Deciding a Combination of Theories

Ming-Hsien Tsai, FLOLAC 2025

Based on Daniel Kroening and Ofer Strichman: Decision Procedures - An Algorithmic Point of View

Introduction

- We have seen decision procedures that focus on one specific theory
- Verification conditions that arise in practice, however, frequently mix expressions from several theories
  - Linear arithmetic + uninterpreted functions
    - $(x_2 \geq x_1) \wedge (x_1 - x_3 \geq x_2) \wedge (x_3 \geq 0) \wedge f(f(x_1) - f(x_2)) \neq f(x_3)$
  - Bit vectors + uninterpreted functions: $f(a[32], b[1]) = f(b[32], a[1]) \wedge a[32] = b[32]$
  - Arrays + linear arithmetic: $x = v\{i \leftarrow e\}[j] \wedge y = v[j] \wedge x > e \wedge x > y$
- Methods for combining decision procedures: Nelson–Oppen, Shostak's Method, DTC (Delayed Theory Combination), Model-based

Recall

- A theory is defined over a signature Σ, which is a set of nonlogical symbols (i.e., function and predicate symbols)
- If T is such a theory, we say it is a Σ-**theory**
- Let T be a Σ-theory
  - A Σ-formula φ is T-**satisfiable** if there exists an interpretation that satisfies both φ and T
  - A Σ-formula φ is T-**valid**, denoted $T \vDash \varphi$, if all interpretations that satisfy T also satisfy φ

Theory Combination

- Theory combination
  - Given two theories T_1 and T_2 with signatures Σ_1 and Σ_2, respectively, the theory combination $T_1 \oplus T_2$ is a $(\Sigma_1 \cup \Sigma_2)$-theory defined by the axiom set $T_1 \cup T_2$
- Theory combination problem
  - Let φ be a $\Sigma_1 \cup \Sigma_2$ formula. The theory combination problem is to decide whether φ is $T_1 \oplus T_2$-valid. Equivalently, the problem is to decide whether the following holds:
    - $T_1 \oplus T_2 \models \varphi$
- Under certain restrictions on the combined theories, the combination problem becomes decidable

Convex Theory

- Convex theory:
  - A Σ-theory T is ***convex*** if for every conjunctive Σ-formula φ:
    - $(\varphi \Rightarrow \bigvee_{i=1}^{n} x_i = y_i)$ is T-valid for some **finite** $n > 1$ $\Rightarrow$ $(\varphi \Rightarrow x_i = y_i)$ is T-valid for some $i \in \{1,\ldots,n\}$
  - where x_i, y_i, for $i \in \{1,\ldots,n\}$, are some variables
- In other words, in a convex theory T, if a formula T-implies a disjunction of equalities, it also T-implies at least one of these equalities separately

Examples of Convex and Nonconvex Theories

- Linear arithmetic over $\mathbb{R}$ is convex
  - A conjunction of linear arithmetic predicates defines a set of values which can be empty, a singleton, or infinitely large
  - Empty case: $x \leq 2 \wedge x \geq 3 \Rightarrow ?$
  - Singleton case: $x \leq 3 \wedge x \geq 3 \Rightarrow x = 3$
  - Infinitely large case: $2 \leq x \wedge x \leq 3 \Rightarrow \underbrace{x = 2 \vee x = 2.1 \wedge x = 2.2 \wedge \cdots}_{\text{infinitely many}}$

Examples of Convex and Nonconvex Theories (cont'd)

- Linear arithmetic over $\mathbb{Z}$ is not convex
  - Example: $x_1 = 1 \wedge x_2 = 2 \wedge 1 \leq x_3 \wedge x_3 \leq 2 \Rightarrow (x_3 = x_1 \vee x_3 = x_2)$
    - Neither $x_1 = 1 \wedge x_2 = 2 \wedge 1 \leq x_3 \wedge x_3 \leq 2 \Rightarrow x_3 = x_1$ nor
    - $x_1 = 1 \wedge x_2 = 2 \wedge 1 \leq x_3 \wedge x_3 \leq 2 \Rightarrow x_3 = x_2$ holds

Examples of Convex and Nonconvex Theories (cont'd)

- The conjunctive fragment of equality logic is convex
  - A conjunction of equalities and disequalities defines sets of variables that are equal (equality sets) and sets of variables that are different
  - It implies any equality between variables in the same equality set separately
- Many theories used in practice are in fact nonconvex
- Nonconvex theories are computationally harder to be combine with other theories

Nelson-Oppen Restrictions

- The Nelson–Oppen combination procedure solves the theory combination problem for theories that comply with several restrictions
- Nelson-Oppen restrictions: In order for the Nelson-Oppen procedure to be applicable, the theories $T_1, \ldots, T_n$ should comply with the following restrictions (which can be overcame by extensions):
  1. $T_1, \ldots, T_n$ are quantifier-free first-order theories with equality
  2. There is a decision procedure for each of the theories $T_1, \ldots, T_n$
  3. The signatures are disjoint, i.e., for all $1 \leq i < j \leq n$, $\Sigma_i \cap \Sigma_j = \varnothing$
  4. $T_1, \ldots, T_n$ are theories that are interpreted over an infinite domain (e.g., linear arithmetic over $\mathbb{R}$, but not the theory of finite-width bit vectors)

Nelson-Oppen for Convex Theories

Algorithm Nelson-Oppen-for-Convex-Theories

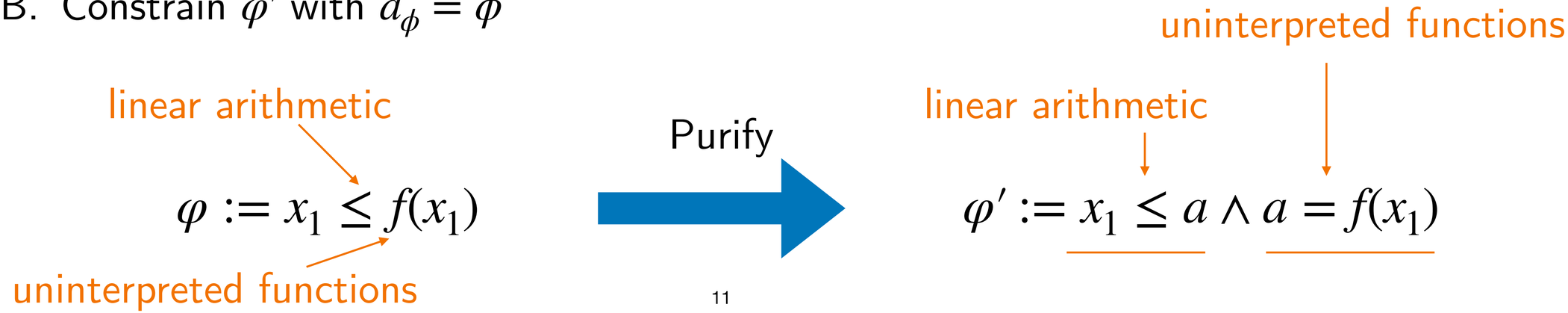
Input: a convex formula φ that mixes convex theories, with Nelson-Oppen restrictions

Output: "Satisfiable" if φ is satisfiable, and "Unsatisfiable" otherwise

1. Purification: Purify φ into $F_1, \ldots, F_n$
2. Apply the decision procedure for T_i to F_i. If there exists i such that F_i is unsatisfiable in T_i, return "Unsatisfiable".
3. Equality propagation: If there exist i, j such that F_i T_i-implies an equality between variables of φ that is not T_j-implied by F_j, add this equality to F_j and go to step 2.
4. Return "Satisfiable".

Purification

- Given a formula φ, purification generates an equisatisfiable formula φ' as follows:
  1. Let $\varphi' := \varphi$
  2. For each "alien" subexpression ϕ in φ':
     A. Replace ϕ with a new auxiliary variable a_ϕ
     B. Constrain φ' with $a_\phi = \phi$



After Purification

- After purification, we are left with a set of pure expressions $F_1, \ldots, F_n$ such that
  - For all i, F_i belongs to theory T_i and is a conjunction of T_i-literals
  - Shared variables are allowed, i.e., it is possible that for some i, j, $i \leq i < j \leq n$, $var(F_i) \cap var(F_j) \neq \emptyset$
  - The formula φ is satisfiable in the combined theory if and only if $\wedge_{i=1}^{n} F_i$ is satisfiable in the combined theory

Application of Nelson-Oppen-for-Convex-Theories

- $\varphi := (f(x_1,0) \geq x_3) \wedge (f(x_2,0) \leq x_3) \wedge (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge (x_3 - f(x_1,0) \geq 1)$
- Purify steps:
  - $(f(x_1, a_0) \geq x_3) \wedge (f(x_2, a_0) \leq x_3) \wedge (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge (x_3 - f(x_1, a_0) \geq 1) \wedge$
  - $(a_0 = 0)$
  - $(a_1 \geq x_3) \wedge (f(x_2, a_0) \leq x_3) \wedge (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge (x_3 - a_1 \geq 1) \wedge$
  - $(a_0 = 0) \wedge (a_1 = f(x_1, a_0))$
  - $\varphi' := (a_1 \geq x_3) \wedge (a_2 \leq x_3) \wedge (x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge (x_3 - a_1 \geq 1) \wedge$
  - $(a_0 = 0) \wedge (a_1 = f(x_1, a_0)) \wedge (a_2 = f(x_2, a_0))$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$
$\star\ x_1 = x_2$	

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$
$\star\ x_1 = x_2$	$x_1 = x_2$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ ← $a_2 = f(x_2, a_0)$ ←
$\star\ x_1 = x_2$	$x_1 = x_2$ ← $\star\ a_1 = a_2$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$
$\star\ x_1 = x_2$ $a_1 = a_2$	$x_1 = x_2$ $\star\ a_1 = a_2$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$	$a_1 = f(x_1, a_0)$
$a_2 \leq x_3$	$a_2 = f(x_2, a_0)$
$x_1 \geq x_2$	
$x_2 \geq x_1$	
$x_3 - a_1 \geq 1$	
$a_0 = 0$	
$\star\ x_1 = x_2$	$x_1 = x_2$
$a_1 = a_2$	$\star\ a_1 = a_2$
$\star\ a_1 = x_3$	

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ → $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$
⋆ $x_1 = x_2$ $a_1 = a_2$ → $a_1 = x_3$ ⋆ FALSE	$x_1 = x_2$ ⋆ $a_1 = a_2$

Application of Nelson-Oppen-for-Convex-Theories (cont'd)

F_1 (arithmetic over $\mathbb{R}$)	F_2 (EUF)
$a_1 \geq x_3$ $a_2 \leq x_3$ $x_1 \geq x_2$ $x_2 \geq x_1$ $x_3 - a_1 \geq 1$ $a_0 = 0$	$a_1 = f(x_1, a_0)$ $a_2 = f(x_2, a_0)$
$\star\ x_1 = x_2$ $a_1 = a_2$ $\star\ a_1 = x_3$ $\star$ FALSE	$x_1 = x_2$ $\star\ a_1 = a_2$

Nelson-Oppen-for-Convex-Theories on Nonconvex Theories

- Nelson-Oppen-for-Convex-Theories may fail if one of the theories is not convex
- Example: $(1 \leq x) \wedge (x \leq 2) \wedge p(x) \wedge \neg p(1) \wedge \neg p(2)$, where $x \in \mathbb{Z}$
  - Purification results in: $1 \leq x \wedge x \leq 2 \wedge p(x) \wedge \neg p(a_1) \wedge \neg p(a_2) \wedge a_1 = 1 \wedge a_2 = 2$
  - Since no equality can be derived, Nelson-Oppen-for-Convex-Theories returns "Satisfiable"
  - However, we know that the formula is unsatisfiable in the combined theory

Nelson-Oppen-for-Convex-Theories on Nonconvex Theories (cont'd)

- To remedy this problem, consider not only implied equalities but also implied **disjunctions of equalities**
- Given such a disjunction, the problem is split into as many parts as there are disjunctions, and the procedure is called recursively
- Continued after purification: F_1 $1 \leq x \wedge x \leq 2 \wedge$ $a_1 = 1 \wedge a_2 = 2$ $p(x) \wedge \neg p(a_1) \wedge \neg p(a_2) \wedge$ F_2
  - F_1 implies $x = 1 \vee x = 2$
  - Case 1 ($x = 1$): F_1 implies $x = a_1$, F_2 is unsatisfiable with $x = a_1$
  - Case 1 ($x = 2$): F_1 implies $x = a_2$, F_2 is unsatisfiable with $x = a_2$

Nelson–Oppen Algorithm

Algorithm Nelson-Oppen

Input: a formula φ that mixes theories, with Nelson-Oppen restrictions

Output: "Satisfiable" if φ is satisfiable, and "Unsatisfiable" otherwise

1. Purification: Purify φ into $F_1, \ldots, F_n$

2. Apply the decision procedure for T_i to F_i. If there exists i such that F_i is unsatisfiable in T_i, return "Unsatisfiable".

3. Equality propagation: If there exist i, j such that F_i T_i-implies an equality between variables of φ that is not T_j-implied by F_j, add this equality to F_j and go to step 2.

4. Splitting: If there exists i such that

   - $F_i \Rightarrow (x_1 = y_1 \vee \cdots x_k = y_k)$ and
   - $\forall j \in \{1,\ldots,k\} \,.\, F_i \not\Rightarrow x_j = y_j$,

   then apply Nelson-Oppen recursively to $\varphi' \wedge x_1 = y_1, \ldots, \varphi' \wedge x_k = y_k$. If any of these subproblems is satisfiable, return "Satisfiable". Otherwise, return "Unsatisfiable".

5. Return "Satisfiable".