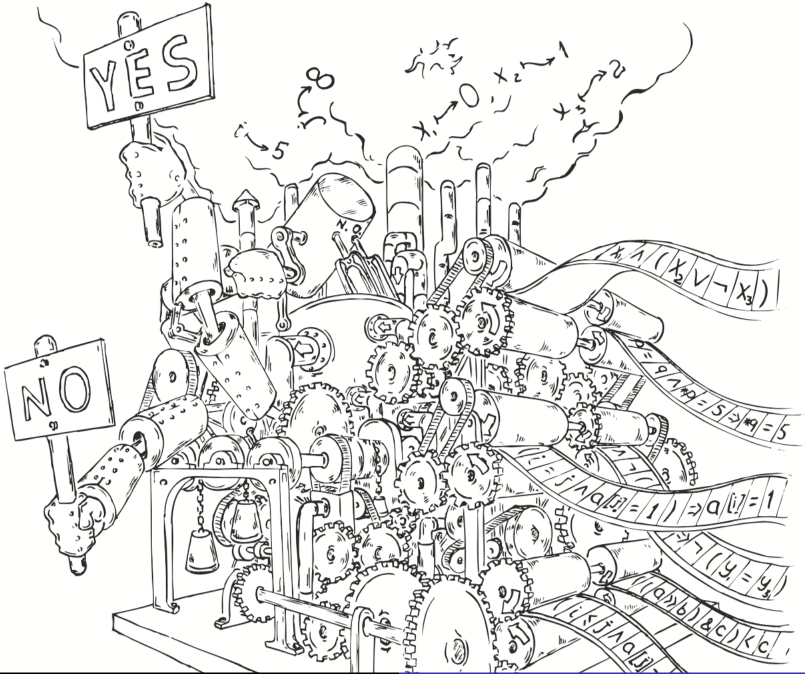

YES
NO

SAT/SMT solvers
9. Deciding a Combination of Theories

Roman Kholin

Lomonosov Moscow State University

Moscow, 2023

Why we need it

1. A combination of linear arithmetic and uninterpreted functions:
   $(x_2 \geq x_1) \wedge (x_1 - x_3 \geq x2) \wedge (x_3 \geq 0) \wedge f(f(x_1) - f(x_2)) \neq f(x_3)$
2. A combination of bit vectors and uninterpreted functions:
   $f(a[32], b[1]) = f(b[32], a[1]) \wedge a[32] = b[32]$
3. A combination of arrays and linear arithmetic:
   $x = v\{i \leftarrow e\}[j] \wedge y = v[j] \wedge x > e \wedge x > y$

Theories

1. Variables
2. Logical symbols: $\vee, \wedge, \rightarrow, \neg, \forall, \exists$
3. Nonlogical symbols, namely function and predicate symbols
4. Syntax

- It is common to consider the equality sign as a logical symbol rather than a predicate
- Signature Σ is a set of nonlogical symbols (i.e., function and predicate symbols)
- A first-order theory is defined by a set of sentences (first-order formulas in which all variables are quantified) or axioms
- 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 ($T \models \phi$) if all interpretations that satisfy T also satisfy ϕ

Theory combination

Given two theories T_1, T_2 with signatures Σ_1, Σ_2 respectively, the theory combination $T_1 \oplus T_2$ is a $(\Sigma_1 \cup \Sigma_2)$-theory defined by the axiom set $T_1 \cup T_2$

Convex theory

Σ-theory T is convex if for every conjunctive Σ-formula ϕ:
$(\phi \implies \vee_{i=1}^{n}(x_i = y_i))$ is T-valid for some finite $n > 1 \implies$
$(\phi \implies (x_i = y_i))$ is T-valid for some $i \in \{1, \ldots, n\}$

$$x \leq 3 \wedge x \geq 3 \implies x = 3$$

$$x_1 = 1 \wedge x_2 = 2 \wedge 1 \leq x_3 \wedge x_3 \leq 2 \implies (x_3 = x_1 \vee x_3 = x_2)$$

Nelson-Oppen restrictions

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
3. The signatures are disjoint
4. Theories that are interpreted over an infinite domain

Purification

Let $\phi' := \phi$

1. For each "alien"subexpression φ replace on a_φ
2. Constrain ϕ' with $a_\varphi = \varphi$

$\varphi := \ x_1 \leq f(x_1)$

After purification, we are left with a set of pure expressions $F_1, \ldots, F_n$, such that:

1. For all i, F_i belongs to theory T_i and is a conjunction of T_i-literals
2. Shared variables are allowed
3. The formula ϕ is satisfiable in the combined theory if and only if $\wedge_{i=1}^n F_i$

Nelson-Oppen for Convex Theories

Input: A convex formula φ that mixes convex theories, with restrictions as specified in Definition 10.5

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".

Example

$$
\begin{gathered}
(f(x_1,0) \geq x_3) \wedge (f(x_2,0) \leq x_3) \wedge \\
(x_1 \geq x_2) \wedge (x_2 \geq x_1) \wedge \\
(x_3 - f(x_1,0) \geq 1) ,
\end{gathered}
$$

Example

$$(x_2 \geq x_1) \wedge (x_1 - x_3 \geq x_2) \wedge (x_3 \geq 0) \wedge (f(f(x_1) - f(x_2)) \neq f(x_3))$$

Nelson-Oppen

Algorithm may fail if one of the theories is not convex:

$(1 \le x) \wedge (x \le 2) \wedge p(x) \wedge \neg p(1) \wedge \neg p(2)$

Nelson-Oppen

Input: A formula φ that mixes theories, with restrictions as specified in Definition 10.5

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

1. *Purification:* Purify φ into $\varphi' := F_1, \ldots, F_n$.
2. Apply the decision procedure for T_i to F_i. If there exists i such that F_i is unsatisfiable, 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
   - $F_i \implies (x_1 = y_1 \vee \cdots \vee x_k = y_k)$ and
   - $\forall j \in \{1, \ldots, k\}.\ F_i \not\Longrightarrow x_j = y_j$,

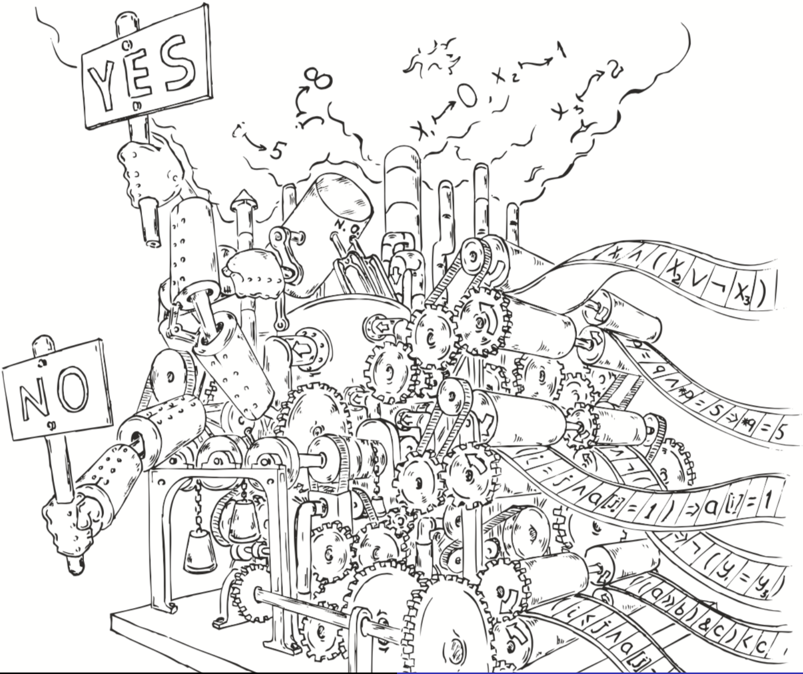
   then apply Nelson–Oppen recursively to

   $$\varphi' \wedge x_1 = y_1, \ldots, \varphi' \wedge x_k = y_k \ .$$

   If any of these subproblems is satisfiable, return "Satisfiable". Otherwise, return "Unsatisfiable".
5. Return "Satisfiable".

Example

$$(1 \leq x) \wedge (x \leq 2) \wedge p(x) \wedge \neg p(1) \wedge \neg p(2)$$


YES
NO
N.O.