Nelson-Oppen Combination

Deepak D'Souza

Department of Computer Science and Automation
Indian Institute of Science, Bangalore.

15 April 2025

Nelson-Oppen Combination [Greg Nelson PhD Thesis 1981]

A way to combine decision procedures for the quantifier-free fragments of two logics to obtain a decision procedure for the quantifier-free fragment of the combined logic.

Examples:

- EUF + LRA
- BA (Basic Array Logic) + LIA

Combined procedure is based on "Equality Sharing" (propagating equalities between variables from one theory to the other).

Some caveats:

- Logics should be stably infinite (if a formula is satisfiable, it is satisfiable in an infinite structure).

Ilustrative Example: LRA + EUF

Example: Is this sentence satisfiable?

$$f(f(x) - f(y)) \neq f(z) \land x \leq y \land y + z \leq x \land z \geq 0$$

Ilustrative Example: LRA + EUF

Example: Is this sentence satisfiable?

$$f(f(x) - f(y)) \neq f(z) \wedge x \leq y \wedge y + z \leq x \wedge z \geq 0$$

No, because the arithmetic constraints imply that $x = y$ and $z = 0$; and the functional constraints must then imply that $f(f(x) - f(y)) = f(0) = f(z)$.

Equality Sharing Procedure

Is this sentence satisfiable?

$$f(f(x) - f(y)) \neq f(z) \wedge x \leq y \wedge y + z \leq x \wedge z \geq 0$$

"Purify" or "Segregate" formula into the two theories, introducing new variables for "foreign" terms:

LRA Constraints: F_1

$$\begin{aligned} x &\leq y \\ y + z &\leq x \\ z &\geq 0 \\ g_2 - g_3 &= g_1 \end{aligned}$$

EUF Constraints: G_1

$$\begin{aligned} f(g_1) &\neq f(z) \\ f(x) &= g_2 \\ f(y) &= g_3 \end{aligned}$$

Equality Sharing Procedure

Both formulas (LRA conjunction, EUF conjunction) are satisfiable.
F_1 implies $x = y$. Propagate equalities:

LRA Constraints: F_2

$$\begin{aligned} x &\leq y \\ y + z &\leq x \\ z &\geq 0 \\ g_2 - g_3 &= g_1 \end{aligned}$$

EUF Constraints G_2

$$\begin{aligned} f(g_1) &\neq f(z) \\ f(x) &= g_2 \\ f(y) &= g_3 \\ x &= y \end{aligned}$$

Equality Sharing Procedure

Formulas are satisfiable. Now G_2 implies $g_2 = g_3$. Propagate equalities:

LRA Constraints: F_3

$$\begin{aligned} x &\leq y \\ y + z &\leq x \\ z &\geq 0 \\ g_2 - g_3 &= g_1 \\ g_2 &= g_3 \end{aligned}$$

EUF Constraints G_3

$$\begin{aligned} f(g_1) &\neq f(z) \\ f(x) &= g_2 \\ f(y) &= g_3 \\ x &= y \end{aligned}$$

Equality Sharing Procedure

Formulas are satisfiable. Now F_3 implies $g_1 = z$. Propagate equalities:

LRA Constraints: F_4

$$\begin{aligned} x &\leq y \\ y + z &\leq x \\ z &\geq 0 \\ g_2 - g_3 &= g_1 \\ g_2 &= g_3 \end{aligned}$$

EUF Constraints G_4

$$\begin{aligned} f(g_1) &\neq f(z) \\ f(x) &= g_2 \\ f(y) &= g_3 \\ x &= y \\ g_1 &= z \end{aligned}$$

G_4 is unsat. So return UNSAT.

If formulas were satisfiable and no more equalities to propagate, return SAT.

Nelson-Oppen Combination

Does this procedure work for integer arithmetic and functions?

Is this sentence satisfiable? (int x)

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

Arithmetic Constraints

$$\begin{aligned} 1 &\leq x \\ x &\leq 2 \\ a &= 1 \\ b &= 2 \end{aligned}$$

Function Constraints

$$\begin{aligned} f(x) &\neq f(a) \\ f(x) &\neq f(b) \end{aligned}$$

Need case-splits for "non-convex" theories.

Convex Formulas

Formula F is convex if whenever

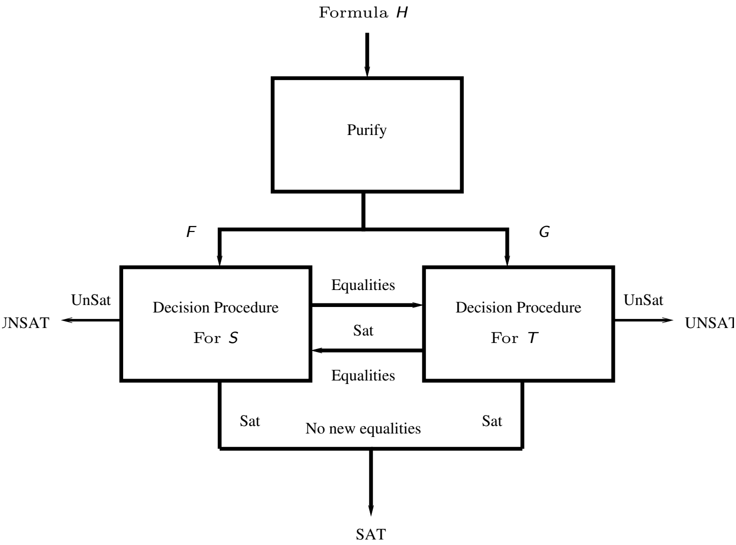
$$F \Rightarrow \bigvee_{i=1}^{n} (x_i = y_i),$$

then

$$F \Rightarrow (x_i = y_i)$$

for some i.

Equality Sharing Algorithm



Equality Sharing Algorithm

1. Purify give formula into S and T formulas F and G.
2. If either F or G is unsat, return UNSAT.
3. If both F and G are (separately) satisfiable, propagate "new" equalities from F to G (not already implied by G). Go back to Step 2.
4. If non-convex, do case-split and check each case separately via Step 2.
5. If nothing to propagate, return SAT.

Correctness of Algo

Theorem (Correctness of Equality Sharing Algo)

Algo return SAT (respectively UNSAT) iff original formula was satisfiable (respectively unsatisfiable).

Residue of a formula

The Residue R_F of a formula F (in a theory S) is the strongest boolean combination of equalties implied by F.

Examples:

Formula	Residue
$x = f(a) \wedge y = f(b)$	$a = b \Rightarrow x = y$
$x \leq y \wedge y \leq x$	$x = y$
$x + y > a - b$	$\neg(x = a \wedge y = b) \wedge \neg(x = b \wedge y = a)$

Claim: If F and G are separately satisfiable and don't imply any new equalities wrt eachother, then $F \wedge G$ is satisfiable iff $R_F \wedge R_G$ is satisfiable.

Correctness of Algo follows from this.