First-Order Logic Theories

3.17.1 Definition (First-Order Logic Theory)

Given a first-order many-sorted signature Σ, a *theory* $\mathcal{T}$ is a set of Σ-algebras.
For some first-order formula ϕ over Σ we say that ϕ is $\mathcal{T}$*-satisfiable* if there is some $\mathcal{A} \in \mathcal{T}$ such that $\mathcal{A}(\beta) \models \phi$ for some β. We say that ϕ is $\mathcal{T}$*-valid* ($\mathcal{T}$*-unsatisfiable*) if for all $\mathcal{A} \in \mathcal{T}$ and all β it holds $\mathcal{A}(\beta) \models \phi$ ($\mathcal{A}(\beta) \not\models \phi$). In case of validity I also write $\models_{\mathcal{T}} \phi$.

Alternatively, $\mathcal{T}$ may contain a set of satisfiable axioms which then stand for all algebras satisfying the axioms.

7.1.1 Definition (Convex Theory)

A theory $\mathcal{T}$ is *convex* if for a conjunctionϕ of literals with $\phi \models_{\mathcal{T}} x_1 \approx y_1 \lor \ldots \lor x_n \approx y_n$ then $\phi \models_{\mathcal{T}} x_k \approx y_k$ for some k.

Another property needed for the Nelson-Oppen procedure to work is that the theory models always include models with an infinite domain. Consider the two theories

$$\mathcal{T}_1 = \{\forall x, y(x \approx a \vee x \approx b)\}$$

and

$$\mathcal{T}_2 = \{\forall x, y, z.(x \not\approx y \vee x \not\approx z \vee y \not\approx z\}$$

that do not share any signature symbols. Models of $\mathcal{T}_1$ have at most two elements, models of $\mathcal{T}_2$ at least three. So the conjunction $(\mathcal{T}_1 \cup \mathcal{T}_2)$ is already unsatisfiable. In order to ensure that different models for the respective theory can be combined, the Nelson-Oppen procedure requires the existence of models with infinite cardinality.

7.1.2 Definition (Stably-Infinite Theory)

A theory $\mathcal{T}$ is *stably-infinite* if for every quantifier-free formula ϕ, if $\mathcal{T} \models \phi$, then then there exists also a model $\mathcal{A}$ of infinite cardinality, such that $\mathcal{A} \models_{\mathcal{T}} \phi$

Nelson-Oppen Combination

7.1.3 Definition (Nelson-Oppen Basic Restrictions)

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two theories. Then the *Nelson-Oppen Basic Restrictions* are:

(i) There are decision procedures for for $\mathcal{T}_1$ and $\mathcal{T}_2$.

(ii) Each decision procedure returns a complete set of variable identities as consequence of a formula.

(iii) $\Sigma_1 \cap \Sigma_2 = \emptyset$ except for common sorts.

(iv) Both theories are convex.

(v) $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably-infinite.

Actually, restriction 7.1.3-2 is not needed, because a given finite quantifier-free formula ϕ over $\Sigma_1 \cup \Sigma_2$ contains only finitely many different variables. Now instead of putting the burden to identify variables on the decision procedure, all potential variable identifications can be guessed and tested afterwards. The disadvantage of this approach is, of course, that there are exponentially many identifications with respect to a fixed number of variables. Therefore, assuming 7.1.3-2 results in a more efficient procedure and is also supported by many procedures from Section 6.

Restriction 7.1.3-5 can be further relaxed to assume that the domains of all shared sorts of all models are either infinite or have the same number of elements.

Purification

Purify $\quad N \uplus \{L[t[s]_i]_p\} \;\Rightarrow_{\text{NO}}\; N \uplus \{L[t[z]_i]_p, z \approx s\}$

if $t = f(t_1, \ldots, t_n)$, $s = h(s_1, \ldots, s_m)$, the function symbols f and h are from different signatures, $1 \leq i \leq n$, (i.e., $t_i = s$) and z is a fresh variable of appropriate sort

Nelson-Oppen Calculus

Now a Nelson-Oppen problem state is a five tuple (N_1, E_1, N_2, E_2, s) with $s \in \{\top, \bot, \text{fail}\}$, the sets E_1 and E_2 contain variable equations, and N_1, N_2 literals over the respective signatures, where

$(N_1; \emptyset; N_2; \emptyset; \bot)$	is the start state for some purified set of atoms $N = N_1 \cup N_2$ where the N_i are built from the respective signatures only
$(N_1; E_1; N_2; E_2; \text{fail})$	is a final state, where $N_1 \cup N_2 \cup E_1 \cup E_2$ is unsatisfiable
$(N_1; E_1; N_2; E_2; \bot)$	is an intermediate state, where $N_1 \cup E_2$ and $N_2 \cup E_1$ have to be checked for satisfiability
$(N_1; \emptyset; N_2; \emptyset; \top)$	is a final state, where $N_1 \cup N_2$ is satisfiable

Solve $(N_1; E_1; N_2; E_2; \bot) \Rightarrow_{\mathrm{NO}} (N_1'; E_1'; N_2'; E_2'; \bot)$
if $N_1' = N_1 \cup E_1 \cup E_2$ and $N_2' = N_2 \cup E_1 \cup E_2$ are both $\mathcal{T}_i$-satisfiable, respectively, E_1' are all new variable equations derivable from N_1', E_2' are all new variable equations derivable from N_2' and $E_1' \cup E_2' \neq \emptyset$

Success $(N_1; E_1; N_2; E_2; \bot) \Rightarrow_{\mathrm{NO}} (N_1'; \emptyset; N_2'; \emptyset; \top)$
if $N_1' = N_1 \cup E_1 \cup E_2$ and $N_2' = N_2 \cup E_1 \cup E_2$ are both $\mathcal{T}_i$-satisfiable, respectively, E_1' are all new variable equations derivable from N_1', E_2' are all new variable equations derivable from N_2' and $E_1' \cup E_2' = \emptyset$

Fail $(N_1; E_1; N_2; E_2; \bot) \Rightarrow_{\mathrm{NO}} (N_1; E_1; N_2; E_2; \mathrm{fail})$
if $N_1' = N_1 \cup E_1 \cup E_2$ or $N_2' = N_2 \cup E_1 \cup E_2$ is $\mathcal{T}_i$-unsatisfiable, respectively

7.1.6 Definition (Arrangement)

Given a (finite) set of parameters X, an *arrangement* A over X is a (finite) set of equalities and inequalities over X such that for all $x_1, x_2 \in X$ either $x_1 \approx x_2 \in A$ or $x_1 \not\approx x_2 \in A$.

7.1.7 Proposition (Nelson-Oppen modulo Arrangement)

Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two theories satisfying the restrictions of Definition 7.1.3 except for restriction 2. Let ϕ be a conjunction of literals over $\Sigma_1 \cup \Sigma_2$. Let N_1 and N_2 be the purified literal sets out of ϕ. Then ϕ is satisfiable iff there is an arrangement A over $\mathrm{vars}(\phi)$ such that $N_1 \cup A$ is $\mathcal{T}_1$-satisfiable and $N_2 \cup A$ is $\mathcal{T}_2$-satisfiable.

7.1.8 Theorem (Nelson-Oppen is Sound, Complete and Terminating)

Let $\mathcal{T}_1, \mathcal{T}_2$ be two theories satisfying the Nelson-Oppen basic restrictions. Let ϕ be a conjunction of literals over $\Sigma_1 \cup \Sigma_2$ and N_1, N_2 be the result of purifying ϕ.
(i) All sequences $(N_1; \emptyset; N_2; \emptyset; \bot) \Rightarrow^*_{\text{NO}} \ldots$ are finite.
Let $(N_1; \emptyset; N_2; \emptyset; \bot) \Rightarrow^*_{\text{NO}} (N_1; E_1; N_2; E_2; s)$ be a derivation with finite state $(N_1; E_1; N_2; E_2; s)$,
(ii) If $s = \text{fail}$ then ϕ is unsatisfiable in $\mathcal{T}_1 \cup \mathcal{T}_2$.
(iii) If $s = \top$ then ϕ is satisfiable in $\mathcal{T}_1 \cup \mathcal{T}_2$.