Combining Decision Procedures: The Nelson-Oppen approach

Albert Oliveras and Enric Rodríguez-Carbonell

Deduction and Verification Techniques
Session 4
Fall 2009, Barcelona
Need for combination

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

\[ a = b + 2 \land A = \text{write}(B, a + 1, 4) \land (\text{read}(A, b + 3) = 2 \lor f(a - 1) \neq f(b + 1)) \]

- 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:

\[
\begin{align*}
f(f(x) - f(y)) &= a \\
f(0) &= a + 2 \\
x &= y
\end{align*}
\]

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

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

\[
\begin{align*}
f(f(x) - f(y)) &= a & \implies f(e_1) &= a \\
e_1 &= f(x) - f(y) & \implies e_1 &= e_2 - e_3 \\
e_2 &= f(x) \\
e_3 &= f(y)
\end{align*}
\]
Motivating example - Convex case

Consider the following set of literals:

\[ f(f(x) - f(y)) = a \]
\[ f(0) = a + 2 \]
\[ x = y \]

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

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

\[ f(0) = a + 2 \implies f(e_4) = a + 2 \implies f(e_4) = e_5 \]
\[ e_4 = 0 \implies e_4 = 0 \]
\[ e_5 = a + 2 \]
SECOND STEP: check satisfiability and exchange entailed equalities

\[
\begin{align*}
EUF & & Arithmetic \\
\begin{align*}
f(e_1) &= a \\
f(x) &= e_2 \\
f(y) &= e_3 \\
f(e_4) &= e_5 \\
x &= y 
\end{align*}
\begin{align*}
e_2 - e_3 &= e_1 \\
e_4 &= 0 \\
e_5 &= a + 2
\end{align*}
\]

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

\[
\begin{align*}
EUF & & Arithmetic \\
 f(e_1) & = & a & e_2 - e_3 & = & e_1 \\
 f(x) & = & e_2 & e_4 & = & 0 \\
 f(y) & = & e_3 & e_5 & = & a + 2 \\
 f(e_4) & = & e_5 & e_2 & = & e_3 \\
 x & = & y & & & \\
\end{align*}
\]

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

\[
\begin{align*}
\text{EUF} & \quad \text{Arithmetic} \\
\ f(e_1) & = \ a \\ 
\ f(x) & = \ e_2 \\ 
\ f(y) & = \ e_3 \\ 
\ f(e_4) & = \ e_5 \\ 
\ x & = \ y \\ 
\ e_1 & = \ e_4 \\
\end{align*}
\]

The two solvers only share constants: \( e_1, e_2, e_3, e_4, e_5, a \)

- \( \text{EUF-Solver says SAT} \)
- \( \text{Ari-Solver says SAT} \)
- \( \text{Ari } \models e_1 = e_4 \)
Motivating example - Convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

\[
\begin{align*}
EUF & \quad & Arithmetic \\
\begin{align*}
f(e_1) &= a \\
f(x) &= e_2 \\
f(y) &= e_3 \\
f(e_4) &= e_5 \\
x &= y \\
e_1 &= e_4
\end{align*} & \quad & \begin{align*}
e_2 - e_3 &= e_1 \\
e_4 &= 0 \\
e_5 &= a + 2 \\
e_2 &= e_3 \\
a &= e_5
\end{align*}
\]

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

\[
\begin{align*}
EUF & & Arithmetic \\
\text{f}(e_1) & = & a & e_2 - e_3 & = & e_1 \\
\text{f}(x) & = & e_2 & e_4 & = & 0 \\
\text{f}(y) & = & e_3 & e_5 & = & a + 2 \\
\text{f}(e_4) & = & e_5 & e_2 & = & e_3 \\
x & = & y & a & = & e_5 \\
e_1 & = & e_4 \\
\end{align*}
\]

The two solvers only share constants: \( e_1, e_2, e_3, e_4, e_5, a \)

- \( \text{EUF-Solver says SAT} \)
- \( \text{Ari-Solver says UNSAT} \)
- Hence the original set of lits was \( \text{UNSAT} \)
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
  \[ S \models_T a_1=b_1 \lor \ldots \lor a_n=b_n \implies S \models a_i=b_i \text{ for some } i \]

**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
Deterministic Nelson-Oppen

1. Purify $S$ and split it into $S_1 \cup S_2$.
   Let $E$ 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 $x = y \in E \setminus S_2$ then
   $S_2 := S_2 \cup \{x = y\}$ and goto 3
5. If $S_2 \models_{T_2} x = y$ with $x = y \in E \setminus S_1$ 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:

\[
1 \leq x \leq 2 \\
f(1) = a \\
f(x) = b \\
a = b + 2 \\
f(2) = f(1) + 3
\]

There are **two theories** involved: \( T_{LA(Z)} \) and \( T_{UF} \)

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

\[
f(1) = a \implies f(e_1) = a \\
e_1 = 1
\]
Motivating example – Non-convex case

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

\[
1 \leq x \leq 2 \\
f(1) = a \\
f(x) = b \\
a = b + 2 \\
f(2) = f(1) + 3
\]

There are **two theories** involved: \( T_{LA(Z)} \) and \( T_{UF} \)

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

\[
f(2) = f(1) + 3 \implies e_2 = 2 \\
f(e_2) = e_3 \\
f(e_1) = e_4 \\
e_3 = e_4 + 3
\]
SECOND STEP: check satisfiability and exchange entailed equalities

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td>$e_3 = e_4 + 3$</td>
</tr>
<tr>
<td>$e_4 = a$</td>
<td>$e_4 = e_4$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td></td>
</tr>
<tr>
<td>$e_3 = e_4 + 3$</td>
<td></td>
</tr>
<tr>
<td>$a = e_4$</td>
<td></td>
</tr>
</tbody>
</table>

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...
SECOND STEP: check satisfiability and exchange entailed equalities

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td></td>
</tr>
<tr>
<td>$e_3 = e_4 + 3$</td>
<td></td>
</tr>
<tr>
<td>$a = e_4$</td>
<td></td>
</tr>
</tbody>
</table>

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 $\models_T x = e_1 \lor x = e_2$. Let’s consider both cases.
Motivating example – Non-convex case(2)

SECOND STEP: check satisfiability and exchange entailed equalities

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td>$x = e_1$</td>
</tr>
<tr>
<td>$e_3 = e_4 + 3$</td>
<td></td>
</tr>
<tr>
<td>$a = e_4$</td>
<td></td>
</tr>
<tr>
<td>$x = e_1$</td>
<td></td>
</tr>
</tbody>
</table>

- *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

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td></td>
</tr>
<tr>
<td>$e_3 = e_4 + 3$</td>
<td></td>
</tr>
<tr>
<td>$a = e_4$</td>
<td></td>
</tr>
</tbody>
</table>

Let’s try now with $x=e_2$
Motivating example – Non-convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ≤ x</td>
<td>( f(e_1) = a )</td>
</tr>
<tr>
<td>x ≤ 2</td>
<td>( f(x) = b )</td>
</tr>
<tr>
<td>( e_1 = 1 )</td>
<td>( f(e_2) = e_3 )</td>
</tr>
<tr>
<td>( a = b + 2 )</td>
<td>( f(e_1) = e_4 )</td>
</tr>
<tr>
<td>( e_2 = 2 )</td>
<td>( x = e_2 )</td>
</tr>
<tr>
<td>( e_3 = e_4 + 3 )</td>
<td></td>
</tr>
<tr>
<td>( a = e_4 )</td>
<td></td>
</tr>
<tr>
<td>( x = e_2 )</td>
<td></td>
</tr>
</tbody>
</table>

- **Ari-Solver** says SAT
- **EUF-Solver** says SAT
- **EUF** \( \vdash_T b = e_3 \), that when sent to Ari makes it **UNSAT**
Motivating example – Non-convex case (2)

SECOND STEP: check satisfiability and exchange entailed equalities

<table>
<thead>
<tr>
<th>Arithmetic</th>
<th>EUF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \leq x$</td>
<td>$f(e_1) = a$</td>
</tr>
<tr>
<td>$x \leq 2$</td>
<td>$f(x) = b$</td>
</tr>
<tr>
<td>$e_1 = 1$</td>
<td>$f(e_2) = e_3$</td>
</tr>
<tr>
<td>$a = b + 2$</td>
<td>$f(e_1) = e_4$</td>
</tr>
<tr>
<td>$e_2 = 2$</td>
<td>$x = e_2$</td>
</tr>
<tr>
<td>$e_3 = e_4 + 3$</td>
<td></td>
</tr>
<tr>
<td>$a = e_4$</td>
<td></td>
</tr>
<tr>
<td>$x = e_2$</td>
<td></td>
</tr>
</tbody>
</table>

Since both $x = e_1$ and $x = e_2$ are UNSAT, the set of literals is UNSAT.
In the previous example Deterministic NO does not work.

This was because $T_{LA}(Z)$ is not convex:

$$S_{LA}(Z) \models_{T_{LA}(Z)} x=e_1 \lor x=e_2,$$

but

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

However, there is a version of NO for non-convex theories.

Given a set constants $C$, an arrangement $A$ over $C$ is:

- A set of equalities and disequalities between constants in $C$
- For each $x, y \in C$ either $x=y \in A$ or $x \neq y \in A$
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 $C$ be the set of shared constants
2. For every arrangement $A$ over $C$ do
   If $(S_1 \cup A)$ is $T_1$-satisfiable and $(S_2 \cup A)$ is $T_2$-satisfiable
   report SAT
3. Report UNSAT