### The Nelson–Oppen Algorithm (Non-deterministic Version)

Suppose that $\exists\vec{x}\, F$ is a purified conjunction of $\Sigma_1$ and $\Sigma_2$-literals.

Let $F_1$ be the conjunction of all literals of $F$ that do not contain $\Sigma_2$-symbols; let $F_2$ be the conjunction of all literals of $F$ that do not contain $\Sigma_1$-symbols. (Equations between variables are in both $F_1$ and $F_2$.)

The Nelson–Oppen algorithm starts with the pair $F_1, F_2$ and applies the following inference rules.

*Unsat:*

$$\frac{F_1, F_2}{\bot}$$

if $\exists\vec{x}\, F_i$ is unsatisfiable w. r. t. $\mathcal{T}_i$ for some $i$.

*Branch:*

$$\frac{F_1, F_2}{F_1 \wedge (x \approx y), F_2 \wedge (x \approx y) \quad | \quad F_1 \wedge (x \not\approx y), F_2 \wedge (x \not\approx y)}$$

if $x$ and $y$ are two different variables appearing in both $F_1$ and $F_2$ such that neither $x \approx y$ nor $x \not\approx y$ occurs in both $F_1$ and $F_2$

"|" means non-deterministic (backtracking!) branching of the derivation into two sub-derivations. Derivations are therefore trees. All branches need to be reduced until termination.

Clearly, all derivation paths are finite since there are only finitely many *shared variables* in $F_1$ and $F_2$, therefore the procedure represented by the rules is terminating.

We call a constraint configuration to which no rule applies *irreducible*.

**Theorem 1.1 (Soundness)** *If "Branch" can be applied to $F_1, F_2$, then $\exists\vec{x}\,(F_1 \wedge F_2)$ is satisfiable in $\mathcal{T}_1 \cup \mathcal{T}_2$ if and only if one of the successor configurations of $F_1, F_2$ is satisfiable in $\mathcal{T}_1 \cup \mathcal{T}_2$.*

**Corollary 1.2** *If all paths in a derivation tree from $F_1, F_2$ end in $\bot$, then $\exists\vec{x}\,(F_1 \wedge F_2)$ is unsatisfiable in $\mathcal{T}_1 \cup \mathcal{T}_2$.*

For completeness we need to show that if one branch in a derivation terminates with an irreducible configuration $F_1, F_2$ (different from $\bot$), then $\exists\vec{x}\,(F_1 \wedge F_2)$ (and, thus, the initial formula of the derivation) is satisfiable in the combined theory.

As $\exists \vec{x}\,(F_1 \wedge F_2)$ is irreducible by "Unsat", the two formulas are satisfiable in their respective component theories, that is, we have $\mathcal{T}_i$-models $\mathcal{A}_i$ of $\exists \vec{x}\, F_i$ for $i \in \{1, 2\}$. We are left with combining the models into a single one that is both a model of the combined theory and of the combined formula. These constructions are called *amalgamations*.

Let $F$ be a $\Sigma_i$-formula and let $S$ be a set of variables of $F$. $F$ is called *compatible* with an equivalence $\sim$ on $S$ if the formula

$$\exists \vec{z} \Big( F \wedge \bigwedge_{x,y\in S,\, x\sim y} x \approx y \wedge \bigwedge_{x,y\in S,\, x\not\sim y} x \not\approx y \Big) \tag{1}$$

is $\mathcal{T}_i$-satisfiable whenever $F$ is $\mathcal{T}_i$-satisfiable. This expresses that $F$ does not contradict equalities between the variables in $S$ as given by $\sim$.

**Proposition 1.3** *If $F_1, F_2$ is a pair of conjunctions over $\mathcal{T}_1$ and $\mathcal{T}_2$, respectively, that is irreducible by "Branch", then both $F_1$ and $F_2$ are compatible with some equivalence $\sim$ on the shared variables $S$ of $F_1$ and $F_2$.*

**Proof.** If $F_1, F_2$ is irreducible by the branching rule, then for each pair of shared variables $x$ and $y$, both $F_1$ and $F_2$ contain either $x \approx y$ or $x \not\approx y$. Choose $\sim$ to be the equivalence given by all (positive) variable equations between shared variables that are contained in $F_1$.

**Lemma 1.4 (Amalgamation Lemma)** *Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two stably infinite theories over disjoint signatures $\Sigma_1$ and $\Sigma_2$. Furthermore let $F_1, F_2$ be a pair of conjunctions of literals over $\mathcal{T}_1$ and $\mathcal{T}_2$, respectively, both compatible with some equivalence $\sim$ on the shared variables of $F_1$ and $F_2$. Then $F_1 \wedge F_2$ is $(\mathcal{T}_1 \cup \mathcal{T}_2)$-satisfiable if and only if each $F_i$ is $\mathcal{T}_i$-satisfiable.*

**Proof.** The "only if" part is obvious.

For the "if" part, assume that each of the $F_i$ is $\mathcal{T}_i$-satisfiable. That is, there exist models $\mathcal{A}_i$ of $\mathcal{T}_i$ and variable assignments $\beta_i$ such that $\mathcal{A}_i, \beta_i \models F_i$. As the $F_i$ are compatible with an equivalence $\sim$ on their shared variables, we may assume that the $\beta_i$ also satisfy the extended conjunctions in (1) with $S$ the set of shared variables. In particular, whenever we have two shared variables $x$ and $y$, $\beta_1(x) = \beta_1(y)$ if and only if $\beta_2(x) = \beta_2(y)$. Since the theories are stably infinite we may additionally assume that the $\mathcal{A}_i$ have countably infinite universes, hence there are bijections $\rho_i$ from the domain of $\mathcal{A}_i$ to $\mathbb{N}$ such that $\rho_1(\beta_1(x))) = \rho_2(\beta_2(x))$ for each shared variable $x$. Now define $\mathcal{A}$ to be the algebra having $\mathbb{N}$ as its domain; for $f$ or $P$ in $\Sigma_i$ define $f_{\mathcal{A}}(n_1, \ldots, n_k) = \rho_i(f_{\mathcal{A}_i}(\rho_i^{-1}(n_1), \ldots, \rho_i^{-1}(n_k)))$ and $P_{\mathcal{A}}(n_1, \ldots, n_k) \Leftrightarrow P_{\mathcal{A}_i}(\rho_i^{-1}(n_1), \ldots, \rho_i^{-1}(n_k))$. Define $\beta(x) = \rho_i(\beta_i(x))$ if $x$ is a variable occurring in $F_i$. By construction of the $\rho_i$ this definition is independent of the choice of $i$. Clearly $\mathcal{A}|_{\Sigma_i}, \beta \models F_i$, for $i = 1, 2$, hence $\mathcal{A}, \beta \models F_1 \wedge F_2$. Moreover, the reducts $\mathcal{A}|_{\Sigma_i}$ are isomorphic (via $\rho_i$) to $\mathcal{A}_i$ and thus are models of $\mathcal{T}_i$, so that $\mathcal{A}$ is a model of $\mathcal{T}_1 \cup \mathcal{T}_2$ as required.

**Theorem 1.5** *The non-deterministic Nelson–Oppen algorithm is terminating and complete for deciding satisfiability of pure conjunctions of literals $F_1$ and $F_2$ over $\mathcal{T}_1 \cup \mathcal{T}_2$ for signature-disjoint, stably infinite theories $\mathcal{T}_1$ and $\mathcal{T}_2$.*

**Proof.** Suppose that $F_1, F_2$ is irreducible by the inference rules of the Nelson–Oppen algorithm. Applying the amalgamation lemma in combination with Prop. 1.3 we infer that $F_1, F_2$ is satisfiable w. r. t. $\mathcal{T}_1 \cup \mathcal{T}_2$.

### Convexity

The number of possible equivalences of shared variables grows superexponentially with the number of shared variables, so enumerating all possible equivalences non-deterministically is going to be inefficient.

A much faster variant of the Nelson–Oppen algorithm exists for convex theories.

A first-order theory $\mathcal{T}$ is called *convex w. r. t. equations*, if for every conjunction $\Gamma$ of $\Sigma$-equations and non-equational $\Sigma$-literals and for all $\Sigma$-equations $A_i$ $(1 \leq i \leq n)$, whenever $\mathcal{T} \models \forall \vec{x}\,(\Gamma \rightarrow A_1 \vee \ldots \vee A_n)$, then there exists some index $j$ such that $\mathcal{T} \models \forall \vec{x}\,(\Gamma \rightarrow A_j)$.

**Theorem 1.6** *If a first-order theory $\mathcal{T}$ is convex w. r. t. equations and has no trivial models (i. e., models with only one element), then $\mathcal{T}$ is stably infinite.*

**Proof.** We shall prove the contrapositive of the statement. Suppose $\mathcal{T}$ is not stably infinite. Then there exists a satisfiable conjunction of literals $\exists \vec{x}\, F$ that has only finite models w. r. t. $\mathcal{T}$. We split $F$ into two conjunctions $F^+$ and $F^-$, such that $F^-$ contains the negative equational literals in $F$ and $F^+$ contains the rest. As $\mathcal{T}$ is a first-order theory, it is compact, hence all models of $F$ are bounded in cardinality by some number $m$. Now consider the clause $C = F^+ \rightarrow \neg F^- \vee \bigvee_{1 \leq i < j \leq m+1} y_i \approx y_j$, with fresh variables $y_1, \ldots, y_{m+1}$ not occurring in $F$. $\mathcal{T} \models \forall \vec{x}, \vec{y}\, C$, as the clause exactly expresses that all models of $F$ have size less than or equal to $m$. However, $\mathcal{T} \not\models \forall \vec{x}, \vec{y}\,(F^+ \rightarrow A)$, for any literal $A$ of $\neg F^-$ (as otherwise $F$ would not be satisfiable), and also $\mathcal{T} \not\models \forall \vec{x}, \vec{y}\,(F^+ \rightarrow y_i \approx y_j)$, for each $i, j$, as otherwise $\mathcal{T}$ would have trivial models, which we have excluded.

**Lemma 1.7** *Suppose $\mathcal{T}$ is convex, $F$ a conjunction of literals, and $S$ a subset of its variables. Let, for any pair of variables $x_i$ and $x_j$ in $S$, $x_i \sim x_j$ if and only if $\mathcal{T} \models \forall \vec{x}\,(F \rightarrow x_i \approx x_j)$. Then $F$ is compatible with $\sim$.*

**Proof.** We show that with this choice of $\sim$ the constraint (1) is satisfiable in $\mathcal{T}$ whenever $F$ is. Suppose, to the contrary, that $F$ is satisfiable but (1) is not, that is,

$$\mathcal{T} \models \forall \vec{z} \Big( F \rightarrow \bigvee_{x,y \in S,\ x \sim y} x \not\approx y \ \vee \bigvee_{x,y \in S,\ x \not\sim y} x \approx y \Big)$$

or, equivalently,

$$\mathcal{T} \models \forall \vec{z} \Big( F^{+} \wedge \bigwedge_{x,y \in S,\ x \sim y} x \approx y \ \rightarrow \ \neg F^{-} \vee \bigvee_{x,y \in S,\ x \not\sim y} x \approx y \Big).$$

By convexity of $\mathcal{T}$, the antecedent implies one of the equations of the succedent. Since the equations $x \approx y$, with $x \sim y$, are entailed by $F$ and since $F$ is satisfiable, this means that this equation must come from the last disjunct. In other words, there exists a pair of different variables $x'$ and $y'$ in $S$ such that $x' \not\sim y'$ and

$$\mathcal{T} \models \forall \vec{z} \Big( F^{+} \wedge \bigwedge_{x,y \in S,\ x \sim y} x \approx y \ \rightarrow \ x' \approx y' \Big).$$

Since

$$\mathcal{T} \models \forall \vec{z} \Big( F \rightarrow \bigwedge_{x,y \in S,\ x \sim y} x \approx y \Big),$$

we derive $\mathcal{T} \models \forall \vec{z} \Big( F \ \rightarrow \ x' \approx y' \Big)$, which is impossible.

### The Nelson–Oppen Algorithm (Deterministic Version for Convex Theories)

*Unsat:*

$$\frac{F_1, F_2}{\bot}$$

if $\exists \vec{x}\, F_i$ is unsatisfiable w. r. t. $\mathcal{T}_i$ for some $i$.

*Propagate:*

$$\frac{F_1, F_2}{F_1 \wedge (x \approx y), F_2 \wedge (x \approx y)}$$

if $x$ and $y$ are two different variables appearing in both $F_1$ and $F_2$ such that
$\mathcal{T}_1 \models \forall \vec{x}\,(F_1 \rightarrow x \approx y)$ and $\mathcal{T}_2 \not\models \forall \vec{x}\,(F_2 \rightarrow x \approx y)$
or $\mathcal{T}_2 \models \forall \vec{x}\,(F_2 \rightarrow x \approx y)$ and $\mathcal{T}_1 \not\models \forall \vec{x}\,(F_1 \rightarrow x \approx y)$.

**Theorem 1.8** *If $\mathcal{T}_1$ and $\mathcal{T}_2$ are signature-disjoint theories that are convex w. r. t. equations and have no trivial models, then the deterministic Nelson–Oppen algorithm is terminating, sound and complete for deciding satisfiability of pure conjunctions of literals $F_1$ and $F_2$ over $\mathcal{T}_1 \cup \mathcal{T}_2$.*

**Proof.** Termination and soundness are obvious: there are only finitely many different equations that can be added, and each of them is entailed by given formulas.

For completeness, we have to show that every configuration that is irreducible by "Unsat" and "Propagate" is satisfiable w. r. t.. $\mathcal{T}_1 \cup \mathcal{T}_2$: Let $F_1, F_2$ be such a configuration. As it is irreducible by "Propagate", we have, for every equation $x \approx y$ between shared variables, $\mathcal{T}_1 \models \forall \vec{x}\,(F_1 \to x \approx y)$ if and only if $\mathcal{T}_2 \models \forall \vec{x}\,(F_2 \to x \approx y)$. Consequently, $F_1$ and $F_2$ are compatible with the same equivalence on the shared variables of $F_1$ and $F_2$. Moreover, each of the formulas $F_i$ is $\mathcal{T}_i$-satisfiable, and since convexity implies stable infiniteness, $F_i$ has a $\mathcal{T}_i$-model with a countably infinite universe. Hence, by the amalgamation lemma, $F_1 \wedge F_2$ is $(\mathcal{T}_1 \cup \mathcal{T}_2)$-satisfiable.

**Corollary 1.9** *The deterministic Nelson–Oppen algorithm for convex theories requires at most $O(n^3)$ calls to the individual decision procedures for the component theories, where $n$ is the number of shared variables.*

### Iterating Nelson–Oppen

The Nelson–Oppen combination procedures can be iterated to work with more than two component theories by virtue of the following observations where signature disjointness is assumed:

**Theorem 1.10** *If $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably infinite, then so is $\mathcal{T}_1 \cup \mathcal{T}_2$.*

**Proof.** The non-deterministic Nelson–Oppen algorithm is sound and complete for $\mathcal{T}_1 \cup \mathcal{T}_2$, that is, an existentially quantified conjunction $F$ over $\Sigma_1 \cup \Sigma_2$ is satisfiable if and only if in every derivation from the purified form of $F$ there exists a branch leading to some irreducible constraint $F_1, F_2$ entailing $F$. The amalgamation lemma 1.4 constructs a model with a countably infinite universe for $F$ from the models of $F_1$ and $F_2$.

**Lemma 1.11** *A first-order theory $\mathcal{T}$ is convex w. r. t. equations if and only if for every conjunction $\Gamma$ of $\Sigma$-equations and non-equational $\Sigma$-literals and for all equations $x_i \approx x'_i$ $(1 \leq i \leq n)$, whenever $\mathcal{T} \models \forall \vec{x}\,(\Gamma \to x_1 \approx x'_1 \vee \ldots \vee x_n \approx x'_n)$, then there exists some index $j$ such that $\mathcal{T} \models \forall \vec{x}\,(\Gamma \to x_j \approx x'_j)$.*

**Lemma 1.12** *Let $\mathcal{T}$ be a first-order theory that is convex w. r. t. equations. Let $F$ is a conjunction of literals; let $F^-$ be the conjunction of all negative equational literals in $F$ and let $F^+$ be the conjunction of all remaining literals in $F$. If $\mathcal{T} \models \forall\vec{x}\,(F \to x \approx y)$, then $\exists\vec{x}\,F$ is $\mathcal{T}$-unsatisfiable or $\mathcal{T} \models \forall\vec{x}\,(F^+ \to x \approx y)$.*

**Proof.** $\mathcal{T} \models \forall\vec{x}\,(F \to x \approx y)$ is equivalent to $\mathcal{T} \models \forall\vec{x}\,(F^+ \to (\neg F^- \vee x \approx y))$. By convexity of $\mathcal{T}$ we know that $\mathcal{T} \models \forall\vec{x}\,(F^+ \to x \approx y)$ or $\mathcal{T} \models \forall\vec{x}\,(F^+ \to A)$ for some literal $\neg A$ in $F^-$. In the latter case, $\exists\vec{x}\,(F^+ \wedge \neg A)$ is $\mathcal{T}$-unsatisfiable; hence $\exists\vec{x}\,F$, that is, $\exists\vec{x}\,(F^+ \wedge F^-)$ is $\mathcal{T}$-unsatisfiable as well.

**Theorem 1.13** *If $\mathcal{T}_1$ and $\mathcal{T}_2$ are convex w. r. t. equations and do not have trivial models, then so is $\mathcal{T}_1 \cup \mathcal{T}_2$.*

**Proof.** Suppose that $\mathcal{T}_1$ and $\mathcal{T}_2$ are convex w. r. t. equations and do not have trivial models. Assume furthermore that $\mathcal{T} \models \forall\vec{x}\,(\Gamma \to x_1 \approx x'_1 \vee \ldots \vee x_n \approx x'_n)$ for some conjunction $\Gamma$ of $(\Sigma_1 \cup \Sigma_2)$-equations and non-equational $(\Sigma_1 \cup \Sigma_2)$-literals. Then $\exists\vec{x}\,(\Gamma \wedge x_1 \not\approx x'_1 \wedge \ldots \wedge x_n \not\approx x'_n)$ is $\mathcal{T}$-unsatisfiable, and we can detect this by some run of the deterministic Nelson–Oppen algorithm starting with $\exists\vec{x},\vec{y}\,(\Gamma_1 \wedge \Gamma_2 \wedge x_1 \not\approx x'_1 \wedge \ldots \wedge x_n \not\approx x'_n)$, where $\Gamma_1 \wedge \Gamma_2$ is the result of purifying $\Gamma$. This run consists of a sequence of "Propagate" steps followed by a final "Unsat" step, and without loss of generality, we use the "Propagate" rule only if "Unsat" cannot be applied. Consequently, whenever we add an equation $x \approx y$ that is entailed by $F_1$ w. r. t. $\mathcal{T}_1$ or by $F_2$ w. r. t. $\mathcal{T}_2$, then it is by Lemma 1.12 already entailed by the positive and the non-equational literals in $F_1$ or $F_2$. Furthermore, due to the convexity of $\mathcal{T}_1$ and $\mathcal{T}_2$, the final "Unsat" step depends on at most one negative equational literal in $F_1$ or $F_2$. We can therefore construct a similar Nelson–Oppen derivation that starts with only the positive and the non-equational literals in $\Gamma_1$ and $\Gamma_2$, plus at most one negative equational literal that may be needed for the "Unsat" step. If a negative equational literal is needed, it is one of the $x_j \not\approx x'_j$; then $\exists\vec{x}\,(\Gamma \wedge x_j \not\approx x'_j)$ is $\mathcal{T}$-unsatisfiable and $\forall\vec{x}\,(\Gamma \to x_j \approx x'_j)$ is $\mathcal{T}$-valid; if no negative equational literal is needed at all, then $\exists\vec{x}\,\Gamma$ is $\mathcal{T}$-unsatisfiable, so $\forall\vec{x}\,(\Gamma \to x_j \approx x'_j)$ is $\mathcal{T}$-valid for every $j$.

### Extensions

Many-sorted logics:

$read/2$ becomes $read : array \times int \to data.$
$write/3$ becomes $write : array \times int \times data \to array.$
Variables: $x : data$

Only one declaration per function/predicate/variable symbol.
All terms, atoms, substitutions must be well-sorted.

Algebras:

Instead of universe $U_{\mathcal{A}}$, one set per sort: $array_{\mathcal{A}}$, $int_{\mathcal{A}}$.

Interpretations of function and predicate symbols correspond to their declarations: $read_{\mathcal{A}} : array_{\mathcal{A}} \times int_{\mathcal{A}} \to data_{\mathcal{A}}$

If we consider combinations of theories with shared sorts but disjoint function and predicate symbols, then we get essentially the same combination results as before.

However, stable infiniteness and/or convexity are only required for the shared sorts.

Non-stably infinite theories:

If we impose stronger conditions on one theory, we can relax the conditions on the other one.

For instance, EUF can be combined with any other theory; stable infiniteness is not required.

Non-disjoint combinations:

Have to ensure that both decision procedures interpret shared symbols in a compatible way.

Some results, e. g. by Ghilardi, using strong model theoretical conditions on the theories.

## Another Combination Method

Shostak's method:

Applicable to combinations of EUF and *solvable* theories.

A $\Sigma$-theory $\mathcal{T}$ is called *solvable*, if there exists an effectively computable function *solve* such that, for any $\mathcal{T}$-equation $s \approx t$:

(A) $\mathit{solve}(s \approx t) = \bot$ if and only if $\mathcal{T} \models \forall \vec{x}\,(s \not\approx t)$;

(B) $\mathit{solve}(s \approx t) = \emptyset$ if and only if $\mathcal{T} \models \forall \vec{x}\,(s \approx t)$; and otherwise

(C) $\mathit{solve}(s \approx t) = \{x_1 \approx u_1, \dots, x_n \approx u_n\}$, where

- the $x_i$ are pairwise different variables occurring in $s \approx t$;
- the $x_i$ do not occur in the $u_j$; and
- $\mathcal{T} \models \forall \vec{x}\,((s \approx t) \leftrightarrow \exists \vec{y}\,(x_1 \approx u_1 \wedge \ldots \wedge x_n \approx u_n))$, where $\vec{y}$ are the variables occurring in one of the $u_j$ but not in $s \approx t$, and $\vec{x} \cap \vec{y} = \emptyset$.

Additionally useful (but not required):

A canonizer, that is, a function that simplifies terms by computing some unique normal form

Main idea of the procedure:

If $s \approx t$ is a positive equation and $\mathit{solve}(s \approx t) = \{x_1 \approx u_1, \dots, x_n \approx u_n\}$, replace $s \approx t$ by $x_1 \approx u_1 \wedge \ldots \wedge x_n \approx u_n$ and use these equations to eliminate the $x_i$ elsewhere.

Practical problem:

Solvability is a rather restrictive condition.

## Literature


Harald Ganzinger: Shostak Light. Automated Deduction, CADE-18, LNCS 2392, pp 332–346, Springer, 2002.

Silvio Ghilardi: Model Theoretic Methods in Combined Constraint Satisfiability. Journal of Automated Reasoning, 33(3–4):221–249, 2005.

Greg Nelson, Derek C. Oppen: Simplification by Cooperating Decision Procedures. ACM Transactions on Programming Languages and Systems, 1(2):245–257, 1979.

Robert E. Shostak: Deciding Combinations of Theories. Journal of the ACM, 31(1):1–12, 1984.