

THE CALCULUS OF COMPUTATION:
Decision Procedures with
Applications to Verification

by
Aaron Bradley
Zohar Manna

Springer 2007

10. Combining Decision Procedures

Combining Decision Procedures: Nelson-Oppen Method

Given

Theories T_i over signatures Σ_i
(constants, functions, predicates)
with corresponding decision procedures P_i for T_i -satisfiability.

Goal

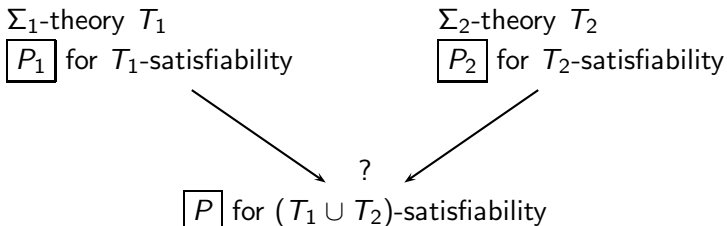
Decide satisfiability of a sentence in theory $\cup_i T_i$.

Example: How do we show that

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

is $(T_E \cup T_{\mathbb{Z}})$ -unsatisfiable?

Combining Decision Procedures



Problem:

Decision procedures are domain specific.

How do we combine them?

Nelson-Oppen Combination Method (N-O Method)

$$\Sigma_1 \cap \Sigma_2 = \emptyset$$

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

We prove T_{\preceq} is stably infinite.

Consider T_{\preceq} -satisfiable quantifier-free Σ_{\preceq} -formula F .

Consider arbitrary satisfying T_{\preceq} -interpretation $I : (D_I, \alpha_I)$,
where α_I maps \preceq to \leq_I .

- ▶ Let A be any infinite set disjoint from D_I
- ▶ Construct new interpretation $J : (D_J, \alpha_J)$

- ▶ $D_J = D_I \cup A$

- ▶ $\alpha_J = \{\preceq \mapsto \leq_J\}$, where for $a, b \in D_J$,

$$a \leq_J b \stackrel{\text{def}}{=} \begin{cases} a \leq_I b & \text{if } a, b \in D_I \\ a = b & \text{otherwise} \end{cases}$$

J is T_{\preceq} -interpretation satisfying F with infinite domain.

Hence, T_{\preceq} is stably infinite.

Example: Consider quantifier-free conjunctive $(\Sigma_E \cup \Sigma_{\mathbb{Z}})$ -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 NO combination of the decision procedures for T_E and $T_{\mathbb{Z}}$ decides the $(T_E \cup T_{\mathbb{Z}})$ -satisfiability of F .

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

For the first two literals imply $x = 1 \vee x = 2$ so that $f(x) = f(1) \vee f(x) = f(2)$.

Contradict last two literals.

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

N-O 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

Σ_1 -formula F_1 and Σ_2 -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 $\text{hd}(t) \in \Sigma_j$,

$$F[f(t_1, \dots, t, \dots, t_n)] \Rightarrow F[f(t_1, \dots, w, \dots, t_n)] \wedge w = t$$

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

$$F[p(t_1, \dots, t, \dots, t_n)] \Rightarrow F[p(t_1, \dots, w, \dots, t_n)] \wedge w = t$$

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

$$F[s = t] \Rightarrow F[\top] \wedge w = s \wedge w = t$$

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

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

where w , w_1 , and w_2 are fresh variables.

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

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

According to transformation 1, since $f \in \Sigma_E$ and $1 \in \Sigma_{\mathbb{Z}}$, replace $f(1)$ by $f(w_1)$ and add $w_1 = 1$. Similarly, replace $f(2)$ by $f(w_2)$ and add $w_2 = 2$.

Now, the literals

$$\Gamma_{\mathbb{Z}} : \{1 \leq x, x \leq 2, w_1 = 1, w_2 = 2\}$$

are $T_{\mathbb{Z}}$ -literals, while the literals

$$\Gamma_E : \{f(x) \neq f(w_1), f(x) \neq f(w_2)\}$$

are T_E -literals. Hence, 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

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

In the first literal, $\text{hd}(f(x)) = f \in \Sigma_E$ and $\text{hd}(x + y) = + \in \Sigma_{\mathbb{Z}}$; thus, by (3), replace the literal with

$$w_1 = f(x) \wedge w_1 = x + y .$$

In the final literal, $f \in \Sigma_E$ but $2 \in \Sigma_{\mathbb{Z}}$, so by (1), replace it with

$$f(x) \neq f(w_2) \wedge w_2 = 2 .$$

Now, separating the literals results in two formulae:

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

is a $\Sigma_{\mathbb{Z}}$ -formula, and

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

is a Σ_E -formula.

The conjunction $F_1 \wedge F_2$ is $(T_E \cup T_{\mathbb{Z}})$ -equisatisfiable to F .

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

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

There are 5 equivalence relations to consider, which we list by stating the partitions:

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 arithmetic $T_{\mathbb{R}}$

$P_{\mathbb{R}}$

Theory of equality T_E

P_E

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

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

Intuitively,

last 3 conjuncts $\Rightarrow x = y \wedge z = 0$

contradicts 1st conjunct

Phase 1: Variable Abstraction

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

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

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

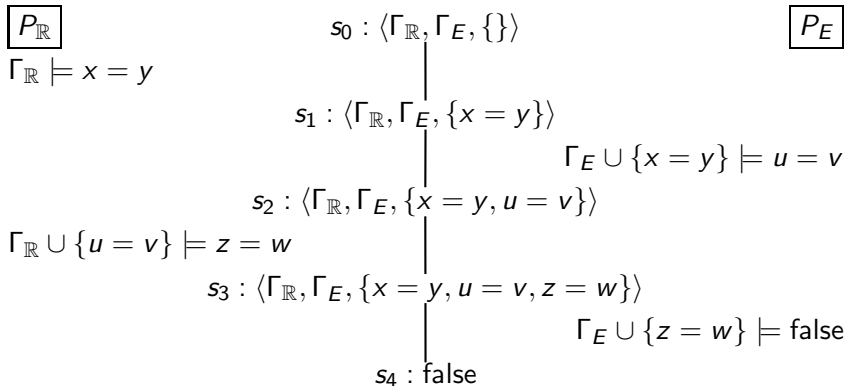
$$\Gamma_{\mathbb{R}} : \{x \leq y, y + z \leq x, 0 \leq z, w = u - v\} \quad \dots T_{\mathbb{R}}\text{-formula}$$

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

Nondeterministic version — over 200 E s!

Let's try the deterministic version.

Phase 2: Equality Propagation



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.

Claim:

Equality propagation is a decision procedure for convex theories.

Def. A Σ -theory T is *convex* iff

for every quantifier-free conjunction Σ -formula F

and for every disjunction $\bigvee_{i=1}^n (u_i = v_i)$

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

then $F \models u_i = v_i$, for some $i \in \{1, \dots, n\}$

Convex Theories

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

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

Consider quantifier-free conjunctive

$$F: 1 \leq z \wedge z \leq 2 \wedge u = 1 \wedge v = 2$$

Then

$$F \models z = u \vee z = v$$

but

$$F \not\models z = u$$

$$F \not\models z = v$$

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

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

but

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

What if T is Not Convex?

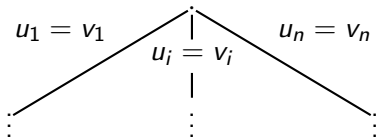
Case split when:

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

but

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

- ▶ 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

$$\boxed{P_E}$$

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

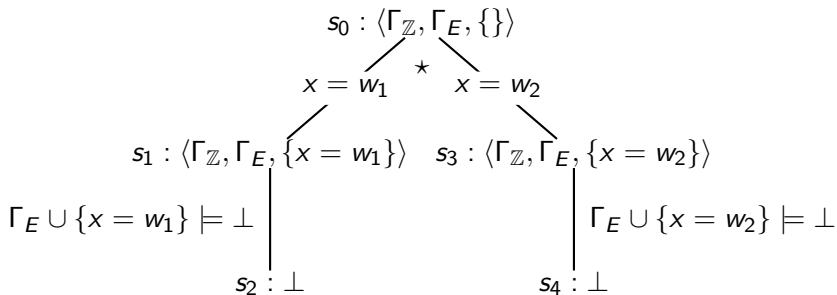
- ▶ Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- ▶ Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.

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



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

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

Example 3: Non-Convex Theory

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

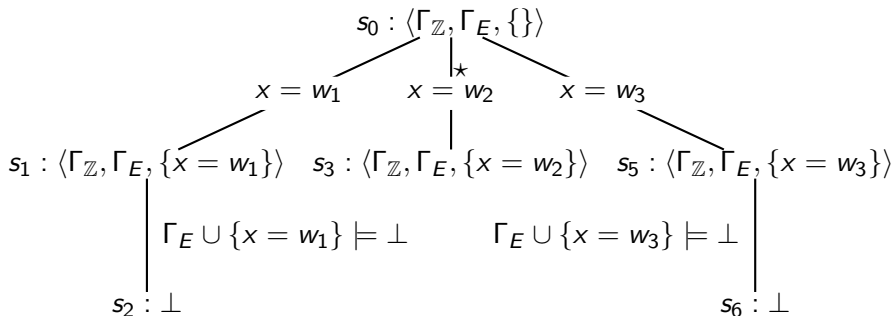
- ▶ Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- ▶ Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.
- ▶ Replace $f(3)$ by $f(w_3)$, and add $w_3 = 3$.

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



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

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