Computer-Aided Reasoning for Software

CSE507

Combining Theories

Today

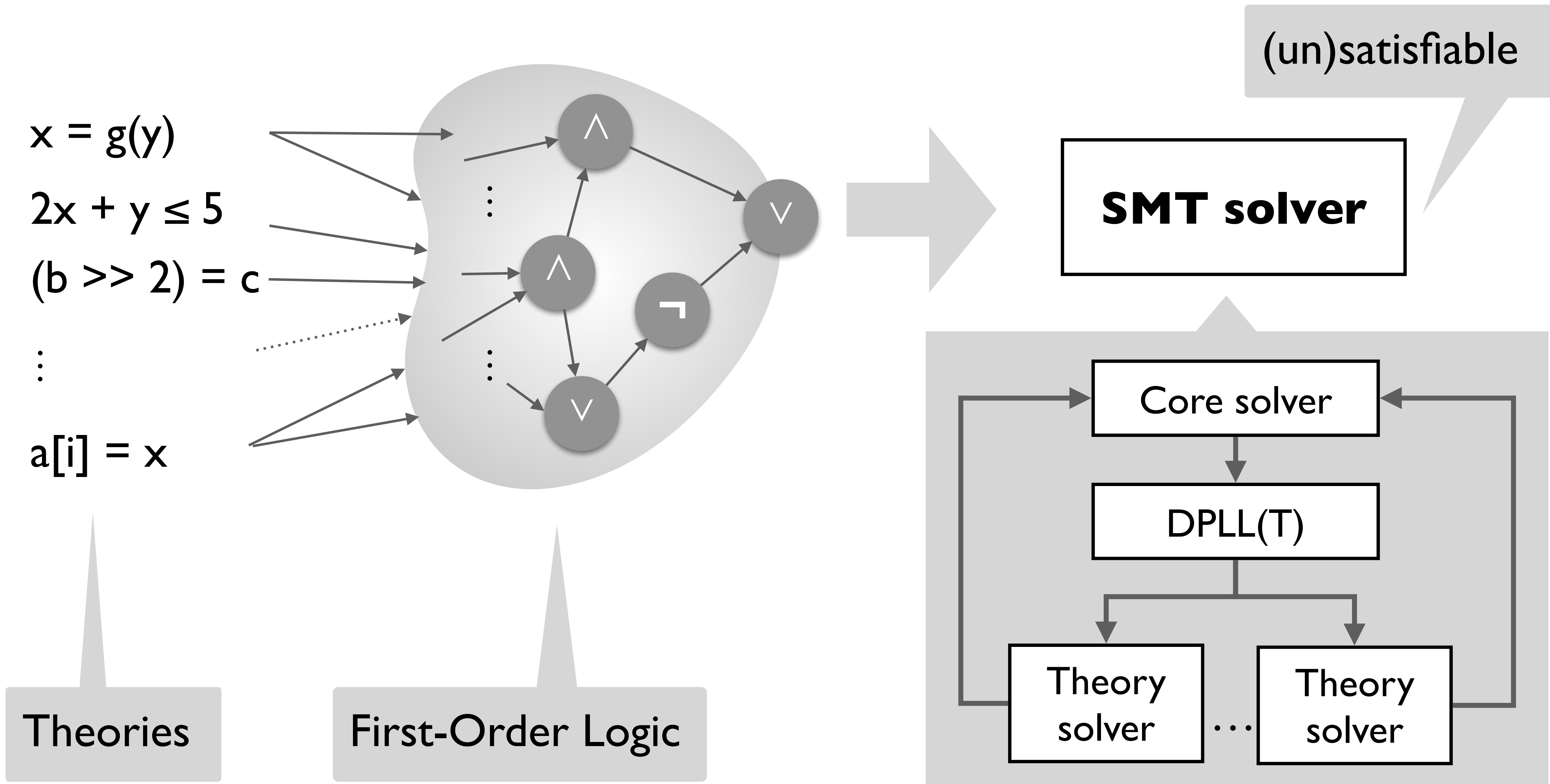
Last lecture

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

Today

- Deciding a combination of theories

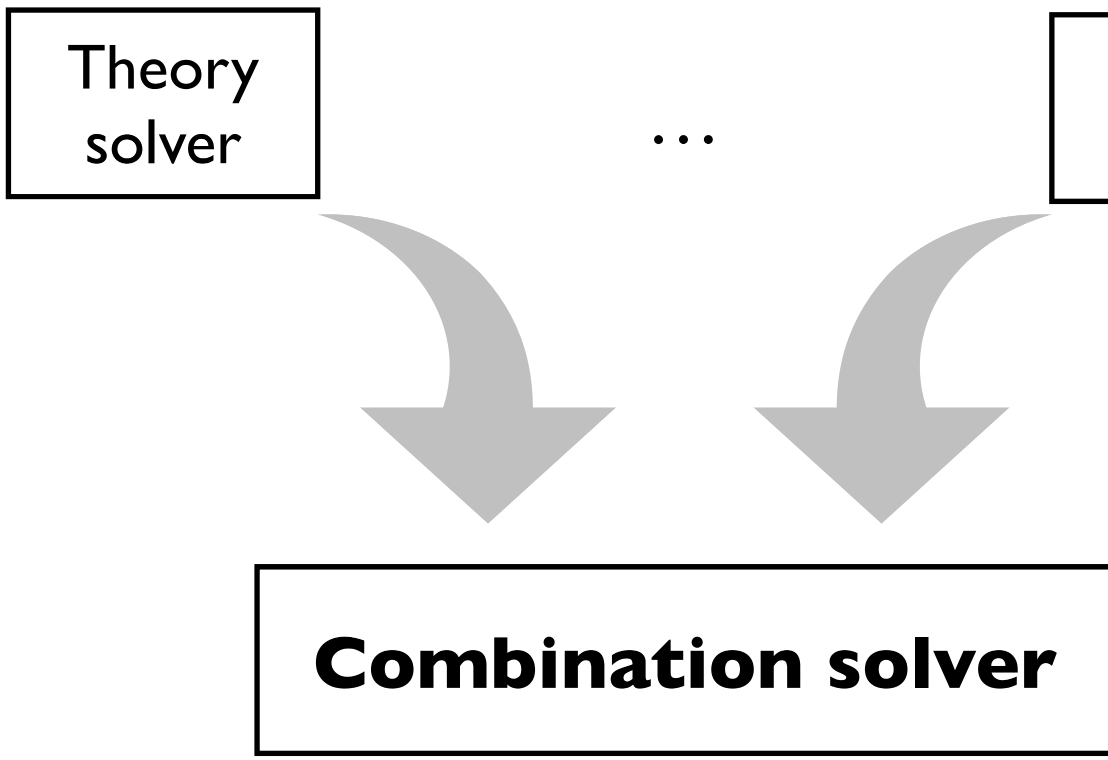
Recall: Satisfiability Modulo Theories (SMT)



Combining theories with Nelson-Oppen

Σ_1-theory T_1
with axioms A_1

Σ_2-theory T_2
with axioms A_2



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

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

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 decidable, quantifier-free conjunctive fragments
- Equality (=) is the only interpreted symbol in the intersection of their signatures: $\Sigma_1 \cap \Sigma_2 = \{ = \}$
- Both are **stably infinite**

A theory T is stably infinite if 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: $\forall x . x = a \lor x = b$

Equality and uninterpreted functions ($T_=$)

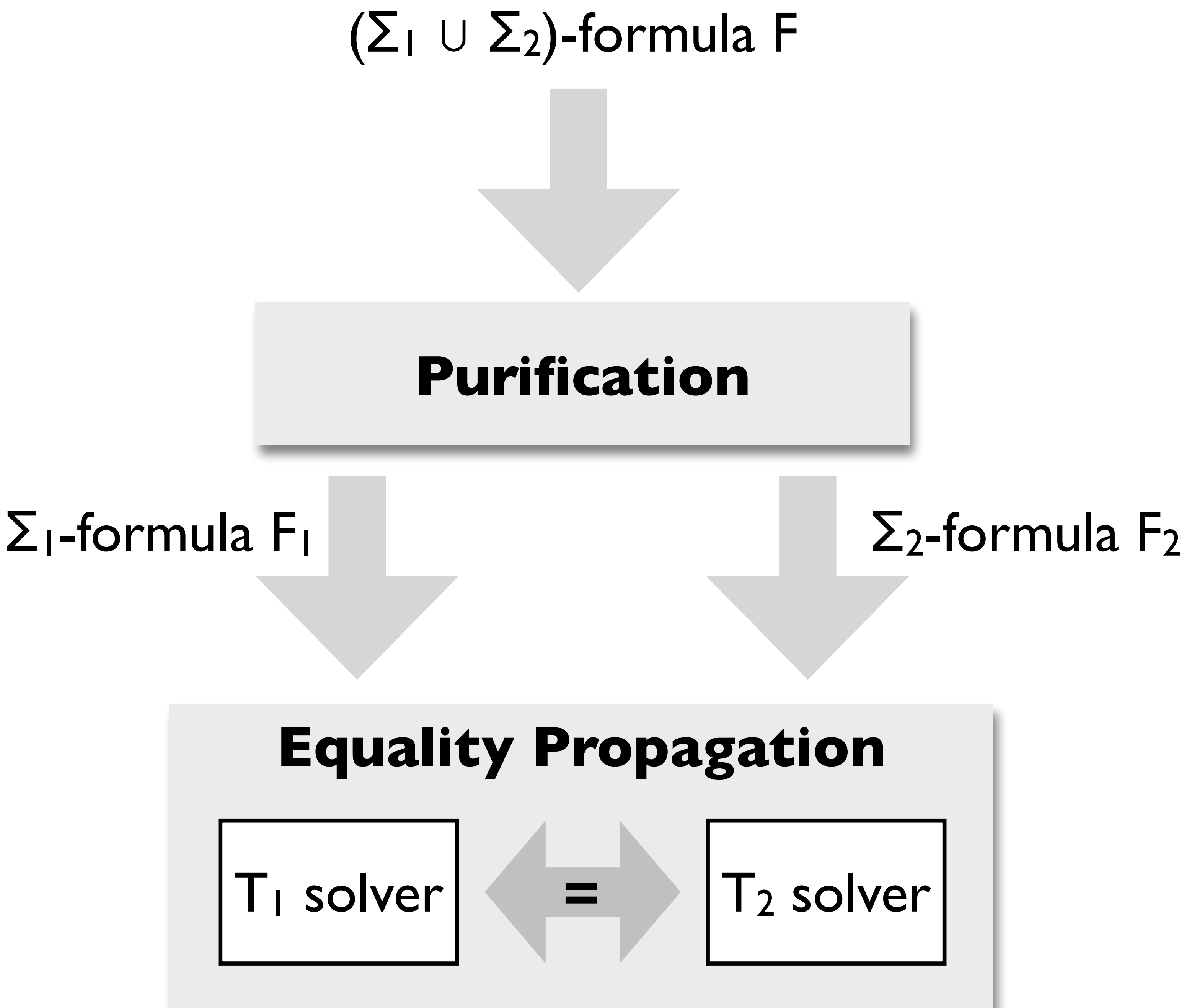
Fixed width bit vectors (T_{bv})

Linear real arithmetic (T_R)

Arrays (T_A)

Linear integer arithmetic (T_R)

Overview of Nelson-Oppen

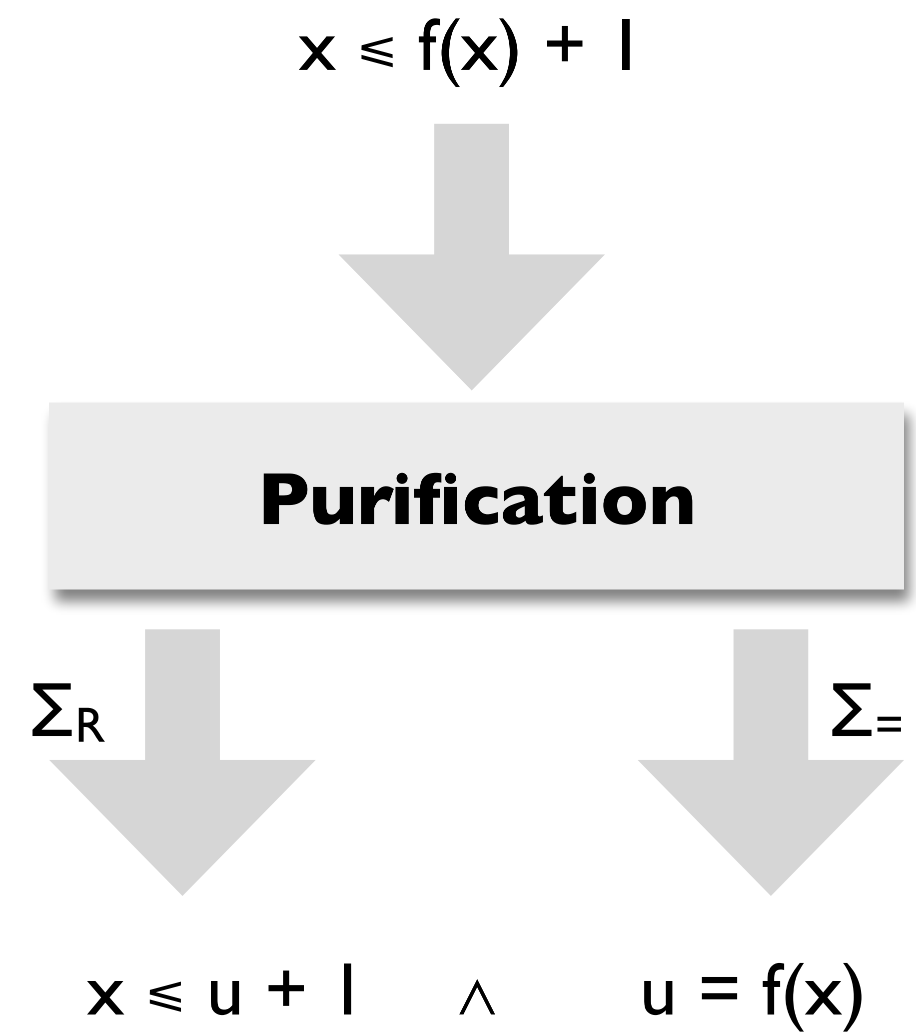


Overview of purification

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

Repeat until fix point:

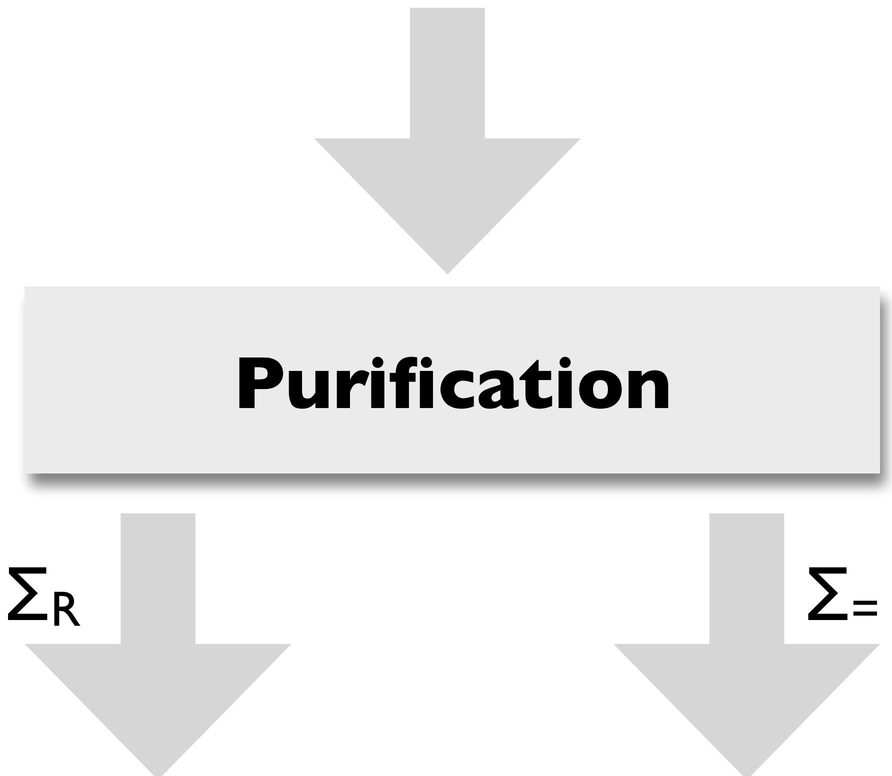
- If f is in T_i and t is not, and u is fresh:
  $F[f(\ldots, t, \ldots)] \rightsquigarrow F[f(\ldots, u, \ldots)] \wedge u = t$
- If p is in T_i and t is not, and v is fresh:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$



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

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



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:
  $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

$f(x + u_1) \leq u_2 + u_3$

Purification

Σ_R

$\Sigma_=$

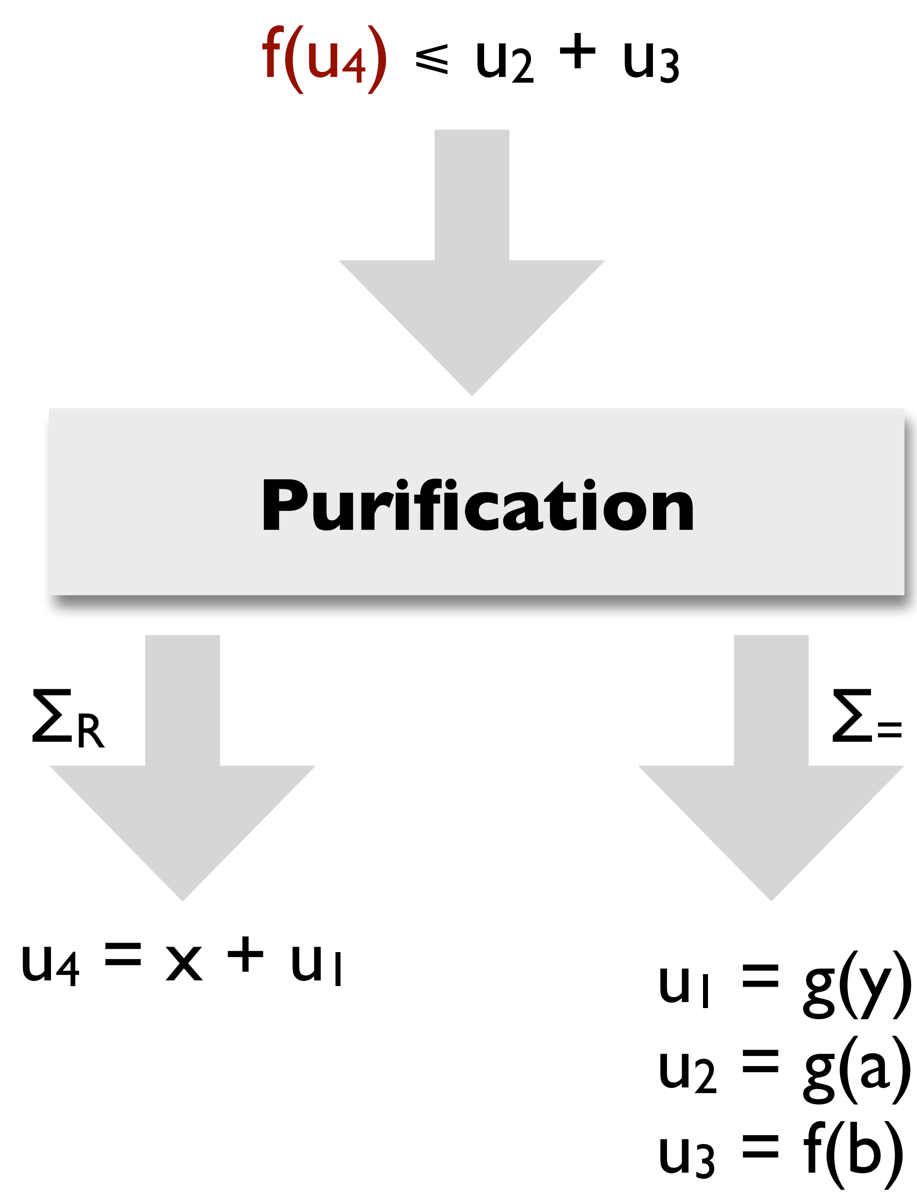
$u_1 = g(y)$
$u_2 = g(a)$
$u_3 = f(b)$

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: $F[p(\ldots, t, \ldots)] \rightsquigarrow F[p(\ldots, v, \ldots)] \wedge v = t$

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 and local constants

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

Purification

Σ_R

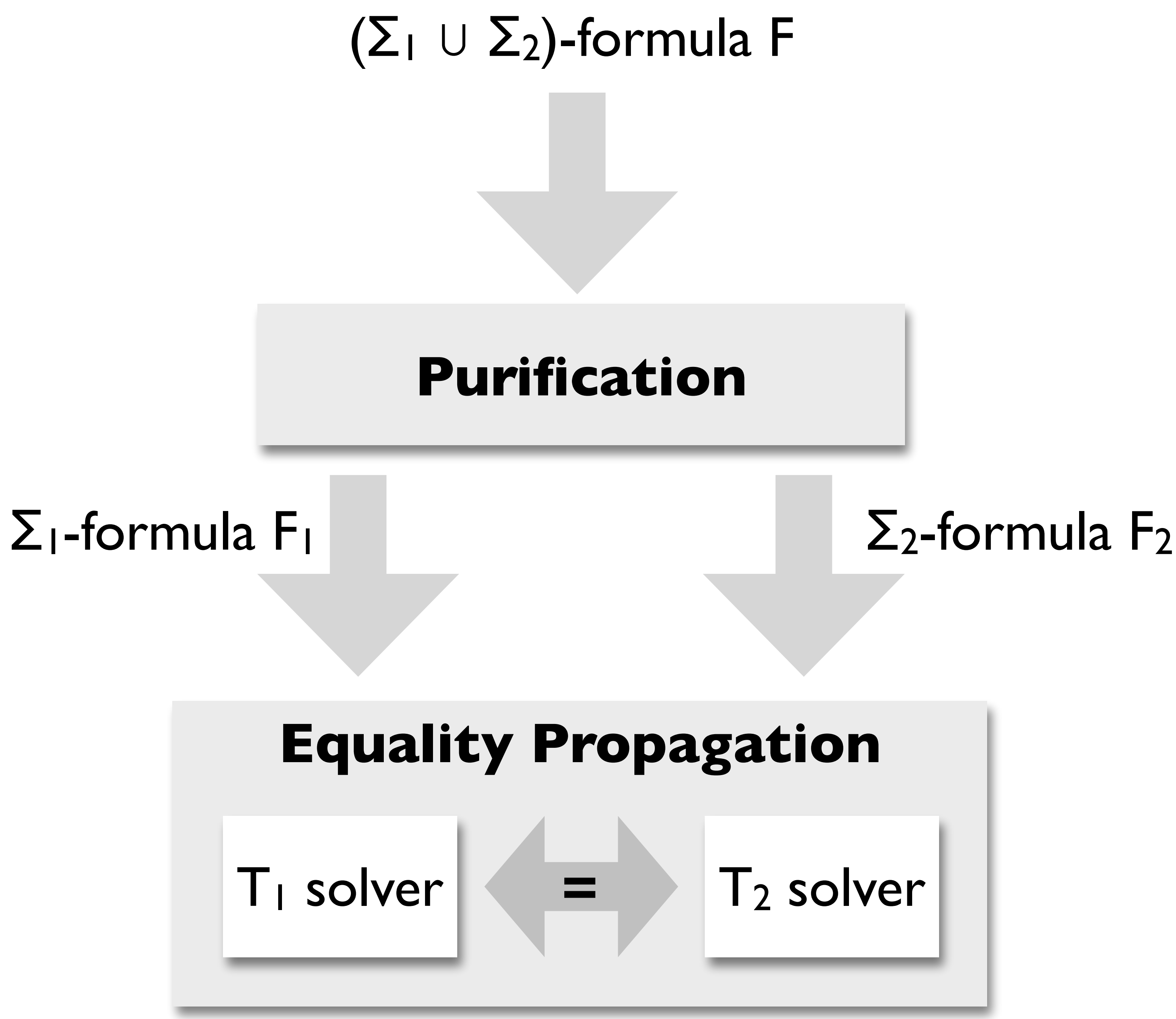
$u_4 = x + u_1$
$u_5 \leq u_2 + u_3$

$\Sigma_=$

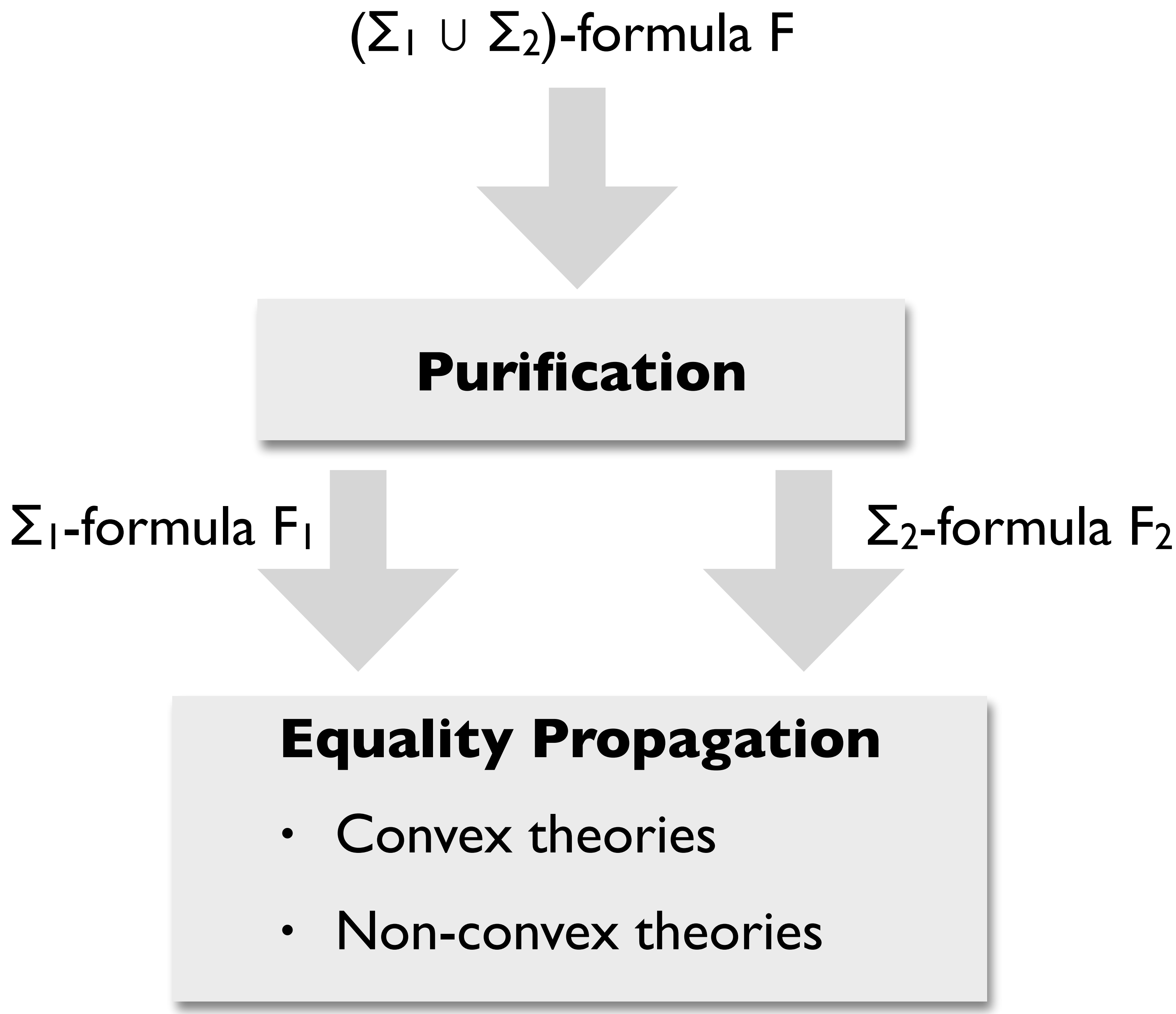
$u_1 = g(y)$
$u_2 = g(a)$
$u_3 = f(b)$
$u_5 = f(u_4)$

Shared: $\{u_1, u_2, u_3, u_4, u_5\}$
Local: $\{x, y, a, b\}$

Overview of Nelson-Oppen



Overview of Nelson-Oppen



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) ✗

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

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 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 constants 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

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

Σ_R	$\Sigma_=$
$x \leq y \land$ $y + z \leq x \land 0$ $\leq z \land$ $w = u - v$	$f(w) \neq f(z) \land$ $u = f(x) \land$ $v = f(y)$
$x = y \land$ $u = v \land$ $w = z \land$	$x = y \land$ $u = v \land$ $w = z \land$ 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 constants 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	$\Sigma_=$
$1 \leq x \wedge$ $x \leq 2 \wedge$ $z_1 = 1 \wedge$ $z_2 = 2$	$f(x) \neq f(z_1) \wedge$ $f(x) \neq f(z_2)$
SAT	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 constants 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. Which disjunctions? How do we propagate disjunctions to theory solvers which reason only about conjunctions?

Nelson-Oppen 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 constants 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

$1 \le x \land x \le 2 \land$
$f(x) \neq f(1) \land f(x) \neq f(2)$

$1 \le x \land$ $x \le 2 \land$ $z_1 = 1 \land$ $z_2 = 2$	$f(x) \neq f(z_1) \land$ $f(x) \neq f(z_2)$
$(x=z_1 \lor x=z_2) \land$	
Σ_Z	$\Sigma_=$

$1 \le x \land$ $x \le 2 \land$ $z_1 = 1 \land$ $z_2 = 2$	$f(x) \neq f(z_1) \land$ $f(x) \neq f(z_2)$
$x = z_1$	$x = z_1 \land$ UNSAT

$1 \le x \land$ $x \le 2 \land$ $z_1 = 1 \land$ $z_2 = 2$	$f(x) \neq f(z_1) \land$ $f(x) \neq f(z_2)$
$x = z_2$	$x = z_2 \land$ UNSAT

Soundness and completeness of Nelson-Oppen

If the theories T_1 and T_2 satisfy Nelson-Open restrictions, then the combination procedure returns UNSAT for a formula F in $T_1 \cup T_2$ iff F is unsatisfiable modulo $T_1 \cup T_2$.

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 non-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 with signatures that are disjoint except for =

Next lecture

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