Combining Decision Procedures: The Nelson-Oppen approach

Albert Oliveras and Enric Rodríguez-Carbonell

Deduction and Verification Techniques
Session 4
Fall 2009, Barcelona

Departament de Llenguatges i Sistemes Informatics
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Need for combination

- In software verification, formulas like the following one arise:

$$a{=}b+2 \wedge A{=}write(B, a+1, 4) \wedge (read(A, b+3){=}2 \vee f(a-1) \neq f(b+1))$$

- Here reasoning is needed over
  - The theory of linear arithmetic ($\mathbb{T}_{LA}$)
  - The theory of arrays ($\mathbb{T}_{A}$)
  - The theory of uninterpreted functions ($\mathbb{T}_{UF}$)
- Remember that T-solvers only deal with conjunctions of lits.
- Given T-solvers for the three individual theories, can we combine them to obtain one for ($\mathbb{T}_{LA} \cup \mathbb{T}_{A} \cup \mathbb{T}_{UF}$)?
- Under certain conditions the Nelson-Oppen combination method gives a positive answer

Motivating example - Convex case

Consider the following set of literals:

$$\begin{aligned} f(f(x) - f(y)) &= a \\ f(0) &= a + 2 \\ x &= y \end{aligned}$$

There are two theories involved: $\mathbb{T}_{LA(\mathbb{R})}$ and $\mathbb{T}_{UF}$

FIRST STEP: purify each literal so that it belongs to a single theory

$$f(f(x) - f(y)) = a \implies \begin{aligned} f(e_1) &= a \\ e_1 &= f(x) - f(y) \end{aligned} \implies \begin{aligned} f(e_1) &= a \\ e_1 &= e_2 - e_3 \\ e_2 &= f(x) \\ e_3 &= f(y) \end{aligned}$$

Motivating example - Convex case

Consider the following set of literals:

$$\begin{aligned} f(f(x) - f(y)) &= a \\ f(0) &= a + 2 \\ x &= y \end{aligned}$$

There are two theories involved: $\mathbb{T}_{LA(\mathbb{R})}$ and $\mathbb{T}_{UF}$

FIRST STEP: purify each literal so that it belongs to a single theory

$$f(0) = a + 2 \implies \begin{aligned} f(e_4) &= a + 2 \\ e_4 &= 0 \end{aligned} \implies \begin{aligned} f(e_4) &= e_5 \\ e_4 &= 0 \\ e_5 &= a + 2 \end{aligned}$$

Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

EUF			*Arithmetic*		
$f(e_1)$	$=$	a	$e_2 - e_3$	$=$	e_1
$f(x)$	$=$	e_2	e_4	$=$	0
$f(y)$	$=$	e_3	e_5	$=$	$a+2$
$f(e_4)$	$=$	e_5			
x	$=$	y			

The two solvers only share constants: $e_1, e_2, e_3, e_4, e_5, a$

To merge the two models into a single one, the solvers have to agree on equalities between shared constants (interface equalities)

This can be done by exchanging entailed interface equalities

Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

EUF			*Arithmetic*		
$f(e_1)$	$=$	a	$e_2 - e_3$	$=$	e_1
$f(x)$	$=$	e_2	e_4	$=$	0
$f(y)$	$=$	e_3	e_5	$=$	$a+2$
$f(e_4)$	$=$	e_5	e_2	$=$	e_3
x	$=$	y			

The two solvers only share constants: $e_1, e_2, e_3, e_4, e_5, a$

- *EUF*-Solver says SAT
- *Ari*-Solver says SAT
- $EUF \models e_2{=}e_3$

Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

EUF			*Arithmetic*		
$f(e_1)$	$=$	a	$e_2 - e_3$	$=$	e_1
$f(x)$	$=$	e_2	e_4	$=$	0
$f(y)$	$=$	e_3	e_5	$=$	$a+2$
$f(e_4)$	$=$	e_5	e_2	$=$	e_3
x	$=$	y			
e_1	$=$	e_4			

The two solvers only share constants: $e_1, e_2, e_3, e_4, e_5, a$

- *EUF*-Solver says SAT
- *Ari*-Solver says SAT
- $Ari \models e_1 = e_4$

Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

EUF			*Arithmetic*		
$f(e_1)$	$=$	a	$e_2 - e_3$	$=$	e_1
$f(x)$	$=$	e_2	e_4	$=$	0
$f(y)$	$=$	e_3	e_5	$=$	$a+2$
$f(e_4)$	$=$	e_5	e_2	$=$	e_3
x	$=$	y	a	$=$	e_5
e_1	$=$	e_4			

The two solvers only share constants: $e_1, e_2, e_3, e_4, e_5, a$

- *EUF*-Solver says SAT
- *Ari*-Solver says SAT
- $EUF \models a{=}e_5$

Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

EUF			*Arithmetic*		
$f(e_1)$	$=$	a	$e_2 - e_3$	$=$	e_1
$f(x)$	$=$	e_2	e_4	$=$	0
$f(y)$	$=$	e_3	e_5	$=$	$a+2$
$f(e_4)$	$=$	e_5	e_2	$=$	e_3
x	$=$	y	a	$=$	e_5
e_1	$=$	e_4			

The two solvers only share constants: $e_1, e_2, e_3, e_4, e_5, a$

- *EUF*-Solver says SAT
- *Ari*-Solver says **UNSAT**
- Hence the original set of lits was **UNSAT**

Nelson-Oppen – The convex case

- A theory T is stably-infinite iff every T-satisfiable quantifier-free formula has an infinite model
- A theory T is convex iff
  $S \models_T a_1{=}b_1 \vee \ldots \vee a_n{=}b_n \implies S \models a_i{=}b_i$ for some i

Deterministic Nelson-Oppen:

- Given two stably-infinite and convex theories T_1 and T_2
- Given a set of literals S over the signature of $T_1 \cup T_2$
- The $(T_1 \cup T_2)$-satisfiability of S can be checked with the algorithm

Nelson-Oppen – The convex case (2)

Deterministic Nelson-Oppen

1. Purify S and split it into $S_1 \cup S_2$.
   Let $\mathcal{E}$ the set of interface equalities between S_1 and S_2
2. If S_1 is T_1-unsatisfiable then **UNSAT**
3. If S_2 is T_2-unsatisfiable then **UNSAT**
4. If $S_1 \models_{T_1} x{=}y$ with $x{=}y \in \mathcal{E} \setminus S_2$ then
   $S_2 := S_2 \cup \{x{=}y\}$ and goto 3
5. If $S_2 \models_{T_2} x{=}y$ with $x{=}y \in \mathcal{E} \setminus S_1$ then
   $S_1 := S_1 \cup \{x{=}y\}$ and goto 2
6. Report **SAT**

Motivating example – Non-convex case

Consider the following **UNSATISFIABLE** set of literals:

$$\begin{array}{rcl} 1 \leq & x & \leq 2 \\ f(1) & = & a \\ f(x) & = & b \\ a & = & b+2 \\ f(2) & = & f(1)+3 \end{array}$$

There are two theories involved: $\mathbb{T}_{LA(\mathbb{Z})}$ and $\mathbb{T}_{UF}$

FIRST STEP: purify each literal so that it belongs to a single theory

$$\begin{array}{rcl} f(1) = a & \Longrightarrow & f(e_1) = a \\ & & e_1 = 1 \end{array}$$

Motivating example – Non-convex case

Consider the following **UNSATISFIABLE** set of literals:

$$\begin{array}{rcl} 1 \leq & x & \leq 2 \\ f(1) & = & a \\ f(x) & = & b \\ a & = & b+2 \\ f(2) & = & f(1)+3 \end{array}$$

There are two theories involved: $\mathbb{T}_{LA(\mathbb{Z})}$ and $\mathbb{T}_{UF}$

FIRST STEP: purify each literal so that it belongs to a single theory

$$f(2) = f(1)+3 \implies \begin{array}{rcl} e_2 & = & 2 \\ f(e_2) & = & e_3 \\ f(e_1) & = & e_4 \\ e_3 & = & e_4+3 \end{array}$$

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2			
e_3	$=$	e_4+3			
a	$=$	e_4			

The two solvers only share constants: $x, e_1, a, b, e_2, e_3, e_4$

- *Ari*-Solver says SAT
- *EUF*-Solver says SAT
- $EUF \models a{=}e_4$

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2			
e_3	$=$	e_4+3			
a	$=$	e_4			

The two solvers only share constants: $x, e_1, a, b, e_2, e_3, e_4$

- *Ari*-Solver says SAT
- *EUF*-Solver says SAT
- No theory entails any other interface equality, but...

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2			
e_3	$=$	e_4+3			
a	$=$	e_4			

The two solvers only share constants: $x, e_1, a, b, e_2, e_3, e_4$

- *Ari*-Solver says SAT
- *EUF*-Solver says SAT
- $Ari \models_T x = e_1 \vee x = e_2$. Let's consider both cases.

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2	x	$=$	e_1
e_3	$=$	e_4+3			
a	$=$	e_4			
x	$=$	e_1			

- *Ari*-Solver says SAT
- *EUF*-Solver says SAT
- $EUF \models_T a{=}b$, that when sent to *Ari* makes it **UNSAT**

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2			
e_3	$=$	e_4+3			
a	$=$	e_4			

Let's try now with $x{=}e_2$

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2	x	$=$	e_2
e_3	$=$	e_4+3			
a	$=$	e_4			
x	$=$	e_2			

- *Ari*-Solver says SAT
- *EUF*-Solver says SAT
- $EUF \models_T b{=}e_3$, that when sent to *Ari* makes it **UNSAT**

Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

Arithmetic			*EUF*		
1	$\leq$	x	$f(e_1)$	$=$	a
x	$\leq$	2	$f(x)$	$=$	b
e_1	$=$	1	$f(e_2)$	$=$	e_3
a	$=$	$b+2$	$f(e_1)$	$=$	e_4
e_2	$=$	2	x	$=$	e_2
e_3	$=$	e_4+3			
a	$=$	e_4			
x	$=$	e_2			

Since both $x{=}e_1$ and $x = e_2$ are **UNSAT**, the set of literals is **UNSAT**

Nelson-Oppen - The non-convex case

- In the previous example Deterministic NO does not work
- This was because $T_{LA(\mathbb{Z})}$ is not convex:

$$S_{LA(\mathbb{Z})} \models_{T_{LA(\mathbb{Z})}} x{=}e_1 \vee x{=}e_2, \text{ but}$$
$$S_{LA(\mathbb{Z})} \not\models_{T_{LA(\mathbb{Z})}} x{=}e_1 \text{ and}$$
$$S_{LA(\mathbb{Z})} \not\models_{T_{LA(\mathbb{Z})}} x{=}e_2$$

- However, there is a version of NO for non-convex theories
- Given a set constants $\mathcal{C}$, an arrangement $\mathcal{A}$ over $\mathcal{C}$ is:
  - A set of equalities and disequalites between constants in $\mathcal{C}$
  - For each $x, y \in \mathcal{C}$ either $x{=}y \in \mathcal{A}$ or $x \neq y \in \mathcal{A}$

Nelson-Oppen – The non-convex case (2)

Non-deterministic Nelson-Oppen:

- Given two stably-infinite theories T_1 and T_2
- Given a set of literals S over the signature $T_1 \cup T_2$
- The $(T_1 \cup T_2)$-satisfiability of S can be checked via:

1. Purify S and split it into $S_1 \cup S_2$
   Let $\mathcal{C}$ be the set of shared constants
2. For every arrangement $\mathcal{A}$ over $\mathcal{C}$ do
   If $(S_1 \cup \mathcal{A})$ is T_1-satisfiable and $(S_2 \cup \mathcal{A})$ is T_2-satisfiable
   report **SAT**
3. Report **UNSAT**