x = w_1\} \rangle$ $s_3 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{x = w_2\} \rangle$

$\Gamma_E \cup \{x = w_1\} \models \bot$ $\Gamma_E \cup \{x = w_2\} \models \bot$

$s_2 : \bot$ $s_4 : \bot$

$\star : \ \Gamma_{\mathbb{Z}} \models x = w_1 \ \vee \ x = w_2$

All leaves are labeled with $\bot \Rightarrow \Gamma$ is $(T_{\mathbb{Z}} \cup T_E)$-unsatisfiable.

Example 3: Non-Convex Theory

$$\Gamma : \left\{ \begin{array}{c} 1 \leq x, \quad x \leq 3, \\ f(x) \neq f(1),\ f(x) \neq f(3),\ f(1) \neq f(2) \end{array} \right\} \quad \text{in } T_{\mathbb{Z}} \cup T_E$$

- Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.
- Replace $f(3)$ by $f(w_3)$, and add $w_3 = 3$.

Result:

$$\Gamma_{\mathbb{Z}} = \left\{ \begin{array}{l} 1 \leq x, \\ x \leq 3, \\ w_1 = 1, \\ w_2 = 2, \\ w_3 = 3 \end{array} \right\} \quad \text{and} \quad \Gamma_E = \left\{ \begin{array}{l} f(x) \neq f(w_1), \\ f(x) \neq f(w_3), \\ f(w_1) \neq f(w_2) \end{array} \right\}$$

$$\text{shared}(\Gamma_{\mathbb{Z}}, \Gamma_E) = \{x, w_1, w_2, w_3\}$$

Example 3: Non-Convex Theory

$$s_0 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{\} \rangle$$

$$x = w_1 \qquad x = w_2 \qquad x = w_3$$

$$s_1 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{x = w_1\} \rangle \quad s_3 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{x = w_2\} \rangle \quad s_5 : \langle \Gamma_{\mathbb{Z}}, \Gamma_E, \{x = w_3\} \rangle$$

$$\Gamma_E \cup \{x = w_1\} \models \bot \qquad \Gamma_E \cup \{x = w_3\} \models \bot$$

$$s_2 : \bot \qquad s_6 : \bot$$

$\star$: $\Gamma_{\mathbb{Z}} \models x = w_1 \ \vee \ x = w_2 \ \vee \ x = w_3$

No more equations on middle leaf $\Rightarrow$ Γ is $(T_{\mathbb{Z}} \cup T_E)$-satisfiable.