# CS156: The Calculus of Computation

Zohar Manna

Autumn 2008

Chapter 10: Combining Decision Procedures

# Combining Decision Procedures: Nelson-Oppen Method

**Given**

Theories $T_i$ over *signatures* $\Sigma_i$
with corresponding decision procedures $P_i$ for $T_i$-satisfiability.

**Goal**

Decide satisfiability of a formula $F$ 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

$$\begin{tikzcd}[column sep=small]
\begin{array}{l}\Sigma_1\text{-theory } T_1 \\ \boxed{P_1} \text{ for } T_1\text{-satisfiability}\end{array} \arrow[dr] & & \begin{array}{l}\Sigma_2\text{-theory } T_2 \\ \boxed{P_2} \text{ for } T_2\text{-satisfiability}\end{array} \arrow[dl] \\
& \overset{?}{\boxed{P} \text{ for } (T_1 \cup T_2)\text{-satisfiability}} &
\end{tikzcd}$$

**Problem**:
Decision procedures are domain specific.
How do we combine them?

# Nelson-Oppen Combination Method (N-O Method)

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

$\Sigma_1$-theory $T_1$
stably infinite

$\Sigma_2$-theory $T_2$
stably infinite

$\boxed{P_1}$ for $T_1$-satisfiability
of quantifier-free $\Sigma_1$-formulae

$\boxed{P_2}$ for $T_2$-satisfiability
of quantifier-free $\Sigma_2$-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 $\Sigma_i$ 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 equivalent DNF and check each disjunct.

# Stably Infinite Theories

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

**Example:** $\Sigma$-theory $T$

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

Axiom

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

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

**All the other theories mentioned so far are stably infinite.**

# Example: $T_E$ is stably infinite

Proof.

Let $F$ be $T_E$-satisfiable quantifier-free $\Sigma_E$-formula with arbitrary satisfying $T_E$-interpretation $I : (D_I, \alpha_I)$.

$\alpha_I$ maps $=$ to $=_I$.

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

- $D_J = D_I \cup A$
- $\alpha_J$ agrees with $\alpha_I$: the extension of functions and predicates for $A$ is irrelevant, except $=_J$. For $\mathsf{v}_1, \mathsf{v}_2 \in D_J$,

$$\mathsf{v}_1 =_J \mathsf{v}_2 \equiv \begin{cases} \mathsf{v}_1 =_I \mathsf{v}_2 & \text{if } \mathsf{v}_1, \mathsf{v}_2 \in D_I \\ \text{true} & \text{if } \mathsf{v}_1 \text{ is the same element as } \mathsf{v}_2 \\ \text{false} & \text{otherwise} \end{cases}$$

$J$ is a $T_E$-interpretation satisfying $F$ with infinite domain. Hence, $T_E$ 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 N-O combination of the decision procedures for $T_E$ and $T_{\mathbb{Z}}$ decides the $(T_E \cup T_{\mathbb{Z}})$-satisfiability of $F$.

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.

# 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:

$$\text{shared}(F_1, F_2) = \text{free}(F_1) \cap \text{free}(F_2)$$

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 $\mathrm{hd}(t) \in \Sigma_j$,

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

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

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

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

$$\begin{aligned} F[s = t] \quad &\Rightarrow \quad F[w = t] \ \wedge \ w = s \\ F[s \neq t] \quad &\Rightarrow \quad F[w \neq t] \ \wedge \ w = s \end{aligned}$$

where $w$ is a fresh variable in each application of a transformation.

# Example

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

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

By 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 $w_2 = 2$.

Hence, construct the $\Sigma_{\mathbb{Z}}$-formula

$$F_{\mathbb{Z}}: \; 1 \leq x \;\wedge\; x \leq 2 \;\wedge\; w_1 = 1 \;\wedge\; w_2 = 2$$

and the $\Sigma_E$-formula

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

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

# Example

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

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

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

$$w_1 = x + y \;\land\; w_1 = f(x) \; .$$

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

$$f(x) \neq f(w_2) \;\land\; w_2 = 2 \; .$$

Now, separating the literals results in two formulae:

$$F_{\mathbb{Z}}: \; w_1 = x + y \;\land\; x \leq y + z \;\land\; x + z \leq y \;\land\; y = 1 \;\land\; w_2 = 2$$

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

$$F_E: \; w_1 = f(x) \;\land\; f(x) \neq f(w_2)$$

is a $\Sigma_E$-formula.
The conjunction $F_{\mathbb{Z}} \land F_E$ 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:

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

- $F_1$ 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:

$$\begin{aligned} \alpha(V,E) : \quad & \bigwedge_{u,v \,\in\, V.\; uEv} u = v \\ \wedge \quad & \bigwedge_{u,v \,\in\, V.\; \neg(uEv)} u \neq v \end{aligned}$$

# Nondeterministic Version

Lemma
the original formula $F$ is $(T_1 \cup T_2)$-satisfiable iff
there exists an equivalence relation $E$ over $V$ 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 1

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

$$F_{\mathbb{Z}}: \; 1 \leq x \; \wedge \; x \leq 2 \; \wedge \; w_1 = 1 \; \wedge \; w_2 = 2$$

and the $\Sigma_E$-formula

$$F_E: \; f(x) \neq f(w_1) \; \wedge \; f(x) \neq f(w_2)$$

with

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

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

## Example 1

1. $\{\{x, w_1, w_2\}\}$, *i.e.*, $x = w_1 = w_2$:
   $x = w_1$ and $f(x) \neq f(w_1) \;\Rightarrow\; F_E \wedge \alpha(V, E)$ is $T_E$-unsatisfiable.
2. $\{\{x, w_1\}, \{w_2\}\}$, *i.e.*, $x = w_1$, $x \neq w_2$:
   $x = w_1$ and $f(x) \neq f(w_1) \;\Rightarrow\; F_E \wedge \alpha(V, E)$ is $T_E$-unsatisfiable.
3. $\{\{x, w_2\}, \{w_1\}\}$, *i.e.*, $x = w_2$, $x \neq w_1$:
   $x = w_2$ and $f(x) \neq f(w_2) \;\Rightarrow\; F_E \wedge \alpha(V, E)$ 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 $w_1 = 1 \wedge w_2 = 2$
   $\Rightarrow\; F_{\mathbb{Z}} \wedge \alpha(V, E)$ 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 $T_{\mathbb{Z}}$)
   $\Rightarrow\; F_{\mathbb{Z}} \wedge \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable.

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

# Example 2

Consider the $(\Sigma_{\mathsf{cons}} \cup \Sigma_{\mathbb{Z}})$-formula

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

After two applications of (1), Phase 1 separates $F$ into the $\Sigma_{\mathsf{cons}}$-formula

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

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

$$F_{\mathbb{Z}}: \ w_1 + w_2 = z \ ,$$

with

$$V = \mathsf{shared}(F_{\mathsf{cons}}, F_{\mathbb{Z}}) = \{z, w_1, w_2\} \ .$$

# Example 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 $F_{cons}$ and $F_{\mathbb{Z}}$:

$F_{cons} \; \wedge \; \alpha(V, E)$ is $T_{\text{cons}}$-satisfiable, and

$F_{\mathbb{Z}} \; \wedge \; \alpha(V, E)$ 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":

1. First, guess an equivalence relation $E$,
2. 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 3

Theory of equality $T_E$ — $\boxed{P_E}$

Rational linear arithmethic $T_{\mathbb{Q}}$ — $\boxed{P_{\mathbb{Q}}}$

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

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

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

# Phase 1: Variable Abstraction

Example 3

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

Replace $f(x)$ by $u$, $f(y)$ by $v$, $u - v$ by $w$

$F_E : \quad f(w) \neq f(z) \;\wedge\; u = f(x) \;\wedge\; v = f(y) \qquad \ldots\, T_E$-formula

$F_{\mathbb{Q}} : \quad x \leq y \;\wedge\; y + z \leq x \;\wedge\; 0 \leq z \;\wedge\; w = u - v \qquad \ldots\, T_{\mathbb{Q}}$-formula

$$\text{shared}(F_E, F_{\mathbb{Q}}) = \{x, y, z, u, v, w\}$$

Nondeterministic version — over 200 $E$s!
Let's try the deterministic version.

# Phase 2: Equality Propagation

Example 3

$$F_E: \quad f(w) \neq f(z) \ \wedge \ u = f(x) \ \wedge \ v = f(y)$$
$$F_{\mathbb{Q}}: \quad x \leq y \ \wedge \ y + z \leq x \ \wedge \ 0 \leq z \ \wedge \ w = u - v$$

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

$F_{\mathbb{Q}} \models x = y$

$\{x = y\}$

$F_E \wedge x = y \models u = v$

$\{x = y, u = v\}$

$F_{\mathbb{Q}} \wedge u = v \models z = w$

$\{x = y, u = v, z = w\}$

$F_E \wedge z = w \models \perp$

$\perp$

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

# Convex Theories

**Definition**

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

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

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

**Claim**

Equality propagation is a decision procedure for convex theories.

## Convex Theories

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

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

Consider quantifier-free conjunctive $\Sigma_{\mathbb{Z}}$-formula

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

Then

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

but

$$F \quad \not\Rightarrow \quad z = u$$

$$F \quad \not\Rightarrow \quad z = v$$

# Convex Theories

Example: Theory of arrays $T_{\mathrm{A}}$ is not convex

Consider the quantifier-free conjunctive $\Sigma_{\mathrm{A}}$-formula

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

Then

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

but

$$F \not\Rightarrow i = j$$
$$F \not\Rightarrow a[j] = v \ .$$

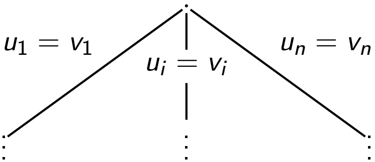
# What if $T$ is Not Convex?

Case split when:

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

but $F \not\Rightarrow u_i = v_i$ for any $i = 1, \ldots, n$

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




**Claim:** Equality propagation (with branching) is a decision procedure for non-convex theories too.

# Example 1: Non-Convex Theory

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

$T_E$ convex $\boxed{P_E}$

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

in $T_{\mathbb{Z}} \cup T_E$.

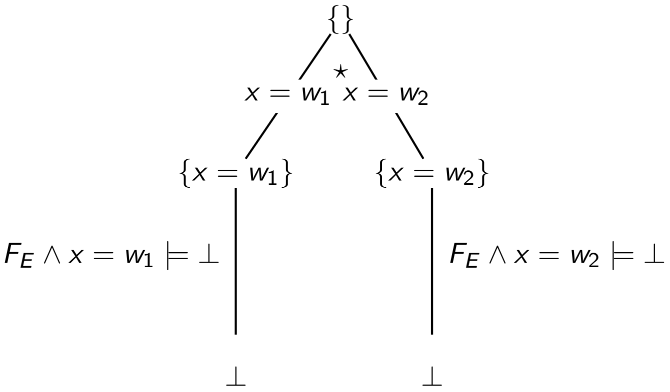
- Replace $f(1)$ by $f(w_1)$, and add $w_1 = 1$.
- Replace $f(2)$ by $f(w_2)$, and add $w_2 = 2$.

Result:

$$\begin{array}{lll} F_{\mathbb{Z}} & : & 1 \leq x \ \wedge \ x \leq 2 \ \wedge \ w_1 = 1 \ \wedge \ w_2 = 2 \\ F_E & : & f(x) \neq f(w_1) \ \wedge \ f(x) \neq f(w_2) \end{array}$$

and

$$V = \text{shared}(F_{\mathbb{Z}}, F_E) = \{x, w_1, w_2\}$$




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

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

# Example 4: Non-Convex Theory

Consider

$$\begin{aligned} F \quad : \quad & 1 \leq x \ \wedge \ x \leq 3 \ \wedge \\ & f(x) \neq f(1) \ \wedge \ f(x) \neq f(3) \ \wedge \ f(1) \neq f(2) \end{aligned}$$

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 $w_3 = 3$.

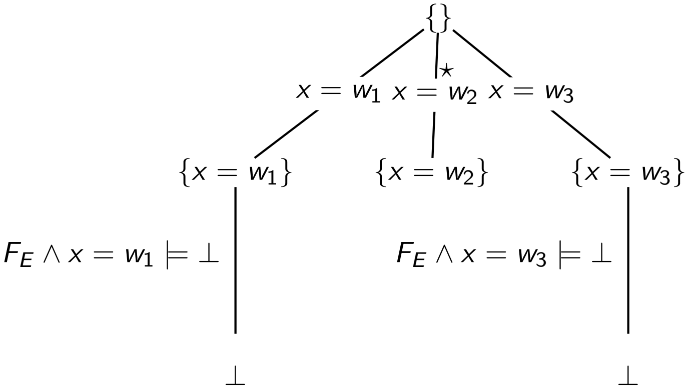
Result:

$$\begin{aligned} F_{\mathbb{Z}} \quad : \quad & 1 \leq x \ \wedge \ x \leq 3 \ \wedge \ w_1 = 1 \ \wedge \ w_2 = 2 \ \wedge \ w_3 = 3 \\ F_E \quad : \quad & f(x) \neq f(w_1) \ \wedge \ f(x) \neq f(w_3) \ \wedge \ f(w_1) \neq f(w_2) \end{aligned}$$

and

$$V = \text{shared}(F_{\mathbb{Z}}, F_E) = \{x, w_1, w_2, w_3\}$$

# Example 4: Non-Convex Theory




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

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