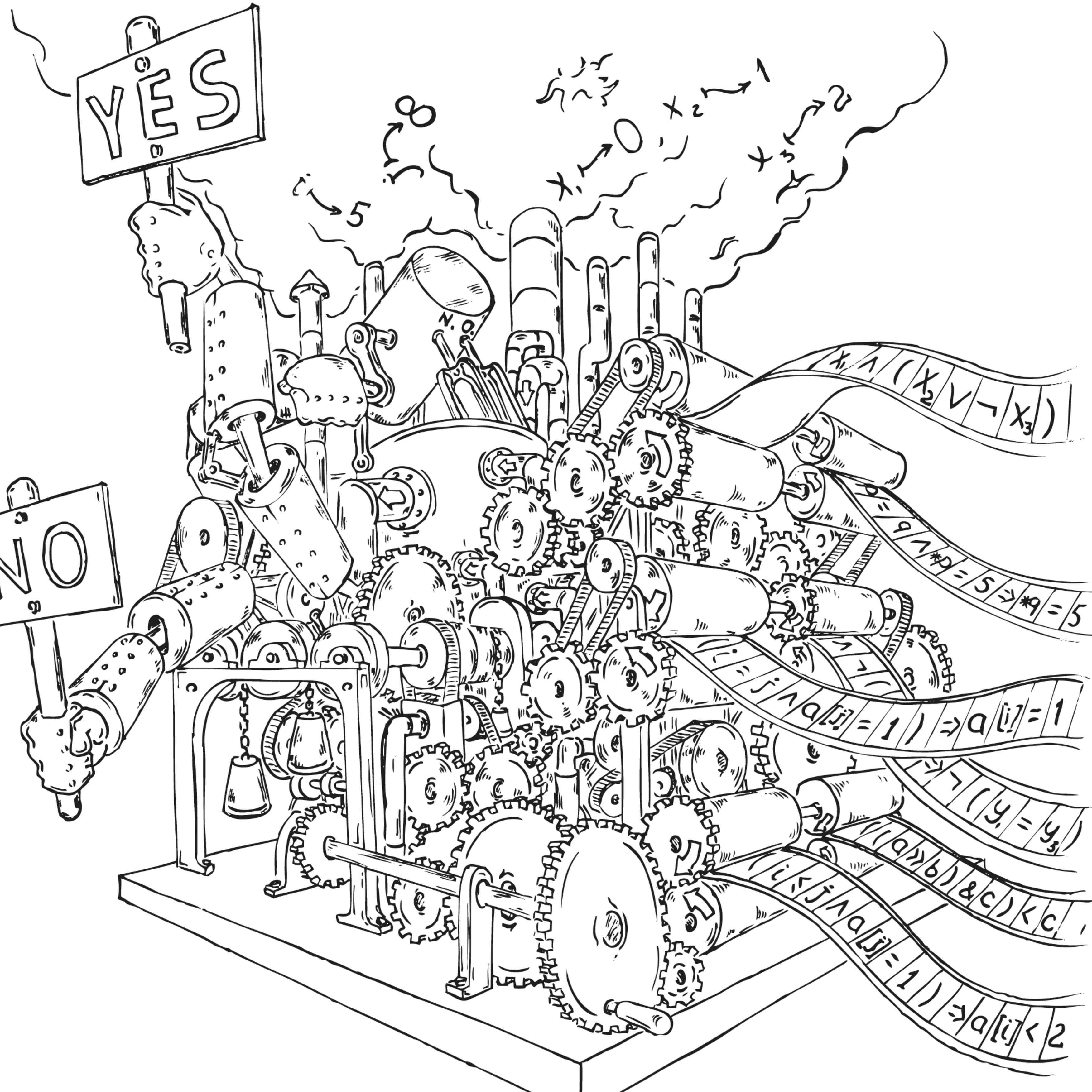
Deciding Combined Theories

Zhilin Wu (吴志林),
State Key Laboratory of Computer Science,
Institute of Software,
Chinese Academy of Sciences


YES
NO

Outline

- Equality logic with uninterpreted functions
- Combining theories
- The Nelson-Oppen method
- Z3求解器演示例子

Theories and Signatures

First-order logic (FOL)

- Signature: constants, function and relation symbols
- Syntax: Obtained from atomic formulas by applying Boolean connectives and quantifications.

Example:

FOL with signature {*R*}, where *R* represents a binary relation.

$$\exists y \,.\, R(x, y)$$

Theories and Signatures

First-order theories

$\boxed{\text{First-order logic with axioms characterizing the theory}}$

Theory of preorders: The axioms are

$$\forall x \,.\, R(x, x)$$

$$\forall x \forall y \forall z \,.\, (R(x, y) \wedge R(y, z)) \rightarrow R(x, z)$$

Theories and Signatures

First-order theories

First-order logic with axioms characterizing the theory

Theory of preorders: The axioms are

$$\forall x \,.\, R(x, x)$$

$$\forall x \forall y \forall z \,.\, (R(x, y) \wedge R(y, z)) \rightarrow R(x, z)$$

First-order theories with equality: equality is part of the signature.

Theories of partial orders (with signature $\{R, =\}$)

$$\forall x \forall y \,.\, (R(x, y) \wedge R(y, x)) \rightarrow x = y$$

Theories and Signatures

First-order theories

First-order logic with axioms characterizing the theory

Theory of preorders: The axioms are

$$\forall x \,.\, R(x, x)$$

$$\forall x \forall y \forall z \,.\, (R(x, y) \wedge R(y, z)) \rightarrow R(x, z)$$

First-order theories with equality: equality is part of the signature.

Theories of partial orders (with signature $\{R, =\}$)

$$\forall x \forall y \,.\, (R(x, y) \wedge R(y, x)) \rightarrow x = y$$

Conjunctive fragments: conjunctions of equalities and inequalities

Equality Logic with Uninterpreted Functions (EUF)

Signature: Set of function symbols $\{F_1, F_2, \ldots\}$.

$$
\begin{array}{lcl}
\mathit{formula} & : & \mathit{formula} \lor \mathit{formula} \\
& | & \neg \mathit{formula} \\
& | & \mathit{atom} \\
\\
\mathit{atom} & : & \mathit{term} = \mathit{term} \\
& | & \mathit{Boolean\text{-}variable} \\
\\
\mathit{term} & : & \mathit{term\text{-}variable} \\
& | & \mathit{function}\,(\,\text{list of } \mathit{terms}\,)
\end{array}
$$

$$x_1 = x_2 \land x_2 = x_3 \land x_4 = x_5 \land x_5 \neq x_1 \land F(x_1) \neq F(x_3)$$

Axioms: For each function symbol *F*, $\forall x_1, x_2 \,.\, x_1 = x_2 \rightarrow F(x_1) = F(x_2)$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$x_1 = x_3 \Rightarrow F(x_1) = F(x_3)$$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$x_1 = x_3 \Rightarrow F(x_1) = F(x_3)$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1), F(x_3)\}$$

Deciding EUF by Congruence Closure

$$x_1 = x_2 \wedge x_2 = x_3 \wedge x_4 = x_5 \wedge x_5 \neq x_1 \wedge F(x_1) \neq F(x_3)$$

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1)\}, \{F(x_3)\}$$

contradiction

$$x_1 = x_3 \Rightarrow F(x_1) = F(x_3)$$

$$\{x_1, x_2, x_3\}, \{x_4, x_5\}, \{F(x_1), F(x_3)\}$$

UNSAT

Deciding EUF by Congruence Closure

First consider a conjunction of equalities/inequalities

1. Initially, define an equivalence class $\{t\}$ for each term t.
2. For each equality $t_1 = t_2$, merge the equivalence classes of t_1 and t_2. Repeat until convergence.
3. For each pair of terms $F(t_1)$ and $F(t_2)$, if t_1 and t_2 are in the same equivalence class, then merge the equivalence classes of $F(t_1)$ and $F(t_2)$. Repeat until convergence.
4. For each inequality $t_1 \neq t_2$, if t_1 is in the same equivalence class as t_2, then return 'UNSAT'.
5. Return 'SAT'.

Deciding EUF by Congruence Closure

Then consider arbitrary boolean combinations of equalities.

Can be obtained by applying De Morgan's law e.g. $\neg(\phi_1 \vee \phi_2) = \neg\phi_1 \wedge \neg\phi_2$

Assume the formulas are in NNF (Negation Normal Form).

Apply the DPLL(T) framework:

1. For each subset of the equalities and inequalities that can make the formula "TRUE" (provided that they are assigned "TRUE"), if the conjunction of the equalities and inequalities in this subset is satisfiable, then return "SAT".

   (DPLL is a strategy to avoid naive enumeration of subsets.)
2. Return "UNSAT".

Outline

- Equality logic with uninterpreted functions
- **Combining theories**
- The Nelson-Oppen method
- Z3求解器演示例子

Combining Theories

We know how to decide LIA and EUF

LIA: $x_1 = x_2 + 1 \wedge x_3 = x_2 + 1$

EUF: $F(x_1) \neq F(x_3)$

Combining Theories

We know how to decide LIA and EUF

LIA: $x_1 = x_2 + 1 \wedge x_3 = x_2 + 1$

EUF: $F(x_1) \neq F(x_3)$

How about the following formula ?

$$x_1 = x_2 + 1 \wedge x_3 = x_2 + 1 \wedge F(x_1) \neq F(x_3)$$

Combining Theories

We know how to decide LIA and EUF

LIA: $x_1 = x_2 + 1 \wedge x_3 = x_2 + 1$

EUF: $F(x_1) \neq F(x_3)$

How about the following formula ?

$$x_1 = x_2 + 1 \wedge x_3 = x_2 + 1 \wedge F(x_1) \neq F(x_3)$$

or even

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge F(F(x_1) - F(x_2)) \neq F(x_3) \text{ ?}$$

Combining Theories

We know how to decide LIA and EUF

LIA: $x_1 = x_2 + 1 \wedge x_3 = x_2 + 1$

EUF: $F(x_1) \neq F(x_3)$

How about the following formula ?

$$x_1 = x_2 + 1 \wedge x_3 = x_2 + 1 \wedge F(x_1) \neq F(x_3)$$

or even

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge F(F(x_1) - F(x_2)) \neq F(x_3) \text{ ?}$$

The combination of LIA and EUF

Combining Theories

We know how to decide BV and EUF

BV: a[31] = b[31]

EUF: $F(x_1, x_2) = F(x_3, x_4)$

How about the following formula ?

a[31] = b[31] ∧ *F*(a[31], b[0]) = *F*(b[31], a[0])

The combination of BV and EUF

Theory-Combination Problem

Theory combination

Given two theories $\mathcal{T}_1$ and $\mathcal{T}_2$
with signatures Σ_1 and Σ_2 and axiom sets A_1 and A_2,
the combination of $\mathcal{T}_1$ and $\mathcal{T}_2$, denoted by $\mathcal{T}_1 \oplus \mathcal{T}_2$,
is a $(\Sigma_1 \cup \Sigma_2)$-theory defined by the axiom set $A_1 \cup A_2$.

Theory combination problem

Let φ be a $\Sigma_1 \cup \Sigma_2$ formula.
Then the theory combination problem is to decide whether
φ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ valid. Equivalently,
the problem is to decide whether the following holds: $A_1 \cup A_2 \models \varphi$.

Theory-Combination Problem

Theory-combination problem is undecidable,
even when the individual theories are decidable.

Under certain restrictions, it becomes decidable.

We will assume the following restrictions:

- $\mathcal{T}_1$ and $\mathcal{T}_2$ are decidable, quantifier-free first-order theories with equality,
- disjoint signatures (except =): $\Sigma_1 \cap \Sigma_2 = \{ = \}$,
- $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably infinite (to be defined).

Outline

- Equality logic with uninterpreted functions
- Combining theories
- **The Nelson-Oppen method**
- Z3求解器演示例子

Stably Infinite Theories

A Σ-theory $\mathcal{T}$ is stably infinite if
every satisfiable Σ-formula has a model with an infinite domain.

Examples of Stably infinite theories

LIA and LRA: Linear integer resp. real arithmetic

EUF: Equality logic with uninterpreted functions

Examples of non-stably infinite theories

Theory of fixed width bit vectors: BV

$\Sigma = \{a, b, =\}$, axiom: $\forall x \,.\, x = a \vee x = b$

The Nelson-Oppen Method

By utilizing DPLL(T),
when deciding combined theories,
we can focus on
conjunctive fragments !

The Nelson-Oppen Method

The 1st Step: Purification

validity-preserving transformation of the formula ϕ after which functions and relations from different theories are not mixed

Continue replacing a minimal “alien” expression *e* by a fresh variable *a* and add *a* = *e* until no more “alien” expressions.

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

The Nelson-Oppen Method

The 1st Step: Purification

validity-preserving transformation of the formula ϕ after which functions and relations from different theories are not mixed

Continue replacing a minimal “alien” expression *e* by a fresh variable *a* and add *a* = *e* until no more “alien” expressions.

$$x_2 \geq x_1 \land x_1 - x_3 \geq x_2 \land x_3 \geq 0 \land F(F(x_1) - F(x_2)) \neq F(x_3)$$

$$\Downarrow$$

$$x_2 \geq x_1 \land x_1 - x_3 \geq x_2 \land x_3 \geq 0 \land F(a) \neq F(x_3) \land a = F(x_1) - F(x_2)$$

The Nelson-Oppen Method

The 1st Step: Purification

validity-preserving transformation of the formula ϕ after which functions and relations from different theories are not mixed

Continue replacing a minimal "alien" expression *e* by a fresh variable *a* and add *a* = *e* until no more "alien" expressions.

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

$$\Downarrow$$

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge F(a) \neq F(x_3) \wedge a = F(x_1) - F(x_2)$$

$$\Downarrow$$

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge F(a) \neq F(x_3) \wedge$$
$$a = a_1 - a_2 \wedge a_1 = F(x_1) \wedge a_2 = F(x_2)$$

The Nelson-Oppen Method

The 1st Step: Purification

validity-preserving transformation of the formula ϕ after which functions and relations from different theories are not mixed

Continue replacing a minimal “alien” expression *e* by a fresh variable *a* and add *a* = *e* until no more “alien” expressions.

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

Note: Purification preserves satisfiability !

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

$$a = a_1 - a_2 \wedge a_1 = F(x_1) \wedge a_2 = F(x_2)$$

The Nelson-Oppen Method

The 1st Step: Purification

The purification of ϕ produces an equisatisfiable formula

$\phi_1 \wedge \phi_2$ such that

ϕ_1 belongs to the theory $\mathcal{T}_1$ and ϕ_2 belongs to the theory $\mathcal{T}_2$

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

$$\Downarrow$$

$$x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge F(a) \neq F(x_3) \wedge$$
$$a = a_1 - a_2 \wedge a_1 = F(x_1) \wedge a_2 = F(x_2)$$

$$\Downarrow$$

ϕ_1 $\quad x_2 \geq x_1 \wedge x_1 - x_3 \geq x_2 \wedge x_3 \geq 0 \wedge a = a_1 - a_2 \wedge$

ϕ_2 $\quad F(a) \neq F(x_3) \wedge a_1 = F(x_1) \wedge a_2 = F(x_2)$

The Nelson-Oppen Method

1. Purify ϕ into $\phi_1 \wedge \phi_2$.
2. If ϕ_1 or ϕ_2 is unsatisfiable, then return "UNSAT".
3. If ϕ_i implies an equality between variables not implied by ϕ_{3-i} for some $i \in \{1,2\}$, then add it to ϕ_{3-i}. Go to step 2.
4. Return "SAT".

The Nelson-Oppen Method

1. Purify ϕ into $\phi_1 \wedge \phi_2$.
2. If ϕ_1 or ϕ_2 is unsatisfiable, then return "UNSAT".
3. If ϕ_i implies an equality between variables not implied by ϕ_{3-i} for some $i \in \{1,2\}$, then add it to ϕ_{3-i}. Go to step 2.
4. Return "SAT".

The algorithm runs in polynomial time,
if the conjunctive fragments of $\mathscr{T}_1$ and $\mathscr{T}_2$
can be decided in polynomial time.

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	
$\boxed{x_1 = x_2}$	
$\boxed{x_3 = 0}$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	$x_1 = x_2$
$\boxed{x_1 = x_2}$	
$\boxed{x_3 = 0}$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	$x_1 = x_2$
$\boxed{x_1 = x_2}$	$\boxed{a_1 = a_2}$
$\boxed{x_3 = 0}$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	$x_1 = x_2$
$\boxed{x_1 = x_2}$	$\boxed{a_1 = a_2}$
$\boxed{x_3 = 0}$	
$a_1 = a_2$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$ $x_1 - x_3 \geq x_2$ $x_3 \geq 0$ $a = a_1 - a_2$ $\boxed{x_1 = x_2}$ $\boxed{x_3 = 0}$ $a_1 = a_2$ $\boxed{a = 0}$ $\boxed{x_3 = a}$	$F(a) \neq F(x_3)$ $a_1 = F(x_1)$ $a_2 = F(x_2)$ $x_1 = x_2$ $\boxed{a_1 = a_2}$

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	$x_1 = x_2$
$\boxed{x_1 = x_2}$	$\boxed{a_1 = a_2}$
$\boxed{x_3 = 0}$	$x_3 = a$
$a_1 = a_2$	
$\boxed{a = 0}$	
$\boxed{x_3 = a}$	

The Nelson-Oppen Method

LIA	EUF
$x_2 \geq x_1$	$F(a) \neq F(x_3)$
$x_1 - x_3 \geq x_2$	$a_1 = F(x_1)$
$x_3 \geq 0$	$a_2 = F(x_2)$
$a = a_1 - a_2$	$x_1 = x_2$
$\boxed{x_1 = x_2}$	$\boxed{a_1 = a_2}$
$\boxed{x_3 = 0}$	$x_3 = a$
$a_1 = a_2$	UNSAT
$\boxed{a = 0}$	
$\boxed{x_3 = a}$	

Life Is Not So Easy :(

Consider

$$\phi \equiv 1 \leq x_1 \wedge x_1 \leq 2 \wedge F(x_1) \neq F(1) \wedge F(x_1) \neq F(2)$$

LIA ϕ_1	EUF ϕ_2
$1 \leq x_1$ $x_1 \leq 2$ $y_1 = 1$ $y_2 = 2$	$F(x_1) \neq F(y_1)$ $F(x_1) \neq F(y_2)$

Life Is Not So Easy :(

Consider

$$\phi \equiv 1 \leq x_1 \wedge x_1 \leq 2 \wedge F(x_1) \neq F(1) \wedge F(x_1) \neq F(2)$$

LIA ϕ_1	EUF ϕ_2
$1 \leq x_1$ $x_1 \leq 2$ $y_1 = 1$ $y_2 = 2$	$F(x_1) \neq F(y_1)$ $F(x_1) \neq F(y_2)$

No equalities between variables are implied by ϕ_1 resp. ϕ_2 and both ϕ_1 and ϕ_2 are satisfiable.

But ϕ is unsatisfiable.

Convex Theories

A theory $\mathcal{T}$ is convex if

for all ϕ in the conjunctive fragment, it holds that

$$\phi \models \bigvee_{i=1}^{n} x_i = y_i \text{ for some } n > 1 \text{ iff}$$

$$\phi \models x_i = y_i \text{ for some } i : 1 \leq i \leq n,$$

where x_1, y_i are variables.

Convex: LRA, EUF

Non-convex: Almost anything else, e.g. LIA

Convex Theories

Examples

LRA is convex.

For contradiction, suppose $\phi \vDash x_1 = y_1 \vee x_2 = y_2$ but $\phi \nvDash x_i = y_i$ for every $i = 1{,}2$.

Then there are $\overrightarrow{u}$ and $\overrightarrow{v}$ in $[\![\phi]\!]$ such that $\overrightarrow{u} \vDash x_1 = y_1$ and $\overrightarrow{v} \vDash x_2 = y_2$, but $\overrightarrow{u} \nvDash x_2 = y_2$, and $\overrightarrow{v} \nvDash x_1 = y_1$.

Since ϕ is in the conjunctive fragment, $[\![\phi]\!]$ is convex.

Therefore, $(\overrightarrow{u} + \overrightarrow{v})/2$ is in $[\![\phi]\!]$. But $(\overrightarrow{u} + \overrightarrow{v})/2 \nvDash x_i = y_i$ for every $i = 1{,}2$.

LIA is non-convex.

$$\phi \equiv y \leq 1 \wedge y \geq 0 \wedge x_1 = 1 \wedge x_0 = 0 \vDash y = x_1 \vee y = x_0$$

but neither $\phi \vDash y = x_1$ nor $\phi \vDash y = x_0$

Propagate Disjunctions For Non-convex Theories

Consider $\phi \equiv 1 \leq x_1 \wedge x_1 \leq 2 \wedge F(x_1) \neq F(1) \wedge F(x_1) \neq F(2)$

LIA	EUF
$1 \leq x_1$ $x_1 \leq 2$ $y_1 = 1$ $y_2 = 2$ $\boxed{x_1 = y_1 \vee x_1 = y_2}$	$F(x_1) \neq F(y_1)$ $F(x_1) \neq F(y_2)$

Propagate Disjunctions For Non-convex Theories

Consider $\phi \equiv 1 \leq x_1 \wedge x_1 \leq 2 \wedge F(x_1) \neq F(1) \wedge F(x_1) \neq F(2)$

LIA	EUF
$1 \leq x_1$ $x_1 \leq 2$ $y_1 = 1$ $y_2 = 2$ $\boxed{x_1 = y_1 \vee x_1 = y_2}$	$F(x_1) \neq F(y_1)$ $F(x_1) \neq F(y_2)$ $x_1 = y_1 \vee x_1 = y_2$

Propagate Disjunctions For Non-convex Theories

Consider $\phi \equiv 1 \leq x_1 \land x_1 \leq 2 \land F(x_1) \neq F(1) \land F(x_1) \neq F(2)$

<table>
<tr><th>LIA</th><th colspan="2">EUF</th></tr>
<tr><td>$1 \leq x_1$</td><td colspan="2">$F(x_1) \neq F(y_1)$</td></tr>
<tr><td>$x_1 \leq 2$</td><td colspan="2">$F(x_1) \neq F(y_2)$</td></tr>
<tr><td>$y_1 = 1$</td><td colspan="2">$x_1 = y_1 \lor x_1 = y_2$</td></tr>
<tr><td>$y_2 = 2$</td><td colspan="2">case split</td></tr>
<tr><td>$\boxed{x_1 = y_1 \lor x_1 = y_2}$</td><td>$x_1 = y_1$
$F(x_1) \neq F(y_1)$
$F(x_1) \neq F(y_2)$</td><td>$x_1 = y_2$
$F(x_1) \neq F(y_1)$
$F(x_1) \neq F(y_2)$</td></tr>
</table>

Propagate Disjunctions For Non-convex Theories

Consider $\phi \equiv 1 \leq x_1 \wedge x_1 \leq 2 \wedge F(x_1) \neq F(1) \wedge F(x_1) \neq F(2)$

<table>
<tr><th>LIA</th><th colspan="2">EUF</th></tr>
<tr><td rowspan="2">$1 \leq x_1$
$x_1 \leq 2$
$y_1 = 1$
$y_2 = 2$
$\boxed{x_1 = y_1 \vee x_1 = y_2}$</td><td colspan="2">$F(x_1) \neq F(y_1)$
$F(x_1) \neq F(y_2)$
$x_1 = y_1 \vee x_1 = y_2$
case split</td></tr>
<tr><td>$x_1 = y_1$
$F(x_1) \neq F(y_1)$
$F(x_1) \neq F(y_2)$
UNSAT</td><td>$x_1 = y_2$
$F(x_1) \neq F(y_1)$
$F(x_1) \neq F(y_2)$
UNSAT</td></tr>
</table>

The Full Nelson-Oppen Method

1. Purify ϕ into $\phi_1 \wedge \phi_2$.
2. If ϕ_1 or ϕ_2 is unsatisfiable, then return "UNSAT".
3. If ϕ_i implies an equality between variables not implied by ϕ_{3-i} for some $i \in \{1,2\}$, then add it to ϕ_{3-i}. Go to step 2.
4. If ϕ_i implies $\bigvee_{j=1}^{n} x_j = y_j$ for some $i \in \{1,2\}$ and $n > 1$, but ϕ_i does not imply $x_j = y_j$ for every j,, then apply the Nelson-Oppen method recursively to $\phi_1 \wedge \phi_2 \wedge x_1 = y_1$, …, $\phi_1 \wedge \phi_2 \wedge x_n = y_n$. If any of them returns "SAT", then return "SAT". Otherwise, return "UNSAT".
5. Return "SAT".

The Full Nelson-Oppen Method

1. Purify ϕ into $\phi_1 \wedge \phi_2$.
2. If ϕ_1 or ϕ_2 is unsatisfiable, then return "UNSAT".
3. If ϕ_i implies an equality between variables not implied by ϕ_{3-i} for some $i \in \{1,2\}$, then add it to ϕ_{3-i}. Go to step 2.

The algorithm is exponential time in the worst case, even if the conjunctive fragments of $\mathscr{T}_1$ and $\mathscr{T}_2$ can be decided in polynomial time.

Oppen method recursively to $\phi_1 \wedge \phi_2 \wedge x_1 = y_1, \ldots,$ $\phi_1 \wedge \phi_2 \wedge x_n = y_n$. If any of them returns "SAT", then return "SAT". Otherwise, return "UNSAT".

5. Return "SAT".

Outline

- Equality logic with uninterpreted functions
- Combining theories
- The Nelson-Oppen method
- **Z3求解器演示例子**

Z3求解器演示例子

把下面两段程序P1和P2的等价性问题编码为
LIA ⊕ EUF公式并调用Z3求解器进行求解

P1

```
int gcd1(int a, int b)
{
  int g;
  if (b == 0) g = a;
  else {
    a = a%b;
    g = gcd1(b, a);}
  return g;
}
```

P2

```
int gcd2(int x, int y)
{
  int z;
  z = x;
  if (y > 0)
    z = gcd2(y, z%y);
  return z;
}
```

Z3求解器演示例子

把P1和P2改写为SSA形式

P1

```
int gcd1(int a, int b)
{
  int g, g1, a1;
  if (b == 0) g1 = a;
  else {
    a1 = a%b;
    g1 = gcd1(b, a1);}
  return g1;
}
```

P2

```
int gcd2(int x, int y)
{
  int z, z1;
  z = x;
  if (y > 0) {
    z1 = gcd2(y, z%y);
   return z1;}
  return z;
}
```

Z3求解器演示例子

```
int gcd1(int a, int b)
{
  int g, g1, a1;
  if (b == 0) g1 = a;
  else {
    a1 = a%b;
    g1 = gcd1(b, a1);}
  return g1;
}
```

ϕ_{P1}:

$$\left(\begin{array}{l} (b = 0 \wedge g1 = a) \vee \\ \left(\begin{array}{l} b > 0 \wedge a1 = mod(a, b) \wedge \\ g1 = gcd1(b, a1) \end{array} \right) \end{array} \right) \wedge gcd1(a, b) = g1$$

Z3求解器演示例子

```
int gcd1(int a, int b)
{
   int g, g1, a1;
   if (b == 0) g1 = a;
   else {
    a1 = a%b;
    g1 = gcd1(b, a1);}
   return g1;
}
```

ϕ_{P1}:

$$\left(\begin{array}{l} (b = 0 \wedge g1 = a) \vee \\ \left(\begin{array}{l} b > 0 \wedge a1 = mod(a,b) \wedge \\ g1 = gcd1(b, a1) \end{array} \right) \end{array} \right) \wedge gcd1(a,b) = g1$$

```
int gcd2(int x, int y)
{
  int z, z1;
  z = x;
  if (y > 0) {
    z1 = gcd2(y, z%y);
    return z1;}
  return z;
}
```

ϕ_{P2}:

$$z = x \wedge (y > 0 \rightarrow (z1 = gcd2(y, mod(z,y)) \wedge gcd2(x,y) = z1)) \wedge$$
$$(y = 0 \rightarrow gcd2(x,y) = z)$$

Z3求解器演示例子

```
int gcd1(int a, int b)
{
  int g, g1, a1;
  if (b == 0) g1 = a;
  else {
   a1 = a%b;
   g1 = gcd1(b, a1);}
  return g1;
}
```

ϕ_{P1}:

$$\left(\begin{array}{l} (b = 0 \wedge g1 = a) \vee \\ \left(\begin{array}{l} b > 0 \wedge a1 = mod(a, b) \wedge \\ g1 = gcd1(b, a1) \end{array} \right) \end{array} \right) \wedge gcd1(a, b) = g1$$

```
int gcd2(int x, int y)
{
  int z, z1;
  z = x;
  if (y > 0) {
    z1 = gcd2(y, z%y);
    return z1;}
  return z;
}
```

ϕ_{P2}:

$$z = x \wedge (y > 0 \rightarrow (z1 = gcd2(y, mod(z, y)) \wedge gcd2(x, y) = z1)) \wedge$$
$$(y = 0 \rightarrow gcd2(x, y) = z)$$

Observing that a1 < b and z%y < y, by the induction principle, the equivalence of P1 and P2 is reduced to checking the validity of

$$(\phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b = 0) \rightarrow gcd1(a, b) = gcd2(x, y)$$

$$\left(\begin{array}{l} \phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b > 0 \wedge \\ gcd1(b, mod(a, b)) = gcd2(x, mod(x, y)) \end{array} \right) \rightarrow gcd1(a, b) = gcd2(x, y)$$

Z3求解器演示例子

the validity of

$$(\phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b = 0) \rightarrow gcd1(a,b) = gcd2(x,y)$$

$$\Downarrow$$

the satisfiability of

$$(\phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b = 0) \wedge \neg gcd1(a,b) = gcd2(x,y)$$

the validity of

$$\begin{pmatrix} \phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b > 0 \wedge \\ gcd1(b, mod(a,b)) = gcd2(x, mod(x,y)) \end{pmatrix} \rightarrow gcd1(a,b) = gcd2(x,y)$$

$$\Downarrow$$

the satisfiability of

$$\begin{pmatrix} \phi_{P_1} \wedge \phi_{P_2} \wedge a = x \wedge b = y \wedge b > 0 \wedge \\ gcd1(b, mod(a,b)) = gcd2(x, mod(x,y)) \end{pmatrix} \wedge \neg gcd1(a,b) = gcd2(x,y)$$

Solve them by Z3: A Demo

References

- Daniel Kroening, Ofer Strichman. Decision procedures: An Algorithmic Point of View, Springer, 2008.
- Aaron R. Bradley, Zohar Manna, The Calculus of Computation: Decision Procedures with Applications to Verification, Springer, 2007.

作业1（必做题）

请写出Nelson-Oppen method

在下面的 LIA $\oplus$ EUF 公式ϕ的详细运行过程

$$\phi \equiv 1 \leq x_1 \wedge x_1 \leq x_2 \wedge x_2 \leq 3 \wedge f(x_1) \neq f(x_2) \wedge f(x_1) \neq f(1) \wedge f(x_2) \neq f(3)$$

作业2 (选做题)

把下面两段程序P1和P2的等价性问题编码为

LIA $\oplus$ EUF公式并调用Z3求解器进行求解

P1

i := 0
while $i < N$ **do**
  k := $f(k, i)$
  i := $i + 1$

P2

i := N
while $i \geq 1$ **do**
  k := $f(k, N - i)$
  i := $i - 1$
if $N \leq 0$ **then**
  i := 0
else
  i := N

作业2 (选做题)

解题思路提示:

1. 将P1和P2合并得到P3(P3只含有一个while 循环),
2. 把P1和P2的等价性问题转换为验证P3的某个assertion是否成立,
3. 然后寻找P3中while循环的合适的loop invariant,
4. 生成验证条件（LIA $\oplus$ EUF公式）,
5. 调用Z3求解器进行求解.

Thanks!