CS 292C Computer-Aided Reasoning for Software

Lecture 8: Combining Theories

Yu Feng

Fall 2020

Summary of previous lecture

- 2nd homework was out (last week)
- Proposal will be due in two days
- SAT Modulo Theories

Theory of equality with uninterpreted functions

- **Signature: {=, x, y, z, …, f, g, …, p, q, …}**
  - The binary predicate = is *interpreted*.
  - All constant, function, and predicate symbols are *uninterpreted.*
- **Axioms**
  - $\forall x.\ x = x$
  - $\forall x,y.\ x=y \rightarrow y=x$
  - $\forall x,y,z.\ x=y \wedge y=z \rightarrow x=z$
  - $\forall x_1,\ldots,x_n,y_1,\ldots,y_n.(x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \rightarrow (f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n))$
  - $\forall x_1,\ldots,x_n,y_1,\ldots,y_n.(x_1 = y_1 \wedge \ldots \wedge x_n = y_n) \rightarrow (p(x_1,\ldots,x_n) \leftrightarrow p(y_1,\ldots,y_n))$
- **Deciding $T_=$**
  - Conjunctions of literals modulo $T_=$ is decidable in polynomial time.

Theory of linear integer and real

Signature

- Integers (or reals)
- Arithmetic operations: multiplication by an integer (or real) number, +, -.
- Predicates: =, $\leq$.
- Expanded with all constant symbols: x, y, z, ...

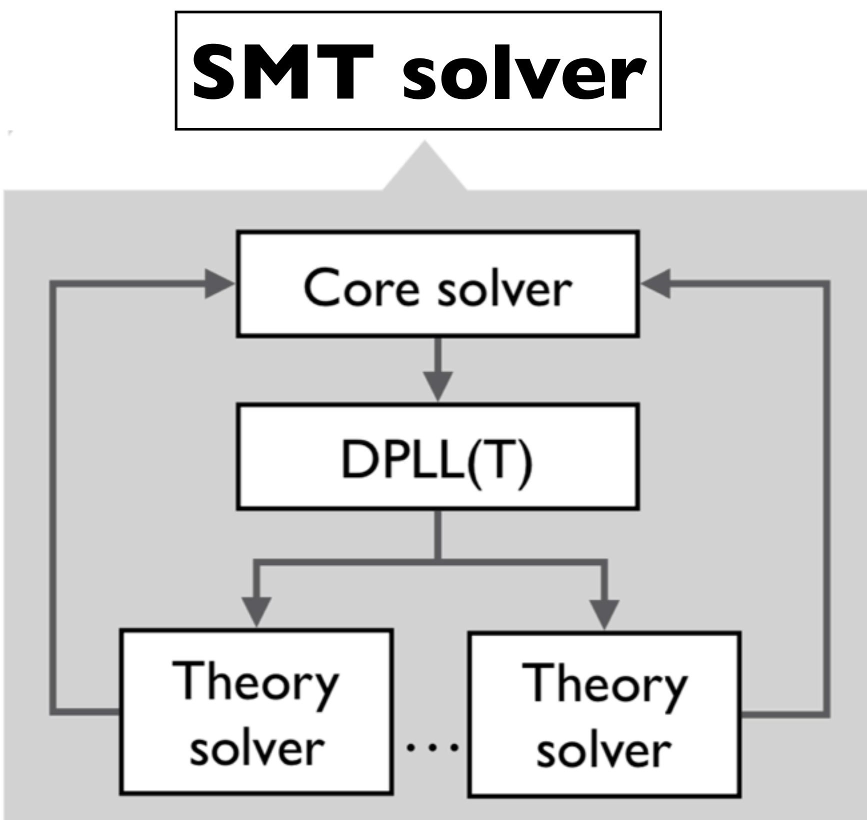
Deciding T_{LIA} and T_{LRA}

- NP-complete for linear integer arithmetic (LIA). Polynomial time for linear real arithmetic (LRA).
- Polynomial time for difference logic (conjunctions of the form $x - y \leq c$, where c is an integer or real number).

Outline of this lecture

- Deciding a combination of theories
- The Nelson-Oppen algorithm

Combine theories



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

This formula does not belong to any individual theory. $T_= \cup T_{LIA}$

Combine theories

Σ_1-theory T_1
with axioms A_1

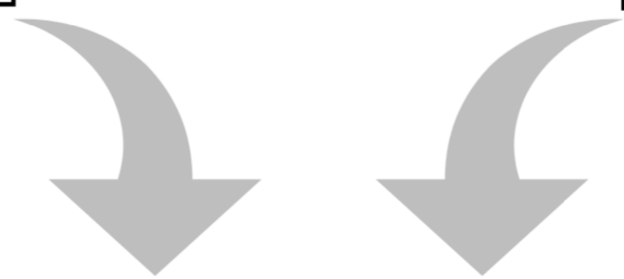
Theory solver

...

Σ_n-theory T_n
with axioms A_n

Theory solver

We will study how to combine two theories in this lecture



Combination solver

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

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
- 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.

Stably infinite

Σ_T: {a,b,=}

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

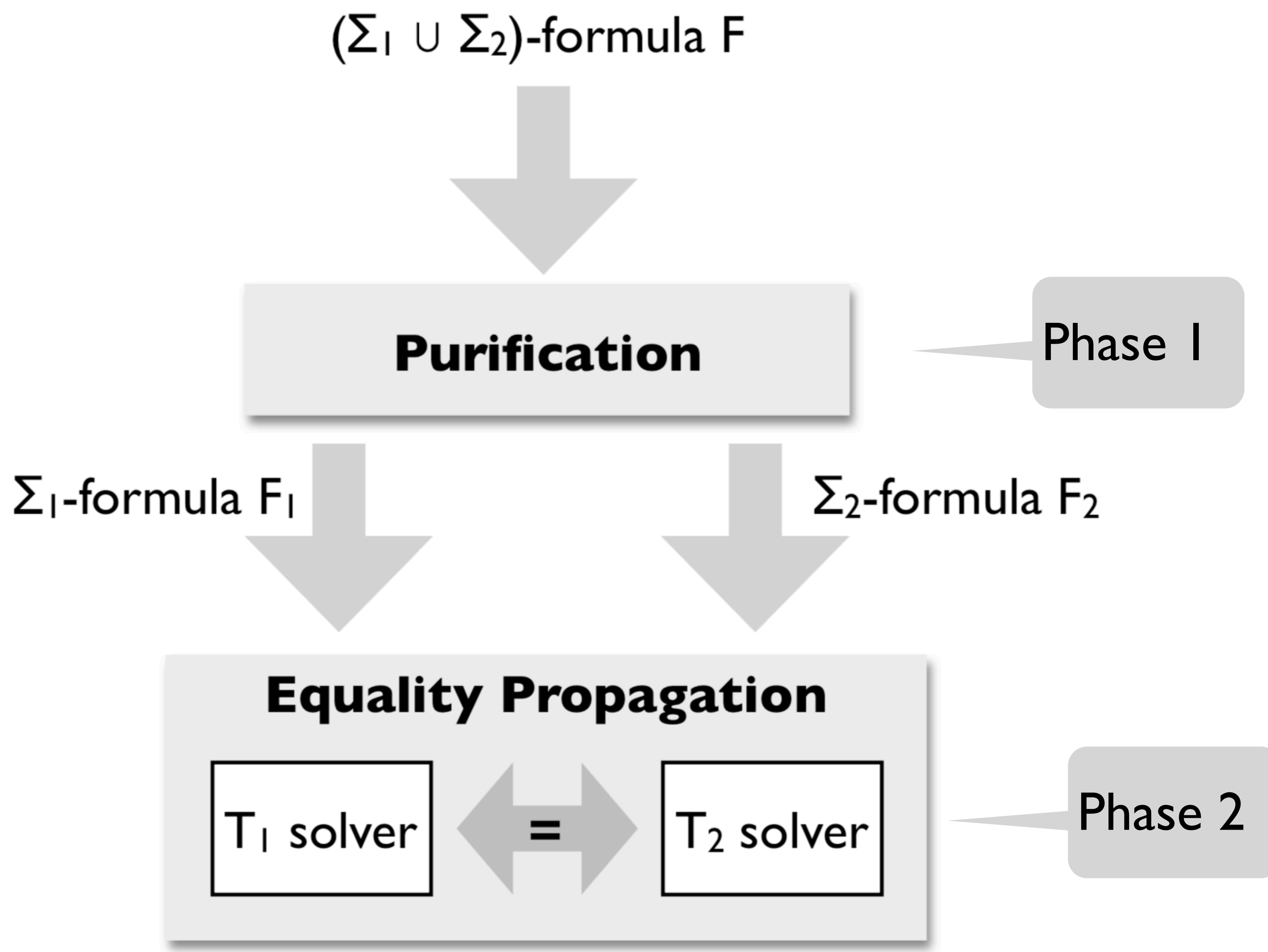
Equality and uninterpreted functions ($T_=$)

Arrays (T_A)

Linear real arithmetic (T_{LRA})

Linear integer arithmetic (T_{LIA})

Overview of Nelson-Oppen



Phase 1: 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

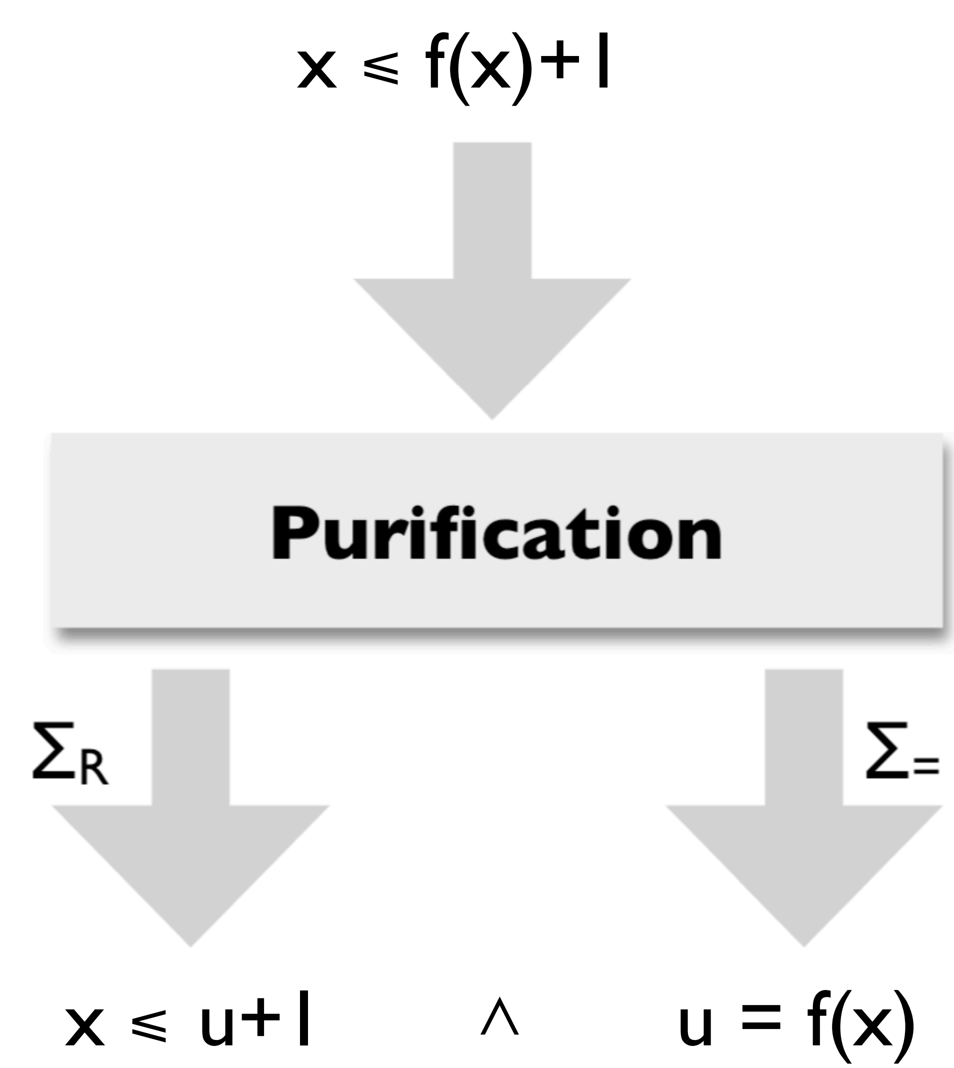
Repeat until fix point:

- 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:

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



Phase 1: Purification

A constant is *shared* if it occurs in both F_1 and F_2

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

Purification

Σ_R

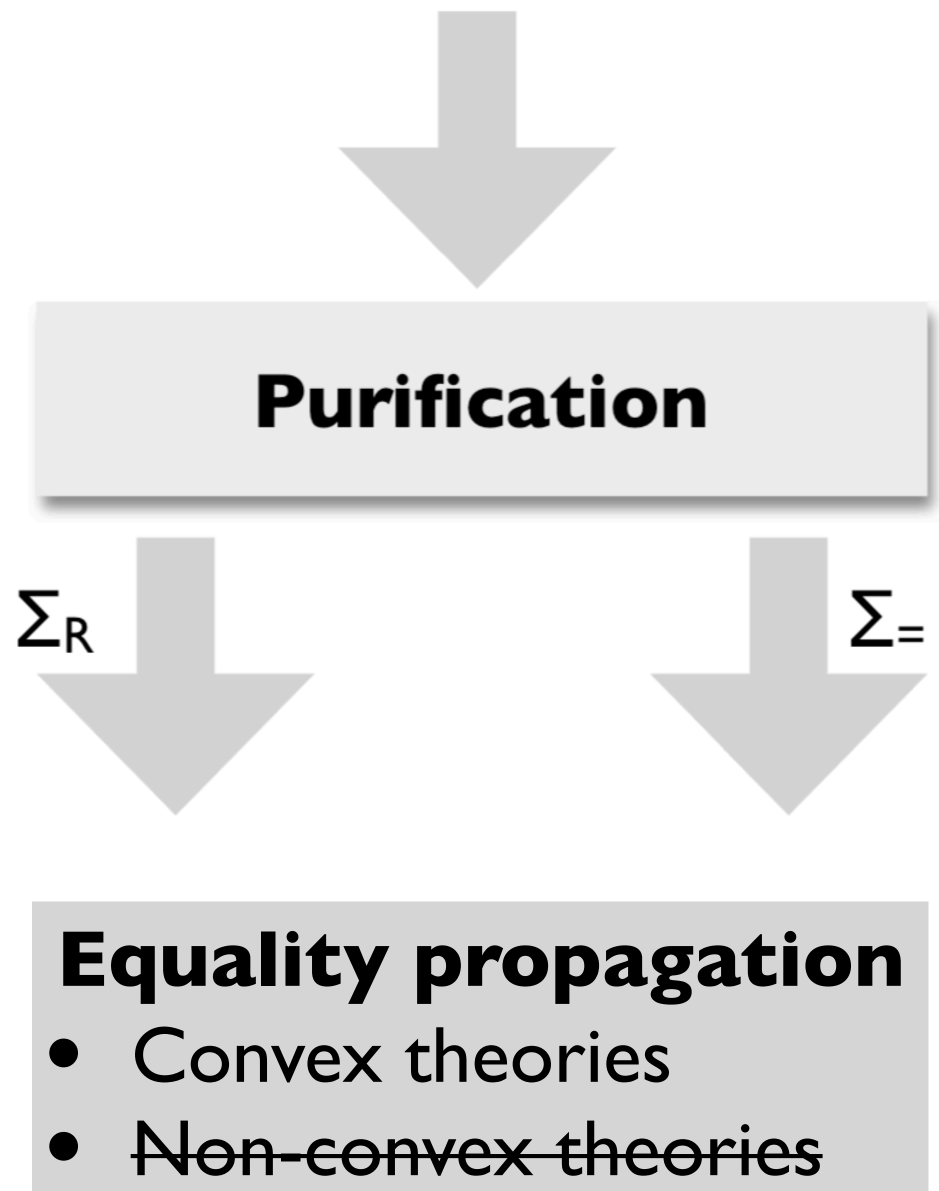
$\Sigma_=$

Shared: $\{w_3, w_1, w_2, x, y, z\}$
Local: $\{\}$

$$w_3 = w_1 - w_2 \wedge x \leq y \wedge y + z \leq x \wedge 0 \leq z$$

$$w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z)$$

Phase 2: Equality propagation



Phase 2: Equality propagation

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 $n>1$, 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.

Linear integer arithmetic (T_{LIA}) ✗

$1 \leq x \wedge x \leq 2 \Rightarrow x = 1 \vee x = 2$
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_{LRA}) ✓

Nelson-Oppen 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 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

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

Purification

Σ_R

$w_3 = w_1 - w_2 \land x \leq y \land y + z \leq x \land 0 \leq z$

$\Sigma_=$

$w_1 = f(x) \land w_2 = f(y) \land f(w_3) \neq f(z)$

TODOs by next lecture

- DPLL (T) algorithm
- Proposal will be due