Computer-Aided Reasoning for Software

CSE507

Combining Theories

courses.cs.washington.edu/courses/cse507/14au/

Emina Torlak
emina@cs.washington.edu

Today

Today

Last lecture

- A survey of theory solvers and deciding $T_=$ with congruence closure

Today

Last lecture

- A survey of theory solvers and deciding $T_=$ with congruence closure

Today

- Deciding a combination of theories

Today

Last lecture

- A survey of theory solvers and deciding $T_=$ with congruence closure

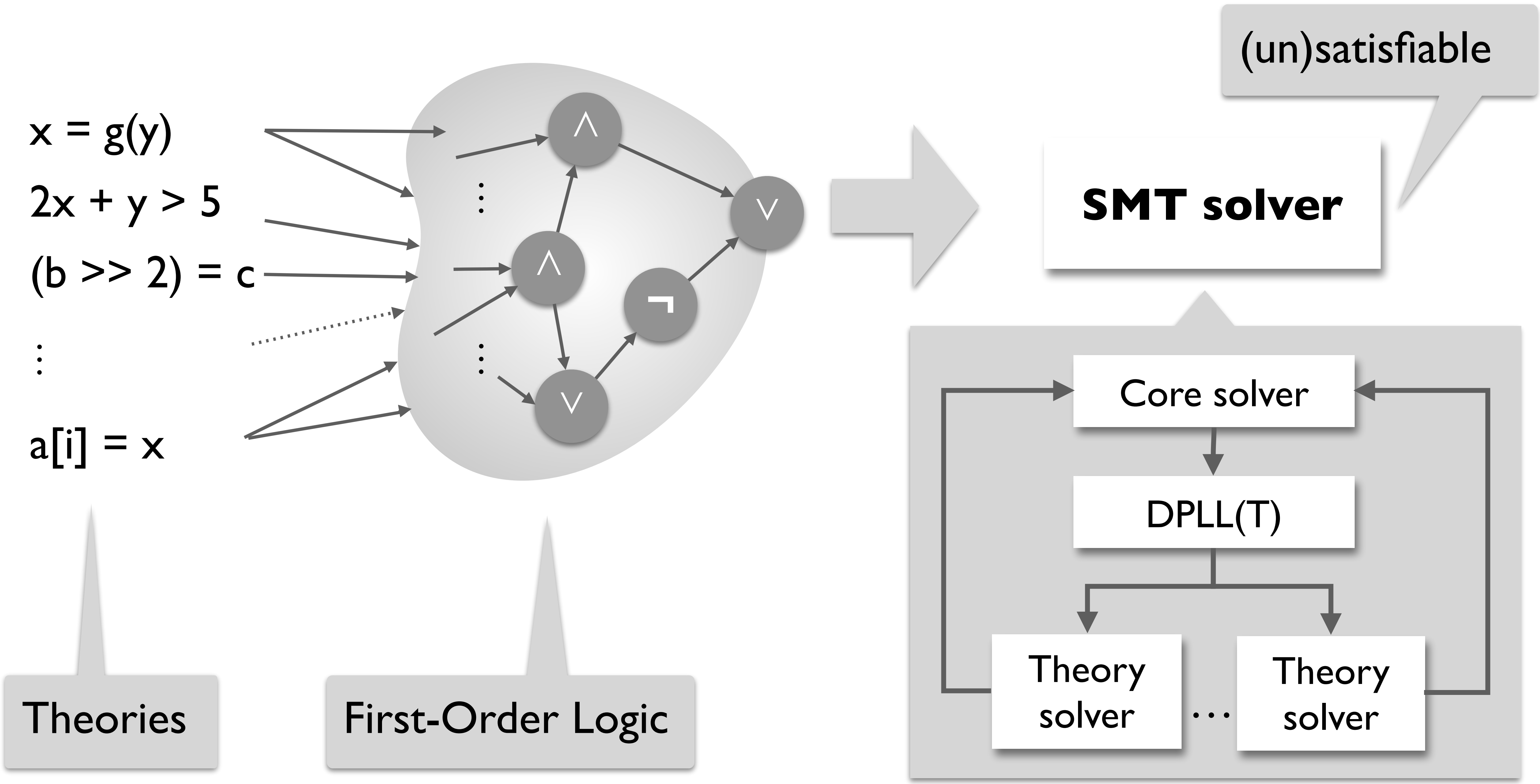
Today

- Deciding a combination of theories

Reminders

- Email us your project topic and brief abstract by 11pm today
- Homework 2 posted
  - Start early
  - Submit self-contained runnable code

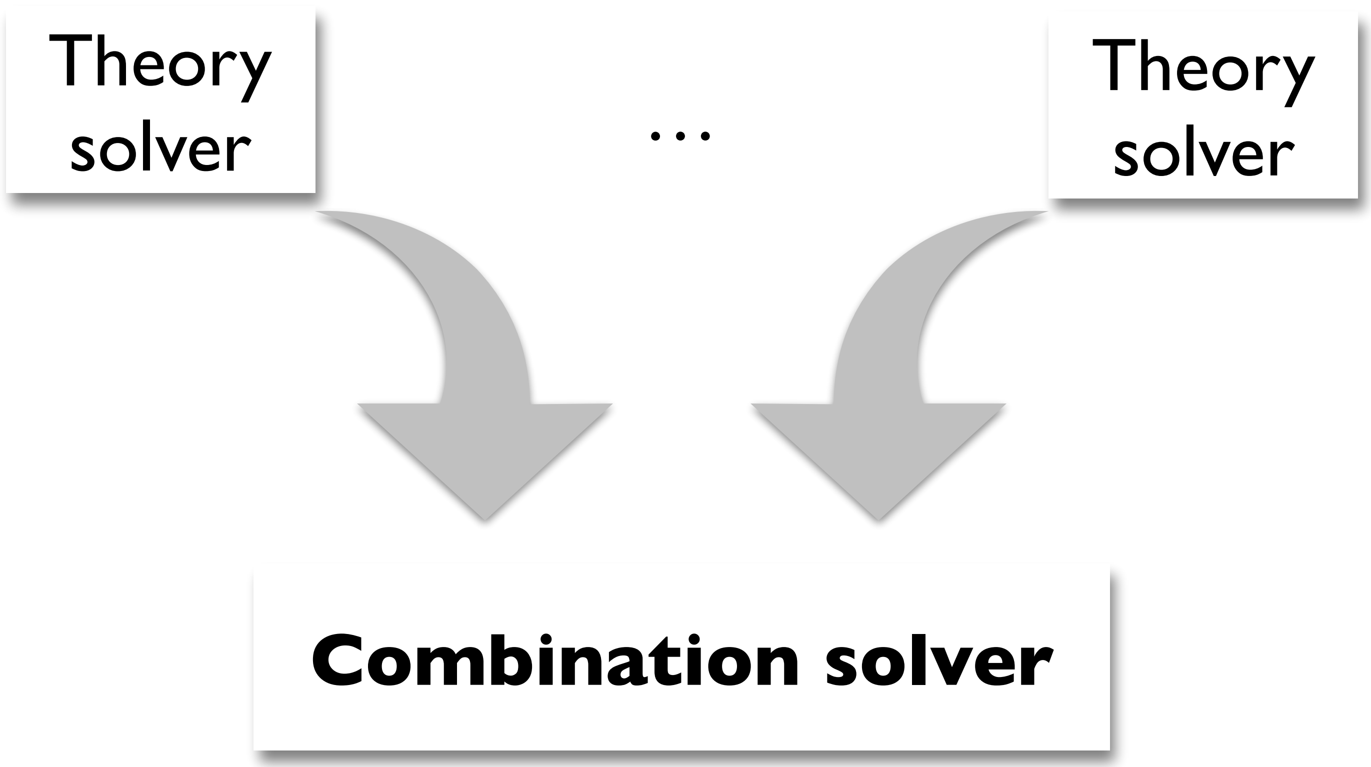
Satisfiability Modulo Theories (SMT)



Combining T-solvers with Nelson-Oppen

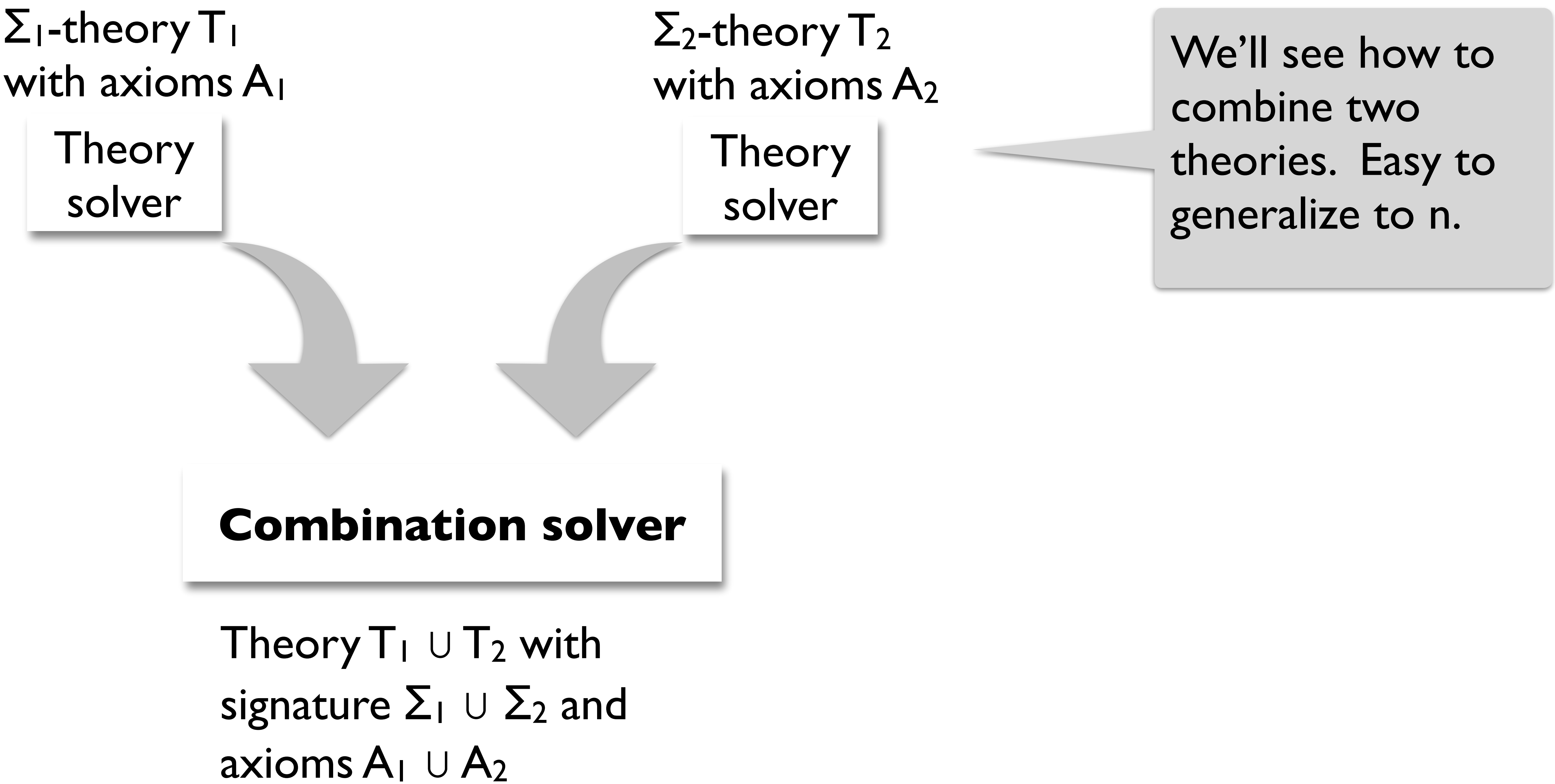
Σ_1-theory T_1
with axioms A_1

Σ_n-theory T_n
with axioms A_n



Theory $T_1 \cup \ldots \cup T_n$ with
signature $\Sigma_1 \cup \ldots \cup \Sigma_n$ and
axioms $A_1 \cup \ldots \cup A_n$

Combining T-solvers with Nelson-Oppen



Combining T-solvers with Nelson-Oppen

Σ_1-theory T_1
with axioms A_1

Theory solver

Σ_2-theory T_2
with axioms A_2

Theory solver

We'll see how to combine two theories. Easy to generalize to n.

Combination solver

Theory $T_1 \cup T_2$ with signature $\Sigma_1 \cup \Sigma_2$ and axioms $A_1 \cup A_2$

The combination problem is undecidable for arbitrary (decidable) theories. It becomes decidable under **Nelson-Oppen restrictions.**

Nelson-Oppen restrictions

T_1 and T_2 can be combined when

- Both are quantifier-free (conjunctive) fragments
- Equality (=) is the only symbol in the intersection of their signatures
- Both are **stably infinite**

Nelson-Oppen restrictions

T_1 and T_2 can be combined when

- Both are quantifier-free (conjunctive) fragments
- Equality (=) is the only symbol in the intersection of their signatures
- Both are **stably infinite**

A theory T is stably infinite iff for every satisfiable Σ_T-formula F, there is a T-model that satisfies F and that has a universe of infinite cardinality.

Examples of (non-)stably infinite theories

Σ_T :   { a, b, = }

A_T: $\forall x \,.\, x = a \vee x = b$

Examples of (non-)stably infinite theories

Σ_T :   { a, b, = }

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

✗

Examples of (non-)stably infinite theories

Σ_T : { a, b, = } ✗

A_T: $\forall x . x = a \lor x = b$

Fixed width bit vectors (T_{bv})

Examples of (non-)stably infinite theories

Σ_T : { a, b, = } ✗

A_T: $\forall\, x\, .\, x = a \vee x = b$

Fixed width bit vectors (T_{bv}) ✗

Examples of (non-)stably infinite theories

Σ_T : { a, b, = } ✗

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

Equality and uninterpreted functions ($T_=$)

Fixed width bit vectors (T_{bv}) ✗

Examples of (non-)stably infinite theories

Σ_T : { a, b, = } ✗

A_T: $\forall x . x = a \lor x = b$

Equality and uninterpreted functions ($T_=$) ✓

Fixed width bit vectors (T_{bv}) ✗

Examples of (non-)stably infinite theories

Σ_T : { a, b, = } ✗

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

Fixed width bit vectors (T_{bv}) ✗

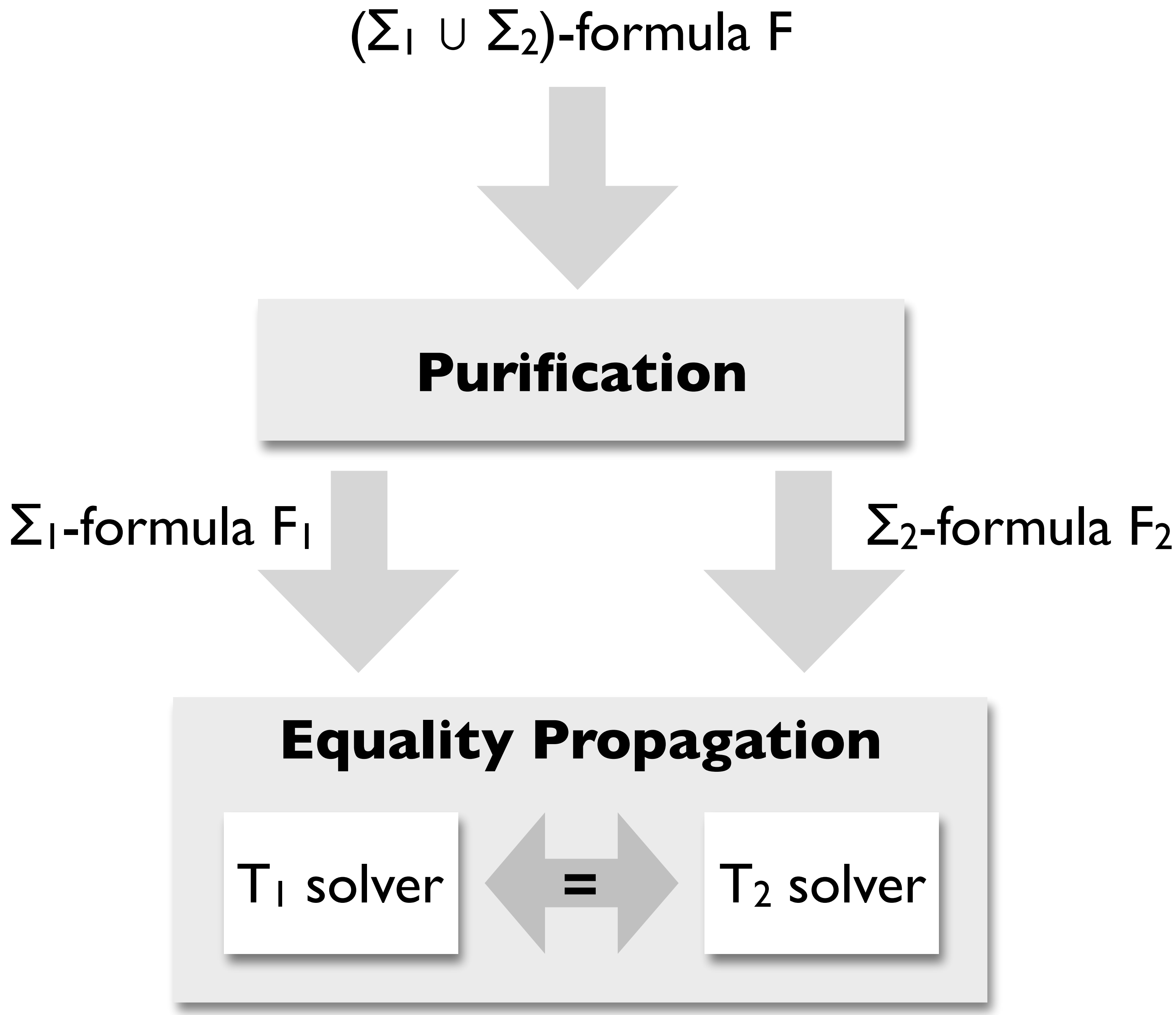
Equality and uninterpreted functions ($T_=$) ✓

Linear real arithmetic (T_R) ✓

Arrays (T_A) ✓

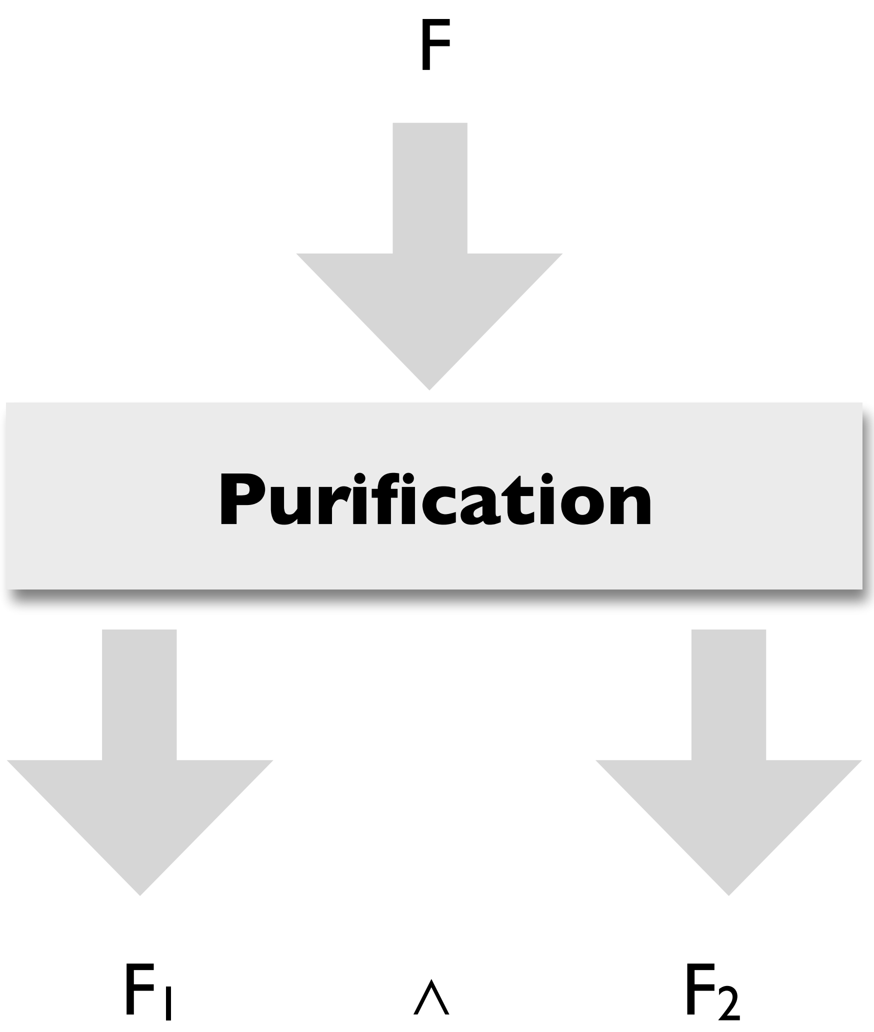
Linear integer arithmetic (T_R) ✓

Overview of Nelson-Oppen



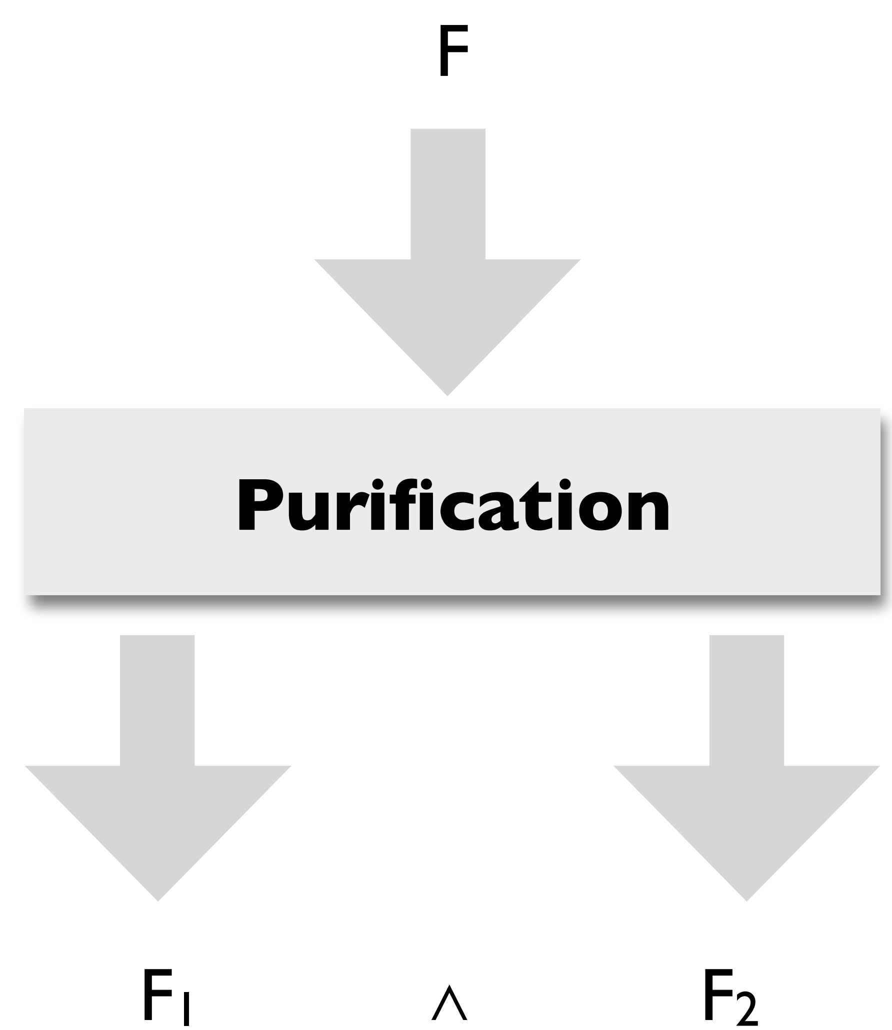
Overview of purification

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2



Overview of purification

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

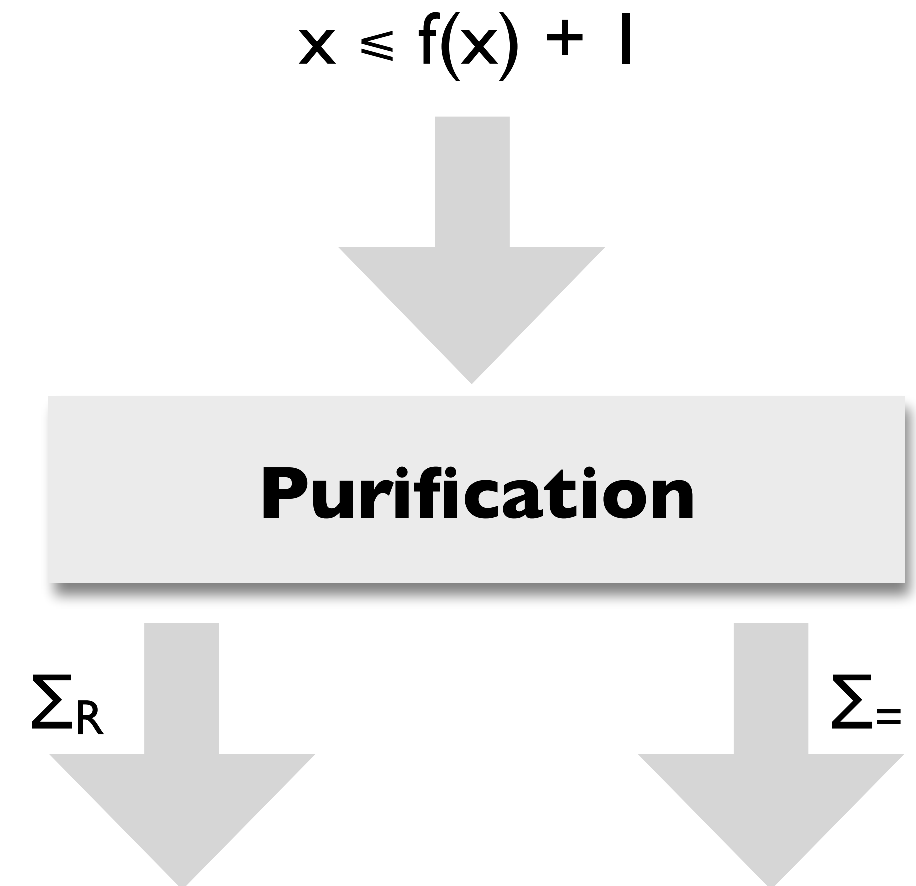


Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

Overview of purification

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2



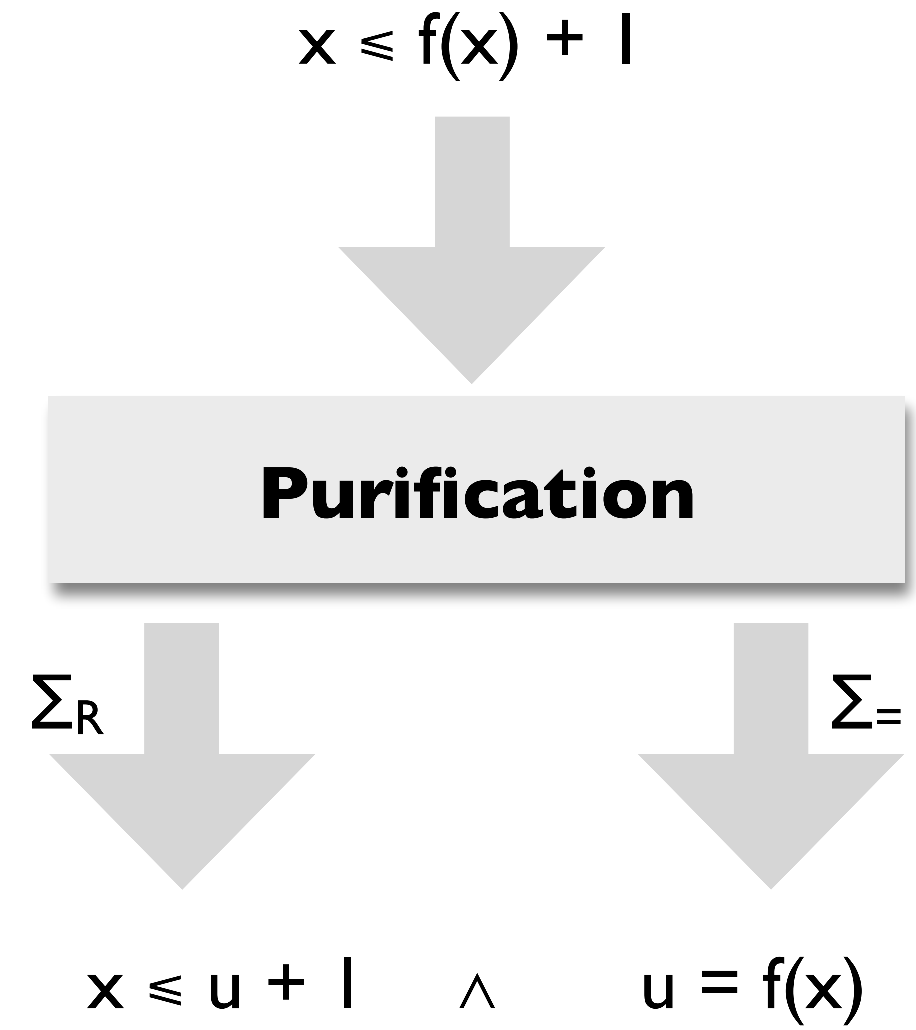
Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$

- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

Overview of purification

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

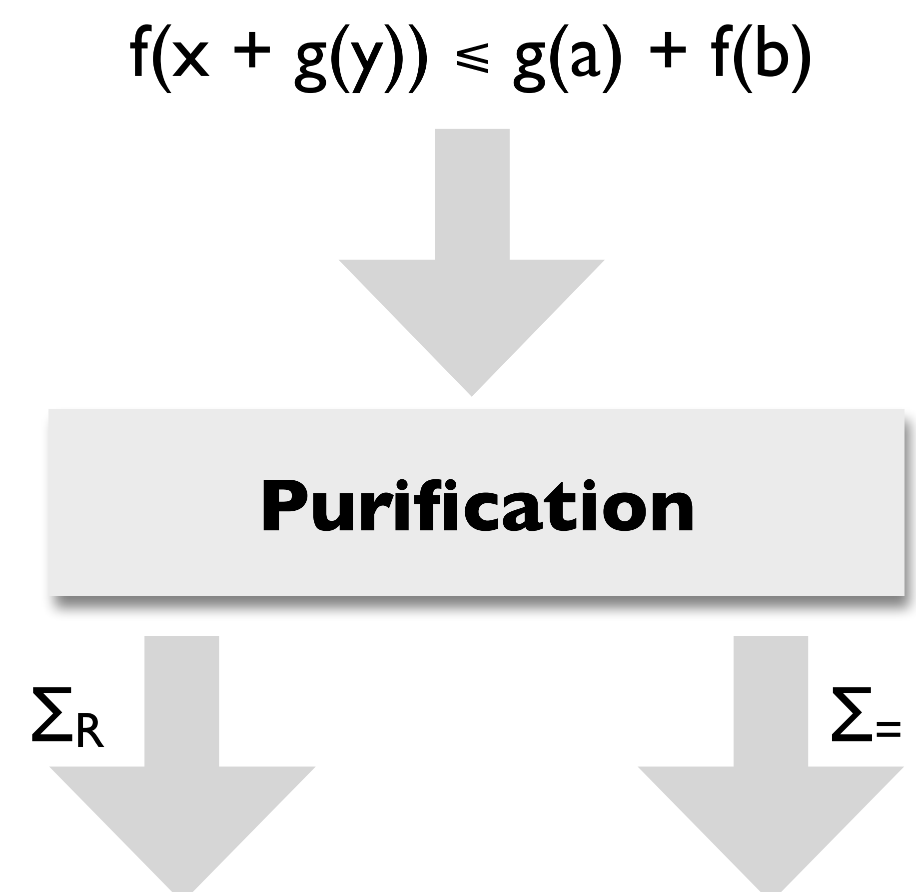


Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\dots, t, \dots)] \rightsquigarrow F[f(\dots, u, \dots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\dots, t, \dots)] \rightsquigarrow F[p(\dots, v, \dots)] \wedge v = t$

Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2



Repeat until fix point:

- If f is in T_i and t is not, and u is fresh: $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh: $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

Another purification example

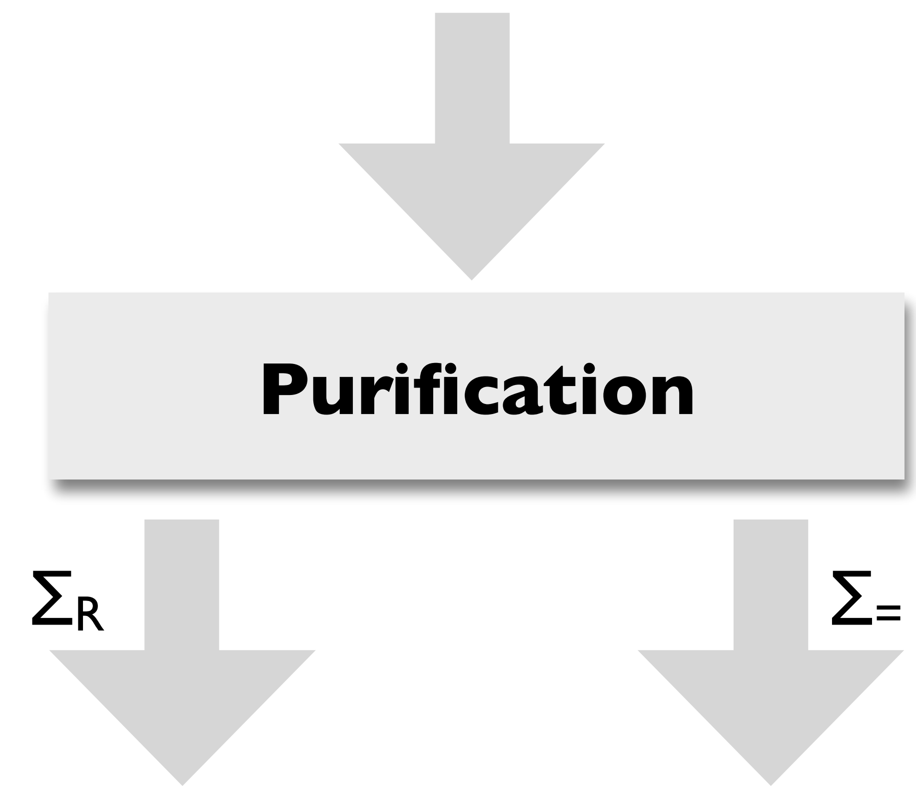
Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$

- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

$$f(x + g(y)) \leqslant g(a) + f(b)$$



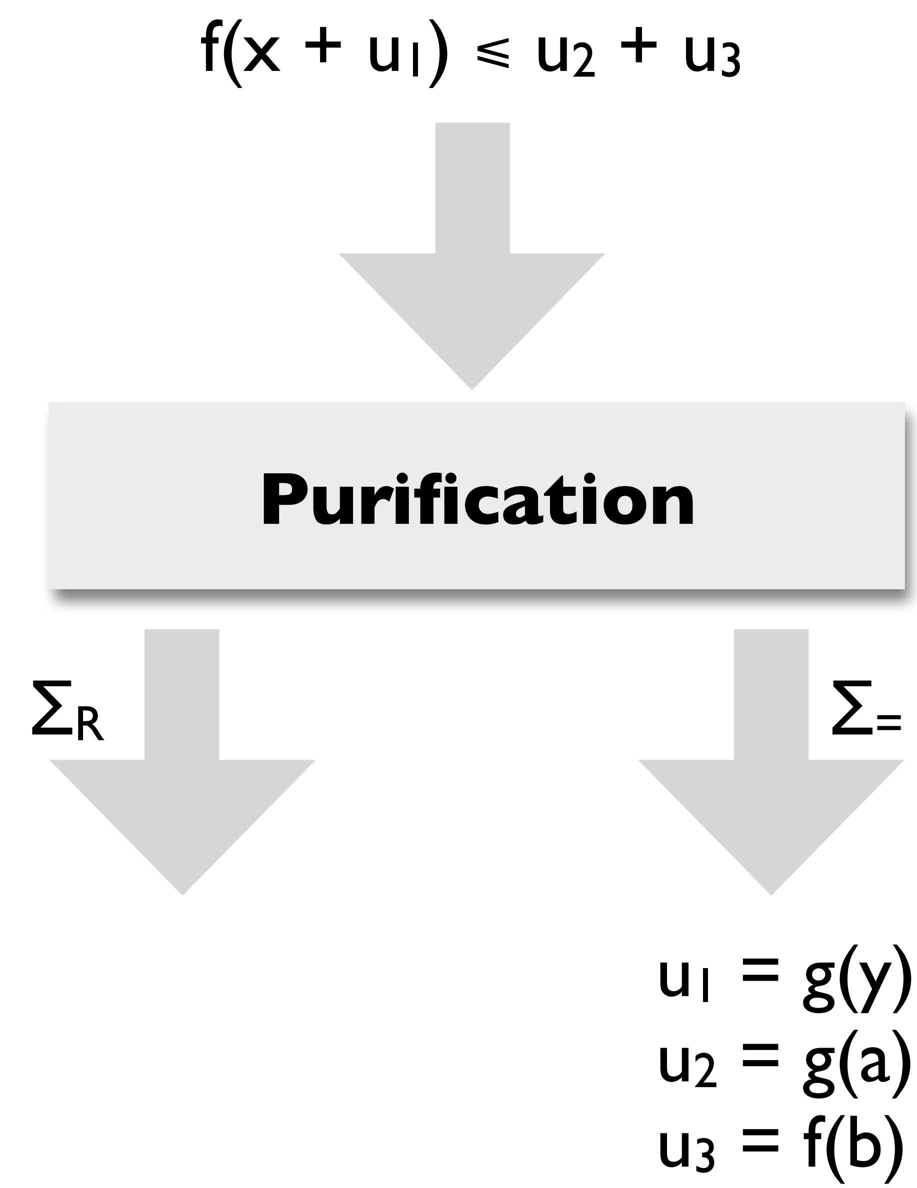
Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$

- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

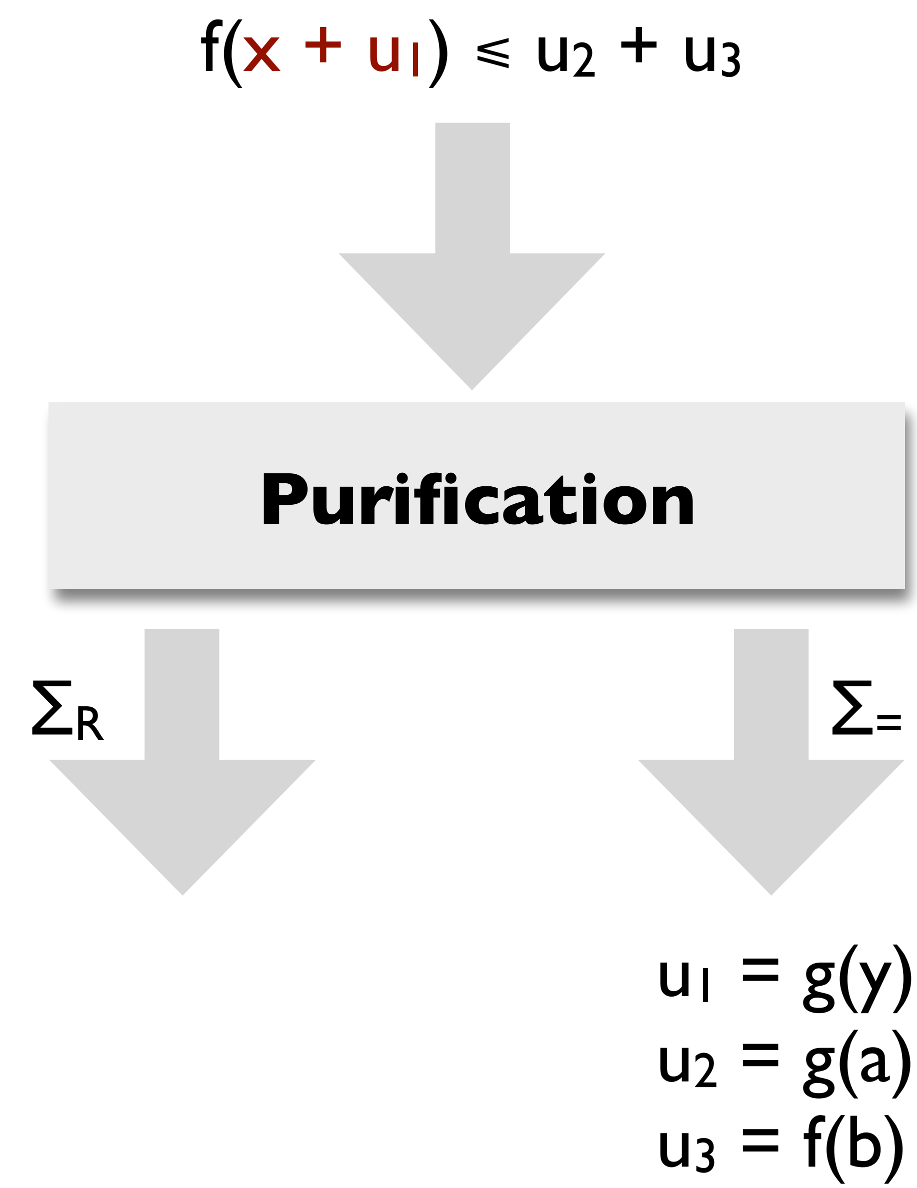


Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

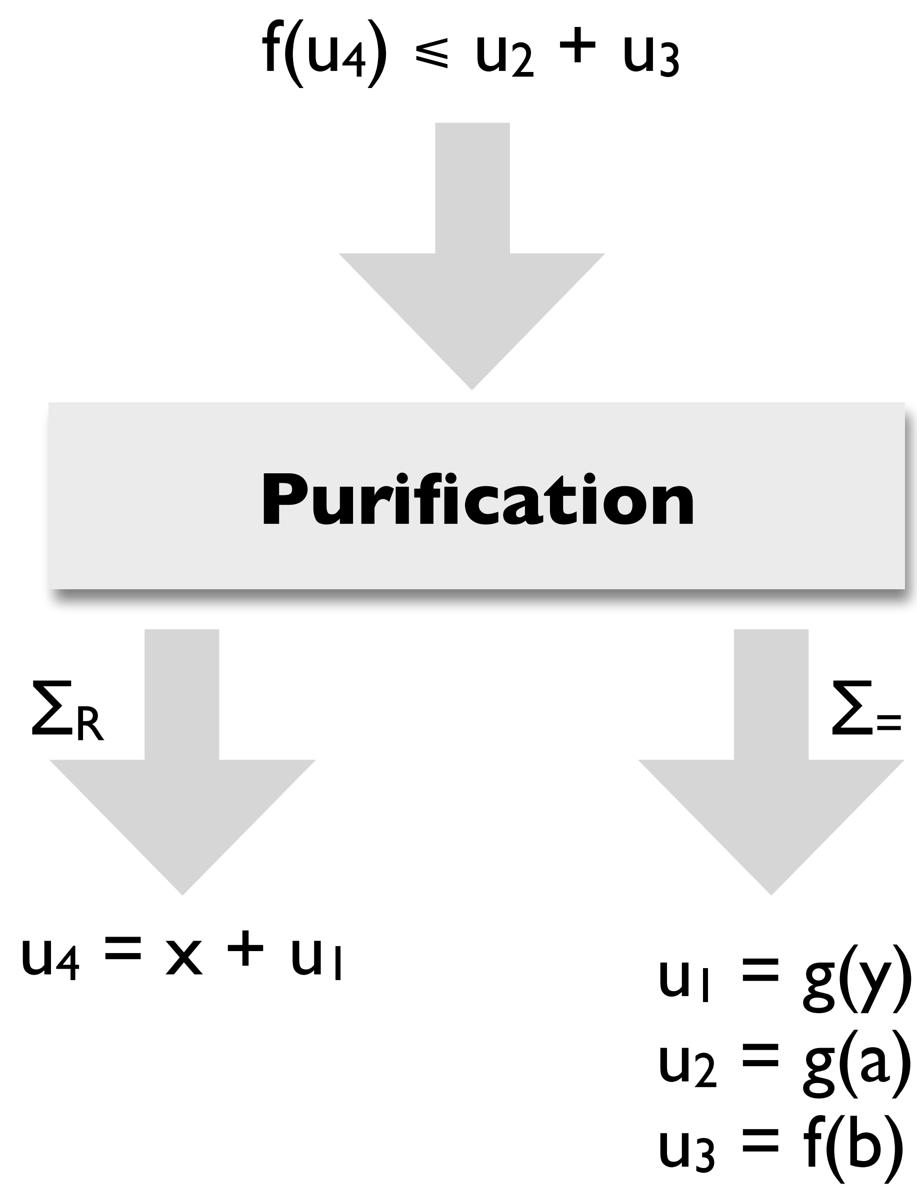


Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

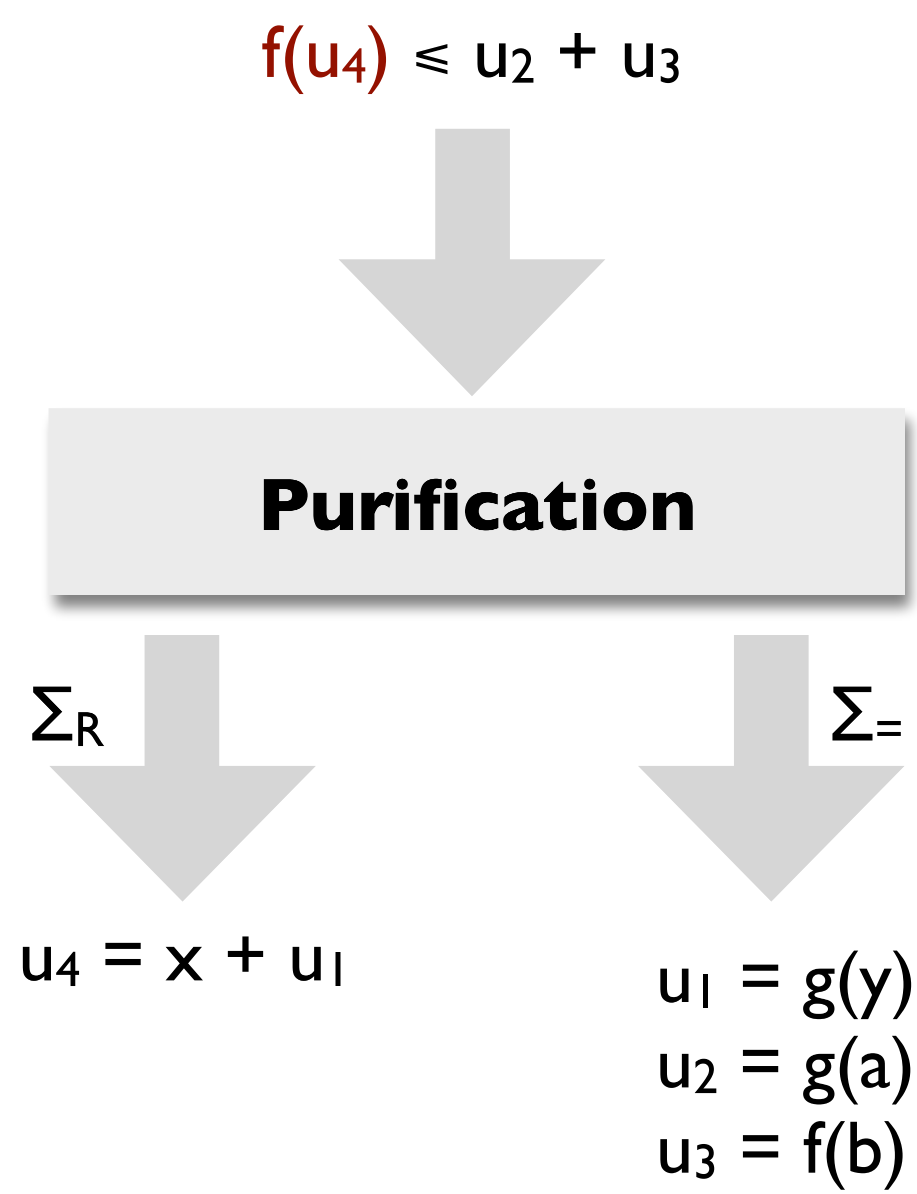


Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

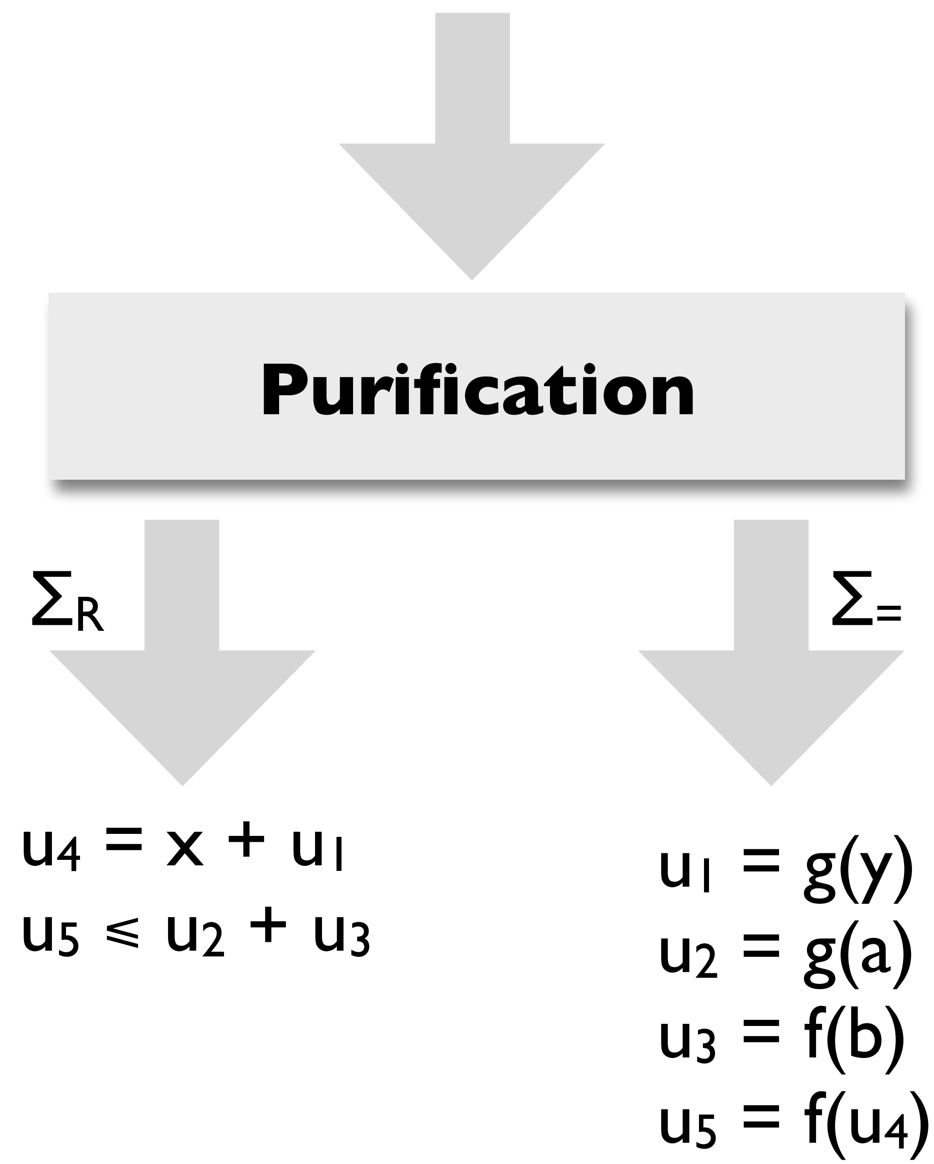


Another purification example

Transforms a $(\Sigma_1 \cup \Sigma_2)$-formula F into an equisatisfiable formula $F_1 \wedge F_2$ with F_1 in T_1 and F_2 in T_2

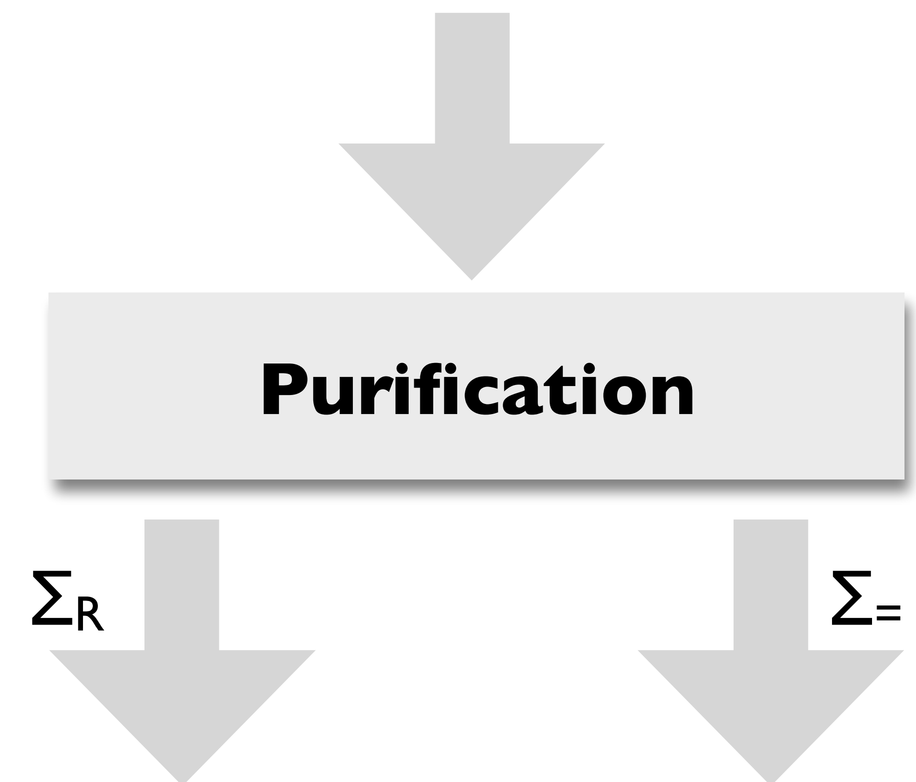
Repeat until fix point:

- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$



Shared and local variables

A variable is *shared* if it occurs in both F_1 and F_2, and it is *local* otherwise.



$u_4 = x + u_1$
$u_5 \leqslant u_2 + u_3$

$u_1 = g(y)$
$u_2 = g(a)$
$u_3 = f(b)$
$u_5 = f(u_4)$

Shared and local variables

A variable is *shared* if it occurs in both F_1 and F_2, and it is *local* otherwise.

Purification

Σ_R

$u_4 = x + u_1$

$u_5 \leqslant u_2 + u_3$

$\Sigma_=$

$u_1 = g(y)$

$u_2 = g(a)$

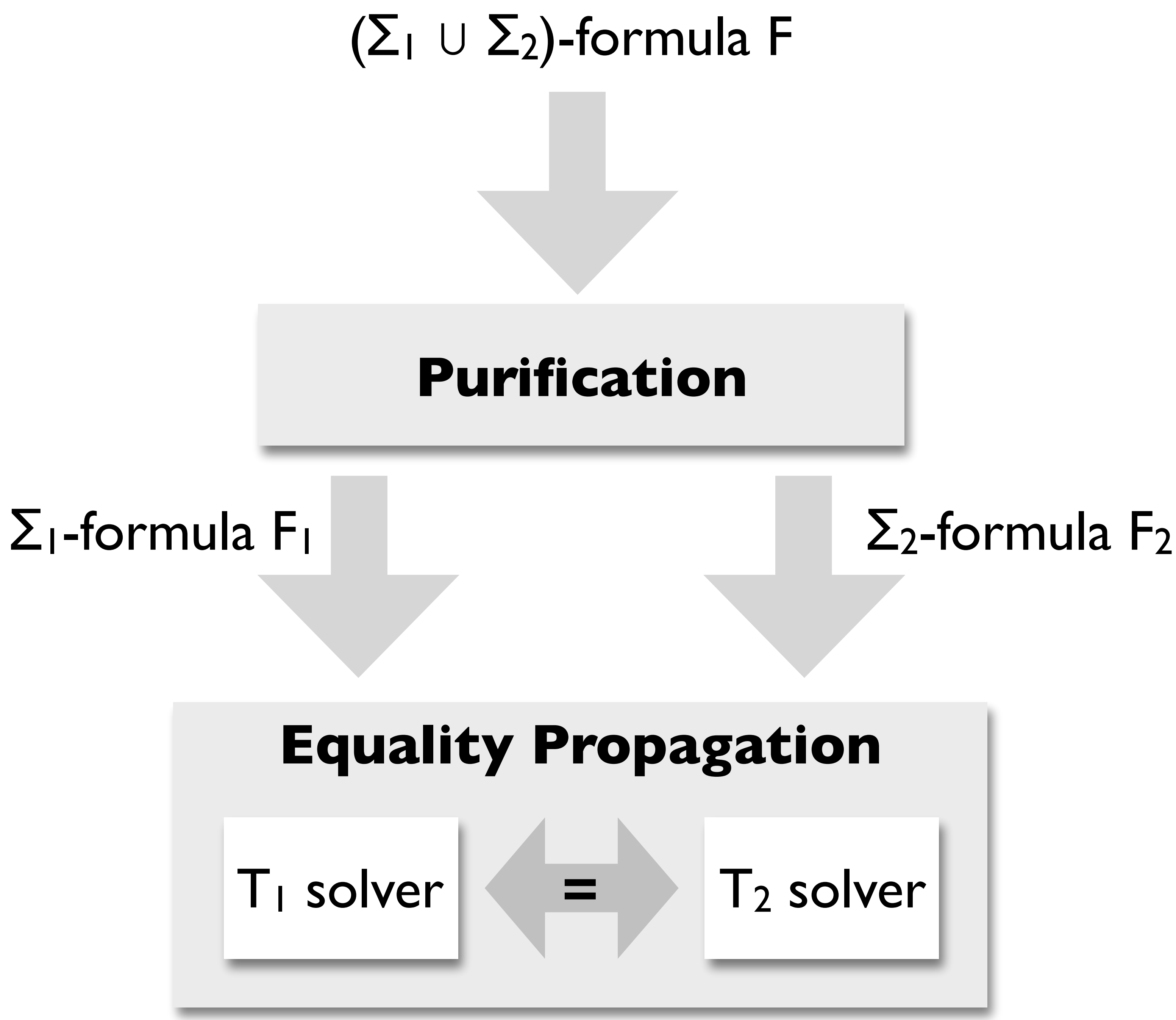
$u_3 = f(b)$

$u_5 = f(u_4)$

Shared: {u1, u2, u3, u4, u5}

Local: {x, y, a, b}

Overview of Nelson-Oppen



Overview of Nelson-Oppen

$(\Sigma_1 \cup \Sigma_2)$-formula F

Purification

Σ_1-formula F_1

Σ_2-formula F_2

Equality Propagation

- Convex theories
- Non-convex theories

Convex theories

A theory T is *convex* if for every conjunctive formula F, the following holds:

If $F \Rightarrow x_1 = y_1 \vee \ldots \vee x_n = y_n$ for a finite $n > 1$,

then $F \Rightarrow x_i = y_i$ for some $i \in \{1, \ldots, n\}$.

Convex theories

A theory T is *convex* if for every conjunctive formula F, the following holds:

If $F \Rightarrow x_1 = y_1 \vee \ldots \vee x_n = y_n$ for a finite $n > 1$,

then $F \Rightarrow x_i = y_i$ for some $i \in \{1, \ldots, n\}$.

If F implies a disjunction of equalities, then it also implies at least one of the equalities.

Examples of (non-)convex theories

Linear arithmetic over integers (T_Z)

Examples of (non-)convex theories

Linear arithmetic over integers (T_Z) ✗

$1 \leq x \wedge x \leq 2 \Rightarrow x = 1 \vee x = 2$ but

not $1 \leq x \wedge x \leq 2 \Rightarrow x = 1$

not $1 \leq x \wedge x \leq 2 \Rightarrow x = 2$

Examples of (non-)convex theories

Linear arithmetic over integers (T_Z) ✗

$1 \leq x \wedge x \leq 2 \Rightarrow x = 1 \vee x = 2$ but

not $1 \leq x \wedge x \leq 2 \Rightarrow x = 1$

not $1 \leq x \wedge x \leq 2 \Rightarrow x = 2$

Equality and uninterpreted functions ($T_=$) ✓

Linear real arithmetic (T_R) ✓

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable

Is F satisfiable if both F_1 and F_2 are satisfiable?

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable

Is F satisfiable if both F_1 and F_2 are satisfiable? **No**:

$x = 1 \wedge 2 = x + y \wedge f(x) \neq f(y)$

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.

Nelson-Oppen method for convex theories

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \land F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \land x = y$
    2. Go to step 2.
4. Return SAT

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \land F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \land x = y$
    2. Go to step 2.
4. Return SAT

$$f(f(x) - f(y)) \neq f(z) \land x \leq y \land y + z \leq x \land 0 \leq z$$

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
   1. $F_j \leftarrow F_j \wedge x = y$
   2. Go to step 2.
4. Return SAT

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

$x \leq y \wedge$ $y + z \leq x \wedge$ $0 \leq z \wedge$ $w = u - v$	$f(w) \neq f(z) \wedge$ $u = f(x) \wedge$ $v = f(y)$
Σ_R	$\Sigma_=$

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

Σ_R	$\Sigma_=$
$x \leq y \wedge$ $y + z \leq x \wedge$ $0 \leq z \wedge$ $w = u - v$	$f(w) \neq f(z) \wedge$ $u = f(x) \wedge$ $v = f(y)$
$x = y \wedge$	$x = y \wedge$

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
   1. $F_j \leftarrow F_j \wedge x = y$
   2. Go to step 2.
4. Return SAT

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

Σ_R	$\Sigma_=$
$x \leq y \wedge$ $y + z \leq x \wedge$ $0 \leq z \wedge$ $w = u - v$	$f(w) \neq f(z) \wedge$ $u = f(x) \wedge$ $v = f(y)$
$x = y \wedge$ $u = v \wedge$	$x = y \wedge$ $u = v \wedge$

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

Σ_R	$\Sigma_=$
$x \leq y \wedge$ $y + z \leq x \wedge$ $0 \leq z \wedge$ $w = u - v$	$f(w) \neq f(z) \wedge$ $u = f(x) \wedge$ $v = f(y)$
$x = y \wedge$ $u = v \wedge$ $w = z \wedge$	$x = y \wedge$ $u = v \wedge$ $w = z \wedge$

Nelson-Oppen for convex theories: example

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

Σ_R	$\Sigma_=$
$x \leq y \wedge$ $y + z \leq x \wedge$ $0 \leq z \wedge$ $w = u - v$	$f(w) \neq f(z) \wedge$ $u = f(x) \wedge$ $v = f(y)$
$x = y \wedge$ $u = v \wedge$ $w = z \wedge$	$x = y \wedge$ $u = v \wedge$ $w = z \wedge$ UNSAT

This doesn't work for non-convex theories ...

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

This doesn't work for non-convex theories ...

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

Σ_Z	$\Sigma_=$
$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$

This doesn’t work for non-convex theories …

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

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

$1 \leq x \wedge x \leq 2 \wedge z_1 = 1 \wedge z_2 = 2$	$f(x) \neq f(z_1) \wedge f(x) \neq f(z_2)$
SAT	SAT
Σ_Z	$\Sigma_=$

This doesn't work for non-convex theories ...

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

This doesn't work for non-convex theories ...

NELSON-OPPEN-CONVEX(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. Return SAT

If T is non-convex, it may imply a disjunction of equalities without implying any single equality.

We have to propagate disjunctions as well as individual equalities. Why is this possible? How do we propagate disjunctions to theory solvers which only reason about conjunctions?

Nelson-Oppen method for non-convex theories

NELSON-OPPEN(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. If $F_i \Rightarrow x_1 = y_1 \vee \ldots \vee x_n = y_n$ but F_j does not, then if NELSON-OPPEN($F_i \wedge F_j \wedge x_k = y_k$) outputs SAT for any k, return SAT. Otherwise, return UNSAT.
5. Return SAT

Nelson-Oppen method for non-convex theories

NELSON-OPPEN(F)

1. Purify F into $F_1 \wedge F_2$
2. Run T_1-solver on F_1 and T_2-solver on F_2 and return UNSAT if either is unsatisfiable
3. If there are shared variables x and y such that $F_i \Rightarrow x = y$ but F_j does not
    1. $F_j \leftarrow F_j \wedge x = y$
    2. Go to step 2.
4. If $F_i \Rightarrow x_1 = y_1 \vee \ldots \vee x_n = y_n$ but F_j does not, then if NELSON-OPPEN($F_i \wedge F_j \wedge x_k = y_k$) outputs SAT for any k, return SAT. Otherwise, return UNSAT.
5. Return SAT

Propagate a *minimal* disjunction.

Nelson-Oppen for non-convex theories: example

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

Nelson-Oppen for non-convex theories: example

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

Σ_Z	$\Sigma_=$
$1 \leq x \wedge$	$f(x) \neq f(z_1) \wedge$
$x \leq 2 \wedge$	$f(x) \neq f(z_2)$
$z_1 = 1 \wedge$	
$z_2 = 2$	

Nelson-Oppen for non-convex theories: example

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

$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$
$(x=z_1 \vee x=z_2) \wedge$ Σ_Z	 $\Sigma_=$

Nelson-Oppen for non-convex theories: example

$$1 \le x \wedge x \le 2 \wedge$$
$$f(x) \ne f(1) \wedge f(x) \ne f(2)$$

$1 \le x \wedge$ $x \le 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \ne f(z_1) \wedge$ $f(x) \ne f(z_2)$
$(x=z_1 \vee x=z_2) \wedge$	
Σ_Z	$\Sigma_=$

$1 \le x \wedge$ $x \le 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \ne f(z_1) \wedge$ $f(x) \ne f(z_2)$
$x = z_1$	$x = z_1 \wedge$ UNSAT

Nelson-Oppen for non-convex theories: example

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

$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$
$(x=z_1 \vee x=z_2) \wedge$ Σ_Z	$\Sigma_=$

$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$
$x = z_1$	$x = z_1 \wedge$ UNSAT

$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$
$x = z_2$	$x = z_2 \wedge$ UNSAT

Complexity of Nelson-Oppen

If decision procedures for convex theories T_1 and T_2 have polynomial time complexity, so does their Nelson-Oppen combination.

If decision procedures for convex theories T_1 and T_2 have NP time complexity, so does their Nelson-Oppen combination.

Summary

Today

- Sound and complete procedure for a combination of restricted theories
- Stably infinite, conjunctive, quantifier-free, signatures disjoint except for =

Next lecture

- Deciding satisfiability of arbitrary boolean combinations of quantifier-free first-order formulas