Chapter 3

First-Order Logic

First-Order logic is a generalization of propositional logic. Propositional logic can represent propositions, whereas first-order logic can represent individuals and propositions about individuals. For example, in propositional logic from "Socrates is a man" and "If Socrates is a man then Socrates is mortal" the conclusion "Socrates is mortal" can be drawn. In first-order logic this can be represented much more fine-grained. From "Socrates is a man" and "All man are mortal" the conclusion "Socrates is mortal" can be drawn.

This chapter introduces first-order logic with equality. However, all calculi presented here, namely Tableaux (Section 3.6) and Superposition (Section **??**) are presented only for its restriction without equality. Purely equational logic and first-order logic with equality are presented separately in Chapter **??** and Chapter **??**, respectively.

3.1 Syntax

Definition 3.1.1 (Many-Sorted Signature)**.** A *many-sorted signature* $\Sigma = (\mathcal{S}, \Omega, \Pi)$ is a pair consisting of a finite non-empty set $\mathcal{S}$ of *sort symbols*, a non-empty set Ω of *operator symbols* (also called *function symbols*) over $\mathcal{S}$ and a set Π of *predicate symbols*. Every operator symbol $f \in \Omega$ has a unique sort declaration $f : S_1 \times \ldots \times S_n \to S$, indicating the sorts of arguments (also called *domain sorts*) and the *range sort* of f, respectively, for some $S_1, \ldots, S_n, S \in \mathcal{S}$ where $n \geq 0$ is called the *arity* of f, also denoted with arity(f). An operator symbol $f \in \Omega$ with arity 0 is called a *constant*. Every predicate symbol $P \in \Pi$ has a unique sort declaration $P \subseteq S_1 \times \ldots \times S_n$. A predicate symbol $P \in \Pi$ with arity 0 is called a *propositional variable*. For every sort $S \in \mathcal{S}$ there must be at least one constant $a \in \Omega$ with range sort S.

In addition to the signature Σ, a variable set $\mathcal{X}$, disjoint from Ω is assumed, so that for every sort $S \in \mathcal{S}$ there exists a countably infinite subset of $\mathcal{X}$ consisting of variables of the sort S. A variable x of sort S is denoted by x_S.

Definition 3.1.2 (Term)**.** Given a signature $\Sigma = (\mathcal{S}, \Omega, \Pi)$, a sort $S \in \mathcal{S}$ and

a variable set $\mathcal{X}$, the set $T_S(\Sigma, \mathcal{X})$ of all *terms* of sort S is recursively defined by (i) $x_S \in T_S(\Sigma, \mathcal{X})$ if $x_S \in \mathcal{X}$, (ii) $f(t_1, \ldots, t_n) \in T_S(\Sigma, \mathcal{X})$ if $f \in \Omega$ and $f : S_1 \times \ldots \times S_n \to S$ and $t_i \in T_{S_i}(\Sigma, \mathcal{X})$ for every $i \in \{1, \ldots, n\}$.

The sort of a term t is denoted by $\mathrm{sort}(t)$, i.e., if $t \in T_S(\Sigma, \mathcal{X})$ then $\mathrm{sort}(t) = S$. A term not containing a variable is called *ground*.

For the sake of simplicity it is often written: $T(\Sigma, \mathcal{X})$ for $\bigcup_{S \in \mathcal{S}} T_S(\Sigma, \mathcal{X})$, the set of all terms, $T_S(\Sigma)$ for the set of all ground terms of sort $S \in \mathcal{S}$, and $T(\Sigma)$ for $\bigcup_{S \in \mathcal{S}} T_S(\Sigma)$, the set of all ground terms over Σ.

Definition 3.1.3 (Equation, Atom, Literal)**.** If $s, t \in T_S(\Sigma, \mathcal{X})$ then $s \approx t$ is an *equation* over the signature Σ. Any equation is an *atom* (also called *atomic formula*) as well as every $P(t_1, \ldots, t_n)$ where $t_i \in T_{S_i}(\Sigma, \mathcal{X})$ for every $i \in \{1, \ldots, n\}$ and $P \in \Pi$, $\mathrm{arity}(P) = n$, $P \subseteq S_1 \times \ldots \times S_n$. An atom or its negation of an atom is called a *literal*.

The literal $s \stackrel{\cdot}{\approx} t$ denotes either $s \approx t$ or $t \approx s$. A literal is *positive* if it is an atom and *negative* otherwise. A negative equational literal $\neg(s \approx t)$ is written as $s \not\approx t$.

C Non equational atoms can be transformed into equations: For this a given signature is extended for every predicate symbol P as follows: (i) add a distinct sort B to $\mathcal{S}$, (ii) introduce a fresh constant true of the sort B to Ω, (iii) for every predicate P, $P \subseteq S_1 \times \ldots \times S_n$ add a fresh function $f_P : S_1, \ldots, S_n \to B$ to Ω, and (iv) encode every atom $P(t_1, \ldots, t_n)$ as a function $f_P : S_1, \ldots, S_n \to B$. Thus, predicate atoms are turned into equations $f_P(t_1, \ldots, t_n) \approx \mathrm{true}$. are overloaded here.

Definition 3.1.4 (Formulas)**.** The set $\mathrm{FOL}(\Sigma, \mathcal{X})$ of *many-sorted first-order formulas with equality* over the signature Σ is defined as follows for formulas $\phi, \psi \in F_\Sigma(\mathcal{X})$ and a variable $x \in \mathcal{X}$:

$\mathrm{FOL}(\Sigma, \mathcal{X})$	Comment
$\bot$	falsum
$\top$	verum
$P(t_1, \ldots, t_n), s \approx t$	atom
$(\neg\phi)$	negation
$(\phi \wedge \psi)$	conjunction
$(\phi \vee \psi)$	disjunction
$(\phi \to \psi)$	implication
$(\phi \leftrightarrow \psi)$	equivalence
$\forall x.\phi$	universal quantification
$\exists x.\phi$	existential quantification

A consequence of the above definition is that $\mathrm{PROP}(\Sigma) \subseteq \mathrm{FOL}(\Sigma', \mathcal{X})$ if the propositional variables of Σ are contained in Σ' as predicates of arity 0. A formula not containing a quantifier is called *quantifier-free*.

Definition 3.1.5 (Positions)**.** It follows from the definitions of terms and formulas that they have tree-like structure. For referring to a certain subtree, called subterm or subformula, respectively, sequences of natural numbers are used, called *positions* (as introduced in Chapter 2.1.3). The set of positions of a term, formula is inductively defined by:

$$\begin{aligned}
\mathrm{pos}(x) &:= \{\epsilon\} \text{ if } x \in \mathcal{X} \\
\mathrm{pos}(\phi) &:= \{\epsilon\} \text{ if } \phi \in \{\top, \bot\} \\
\mathrm{pos}(\neg\phi) &:= \{\epsilon\} \cup \{1p \mid p \in \mathrm{pos}(\phi)\} \\
\mathrm{pos}(\phi \circ \psi) &:= \{\epsilon\} \cup \{1p \mid p \in \mathrm{pos}(\phi)\} \cup \{2p \mid p \in \mathrm{pos}(\psi)\} \\
\mathrm{pos}(s \approx t) &:= \{\epsilon\} \cup \{1p \mid p \in \mathrm{pos}(s)\} \cup \{2p \mid p \in \mathrm{pos}(t)\} \\
\mathrm{pos}(f(t_1, \ldots, t_n)) &:= \{\epsilon\} \cup \textstyle\bigcup_{i=1}^{n} \{ip \mid p \in pos(t_i)\} \\
\mathrm{pos}(P(t_1, \ldots, t_n)) &:= \{\epsilon\} \cup \textstyle\bigcup_{i=1}^{n} \{ip \mid p \in pos(t_i)\} \\
\mathrm{pos}(\forall x.\phi) &:= \{\epsilon\} \cup \{1p \mid p \in \mathrm{pos}(\phi)\} \\
\mathrm{pos}(\exists x.\phi) &:= \{\epsilon\} \cup \{1p \mid p \in \mathrm{pos}(\phi)\}
\end{aligned}$$

where $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ and $t_i \in T(\Sigma, \mathcal{X})$ for all $i \in \{1, \ldots, n\}$.

The *prefix orders* (above, strictly above and parallel), the selection and replacement with respect to positions are defined exactly as in Chapter 2.1.3.

An term t (formula ϕ) is said to *contain* another term s (formula ψ) if $t_p = s$ ($\phi_p = \psi$). It is called a *strict subexpression* if $p \neq \epsilon$. The term t (formula ϕ) is called an *immediate subexpression* of s (formula ψ) if $|p| = 1$. For terms a subexpression is called a *subterm* and for formulas a *subformula*, respectively.

The *size* of a term t (formula ϕ), written $|t|$ ($|\phi|$), is the cardinality of $\mathrm{pos}(t)$, i.e., $|t| := |\,\mathrm{pos}(t)|$ ($|\phi| := |\,\mathrm{pos}(\phi)|$). The *depth* of a term, formula is the maximal length of a position in the term, formula: $\mathrm{depth}(t) := max\{|p| \mid p \in \mathrm{pos}(t)\}$ ($\mathrm{depth}(\phi) := max\{|p| \mid p \in \mathrm{pos}(\phi)\}$). The set of *all* variables occurring in a term t (formula ϕ) is denoted by $\mathrm{vars}(t)$ ($\mathrm{vars}(phi)$) and formally defined as $\mathrm{vars}(t) := \{x \in \mathcal{X} \mid x = t|_p, p \in \mathrm{pos}(t)\}$ ($\mathrm{vars}(\phi) := \{x \in \mathcal{X} \mid x = \phi|_p, p \in \mathrm{pos}(\phi)\}$). A term t (formula ϕ) is *ground* if $vars(t) = \emptyset$ ($vars(\phi) = \emptyset$).

Note that $\mathrm{vars}(\forall x.a \approx b) = \emptyset$ where a, b are constants. This is justified by the fact that the formula does not depend on the quantifier, see semantics below. The set of *free* variables of a formula ϕ (term t) is given by $\mathrm{fvars}(\phi, \emptyset)$ ($\mathrm{fvars}(t, \emptyset)$) and recursively defined by $\mathrm{fvars}(\psi_1 \circ \psi_2, B) := \mathrm{fvars}(\psi_1, B) \cup \mathrm{fvars}(\psi_2, B)$ where $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$, $\mathrm{fvars}(\forall x.\psi, B) := \mathrm{fvars}(\psi, B \cup \{x\})$, $\mathrm{fvars}(\exists x.\psi, B) := \mathrm{fvars}(\psi, B \cup \{x\})$, $\mathrm{fvars}(\neg\psi, B) := \mathrm{fvars}(\psi, B)$, $\mathrm{fvars}(L, B) := \mathrm{vars}(\psi) \setminus B$ ($\mathrm{fvars}(t, B) := \mathrm{vars}(t) \setminus B$. For $\mathrm{fvars}(\phi, \emptyset)$ I also write $\mathrm{fvars}(\phi)$

In $\forall x.\phi$ ($\exists x.\phi$) the formula ϕ is called the *scope* of the quantifier. An occurrence q of a variable x in a formula ϕ ($\phi|_q = x$) is called *bound* if there is some $p < q$ with $\phi|_p = \forall x.\phi'$ or $\phi|_p = \exists x.\phi'$. Any other occurrence of a variable is called *free*. A formula not containing a free occurrence of a variable is called *closed*. If $\{x_1, \ldots, x_n\}$ are the variables freely occurring in a formula ϕ then $\forall x_1, \ldots, x_n.\phi$ and $\exists x_1, \ldots, x_n.\phi$ (abbreviations for $\forall x_1.\forall x_2 \ldots \forall x_n.\phi$, $\exists x_1.\forall x_2 \ldots \forall x_n.\phi$, respectively) are the *universal* and the *existential closure* of ϕ.

Example 3.1.6. For the literal $\neg P(f(x, g(a)))$ the atom $P(f(x, g(a)))$ is an immediate subformula of occurring at position 1. The terms x and $g(a)$ are strict subterms occurring at positions 111 and 112, respectively. The formula $\neg P(f(x, g(a)))[b]_{111} = \neg P(f(b, g(a)))$ is obtained by replacing x with b. $\text{pos}(\neg P(f(x, g(a)))) = \{\epsilon, 1, 11, 111, 112, 1121\}$ meaning its size is 6, its depth 4 and $vars(\neg P(f(x, g(a)))) = \{x\}$.

The *polarity* of a subformula $\psi = \phi|_p$ at position p is $pol(\phi, p)$ where pol is recursively defined by

$$\begin{aligned}
\text{pol}(\phi, \epsilon) &:= 1 \\
\text{pol}(\neg\phi, 1p) &:= -\,\text{pol}(\phi, p) \\
\text{pol}(\phi_1 \circ \phi_2, ip) &:= \text{pol}(\phi_i, p) \text{ if } \circ \in \{\wedge, \vee\} \\
\text{pol}(\phi_1 \to \phi_2, 1p) &:= -\,\text{pol}(\phi_1, p) \\
\text{pol}(\phi_1 \to \phi_2, 2p) &:= \text{pol}(\phi_2, p) \\
\text{pol}(\phi_1 \leftrightarrow \phi_2, ip) &:= 0 \\
\text{pol}(P(t_1, \ldots, t_n), p) &:= 1 \\
\text{pol}(t \approx s, p) &:= 1 \\
\text{pol}(\forall x.\phi, 1p) &:= \text{pol}(\phi, p) \\
\text{pol}(\exists x.\phi, 1p) &:= \text{pol}(\phi, p)
\end{aligned}$$

3.2 Semantics

Definition 3.2.1 (Σ-algebra)**.** Let $\Sigma = (\mathcal{S}, \Omega, \Pi)$ be a signature with set of sorts $\mathcal{S}$, operator set Ω and predicate set Π. A Σ-*algebra* $\mathcal{A}$, also called Σ-*interpretation*, is a mapping that assigns (i) a non-empty carrier set $S^{\mathcal{A}}$ to every sort $S \in \mathcal{S}$, so that $(S_1)^{\mathcal{A}} \cap (S_2)^{\mathcal{A}} = \emptyset$ for any distinct sorts $S_1, S_2 \in \mathcal{S}$, (ii) a total function $f^{\mathcal{A}} : (S_1)^{\mathcal{A}} \times \ldots \times (S_n)^{\mathcal{A}} \to (S)^{\mathcal{A}}$ to every operator $f \in \Omega$, $\text{arity}(f) = n$ where $f : S_1 \times \ldots \times S_n \to S$, (iii) a relation $P^{\mathcal{A}} \subseteq ((S_1)^{\mathcal{A}} \times \ldots \times (S_m)^{\mathcal{A}})$ to every predicate symbol $P \in \Pi$, $\text{arity}(P) = m$. (iv) the equality relation becomes $\approx^{\mathcal{A}} = \{(e, e) \mid e \in \mathcal{U}^{\mathcal{A}}\}$ where the set $\mathcal{U}^{\mathcal{A}} := \bigcup_{S \in \mathcal{S}} (S)^{\mathcal{A}}$ is called the *universe* of $\mathcal{A}$.

A (variable) *assignment*, also called a *valuation* for an algebra $\mathcal{A}$ is a function $\beta : \mathcal{X} \to \mathcal{U}_{\mathcal{A}}$ so that $\beta(x) \in S_{\mathcal{A}}$ for every variable $x \in \mathcal{X}$, where $S = \text{sort}(x)$. A *modification* $\beta[x \mapsto e]$ of an assignment β at a variable $x \in \mathcal{X}$, where $e \in S_{\mathcal{A}}$ and $S = \text{sort}(x)$, is the assignment defined as follows:

$$\beta[x \mapsto e](y) = \begin{cases} e & \text{if } x = y \\ \beta(y) & \text{otherwise.} \end{cases}$$

Informally speaking, the assignment $\beta[x \mapsto e]$ is identical to β for every variable except x, which is mapped by $\beta[x \mapsto e]$ to e.

The homomorphic extension $\mathcal{A}(\beta)$ of β onto terms is a mapping $T(\Sigma, \mathcal{X}) \to \mathcal{U}_{\mathcal{A}}$ defined as (i) $\mathcal{A}(\beta)(x) = \beta(x)$, where $x \in \mathcal{X}$ and (ii) $\mathcal{A}(\beta)(f(t_1, \ldots, t_n)) = f_{\mathcal{A}}(\mathcal{A}(\beta)(t_1), \ldots, \mathcal{A}(\beta)(t_n))$, where $f \in \Omega$, $\text{arity}(f) = n$.

Given a term $t \in T(\Sigma, \mathcal{X})$, the value $\mathcal{A}(\beta)(t)$ is called the *interpretation* of t under $\mathcal{A}$ and β. If the term t is ground, the value $\mathcal{A}(\beta)(t)$ does not depend on a particular choice of β, for which reason the interpretation of t under $\mathcal{A}$ is denoted by $\mathcal{A}(t)$.

An algebra $\mathcal{A}$ is called *term-generated*, if every element e of the universe $\mathcal{U}_\mathcal{A}$ of $\mathcal{A}$ is the image of some ground term t, i.e., $\mathcal{A}(t) = e$.

Definition 3.2.2 (Semantics)**.** An algebra $\mathcal{A}$ and an assignment β are extended to formulas $\phi \in \mathrm{FOL}(\Sigma, \mathcal{X})$ by

$$
\begin{array}{rcl}
\mathcal{A}(\beta)(\bot) & := & 0 \\
\mathcal{A}(\beta)(\top) & := & 1 \\
\mathcal{A}(\beta)(s \approx t) & := & 1 \text{ if } \mathcal{A}(\beta)(s) = \mathcal{A}(\beta)(t) \text{ and } 0 \text{ otherwise} \\
\mathcal{A}(\beta)(P(t_1, \ldots, t_n)) & := & 1 \text{ if } (\mathcal{A}(\beta)(t_1), \ldots, \mathcal{A}(\beta)(t_n)) \in P_\mathcal{A} \text{ and } 0 \text{ otherwise} \\
\mathcal{A}(\beta)(\neg\phi) & := & 1 - \mathcal{A}(\beta)(\phi) \\
\mathcal{A}(\beta)(\phi \wedge \psi) & := & \min(\{\mathcal{A}(\beta)(\phi), \mathcal{A}(\beta)(\psi)\}) \\
\mathcal{A}(\beta)(\phi \vee \psi) & := & \max(\{\mathcal{A}(\beta)(\phi), \mathcal{A}(\beta)(\psi)\}) \\
\mathcal{A}(\beta)(\phi \to \psi) & := & \max(\{(1 - \mathcal{A}(\beta)(\phi)), \mathcal{A}(\beta)(\psi)\}) \\
\mathcal{A}(\beta)(\phi \leftrightarrow \psi) & := & \text{if } \mathcal{A}(\beta)(\phi) = \mathcal{A}(\beta)(\psi) \text{ then 1 else 0} \\
\mathcal{A}(\beta)(\exists x_S.\phi) & := & 1 \text{ if } \mathcal{A}(\beta[x \mapsto e])(\phi) = 1 \text{ for some } e \in S_\mathcal{A} \text{ and } 0 \text{ otherwise} \\
\mathcal{A}(\beta)(\forall x_S.\phi) & := & 1 \text{ if } \mathcal{A}(\beta[x \mapsto e])(\phi) = 1 \text{ for all } e \in S_\mathcal{A} \text{ and } 0 \text{ otherwise}
\end{array}
$$

A formula ϕ is called *satisfiable by* $\mathcal{A}$ *under* β (or *valid in* $\mathcal{A}$ *under* β) if $\mathcal{A}, \beta \models \phi$; in this case, ϕ is also called *consistent*; *satisfiable by* $\mathcal{A}$ if $\mathcal{A}, \beta \models \phi$ for some assignment β; *satisfiable* if $\mathcal{A}, \beta \models \phi$ for some algebra $\mathcal{A}$ and some assignment β; *valid in* $\mathcal{A}$, written $\mathcal{A} \models \phi$, if $\mathcal{A}, \beta \models \phi$ for any assignment β; in this case, $\mathcal{A}$ is called a *model* of ϕ; *valid*, written $\models \phi$, if $\mathcal{A}, \beta \models \phi$ for any algebra $\mathcal{A}$ and any assignment β; in this case, ϕ is also called a *tautology*; *unsatisfiable* if $\mathcal{A}, \beta \not\models \phi$ for any algebra $\mathcal{A}$ and any assignment β; in this case ϕ is also called *inconsistent*.

Note that $\bot$ is *inconsistent* whereas $\top$ is valid. If ϕ is a sentence that is a formula not containing a free variable, it is valid in $\mathcal{A}$ if and only if it is satisfiable by $\mathcal{A}$. This means the truth of a sentence does not depend on the choice of an assignment.

Given two formulas ϕ and ψ, ϕ *entails* ψ, or ψ is a *consequence* of ϕ, written $\phi \models \psi$, if for any algebra $\mathcal{A}$ and assignment β, if $\mathcal{A}, \beta \models \phi$ then $\mathcal{A}, \beta \models \psi$. The formulas ϕ and ψ are called *equivalent*, written $\phi \models\models \psi$, if $\phi \models \psi$ and $\psi \models \phi$. Two formulas ϕ and ψ are called *equisatisfiable*, if ϕ is satisfiable iff ψ is satisfiable (not necessarily in the same models). Note that if ϕ and ψ are equivalent then they are equisatisfiable, but not the other way around. The notions of "entailment", "equivalence" and "equisatisfiability" are naturally extended to sets of formulas, that are treated as conjunctions of single formulas. Thus, given formula sets M_1 and M_2, the set M_1 entails M_2, written $M_1 \models M_2$, if for any algebra $\mathcal{A}$ and assignment β, if $\mathcal{A}, \beta \models \phi$ for every $\phi \in M_1$ then $\mathcal{A}, \beta \models \psi$ for every $\psi \in M_2$. The sets M_1 and M_2 are equivalent, written $M_1 \models\models M_2$, if $M_1 \models M_2$ and $M_2 \models M_1$. Given an arbitrary formula ϕ and formula set M, $M \models \phi$ is written to denote $M \models \{\phi\}$; analogously, $\phi \models M$ stands for $\{\phi\} \models M$.

Since clauses are implicitly universally quantified disjunctions of literals, a clause C is satisfiable by an algebra $\mathcal{A}$ if for every assignment β there is a literal $L \in C$ with $\mathcal{A}, \beta \models L$. Note that if $C = \{L_1, \ldots, L_k\}$ is a ground clause, i.e., every L_i is a ground literal, then $\mathcal{A} \models C$ if and only if there is a literal L_j in C so that $\mathcal{A} \models L_j$. A clause set N is satisfiable iff all clauses $C \in N$ are satisfiable by the same algebra $\mathcal{A}$. Accordingly, if N and M are two clause sets, $N \models M$ iff every model $\mathcal{A}$ of N is also a model of M.

3.3 Equality

The equality predicate is build into the first-order language in Section 3.1 and not part of the signature. It is a first class citizen. This is the case although it can be actually axiomatized in the language. The motivation is that firstly, many real world problems naturally contain equations. They are a means to define functions. Then predicates over terms model properties of the functions. Secondly, without special treatment in a calculus, it is almost impossible to automatically prove non-trivial properties of a formula containing equations.

In this section I firstly show that any formula can be transformed into a formula where all atoms are equations. Secondly, that any formula containing equations can be transformed into a formula where the equality predicate is replaced by a fresh predicate together with some axioms. In the first case the respective clause sets are equivalent, in the second case the transformation is satisfiability preserving. For the replacement of any predicate R by equations over a fresh function f_R we assume an additional fresh sort Bool with two fresh constants true and false.

InjEq $\chi[R(t_{1,1}, \ldots, t_{1,n})]_{p_1} \ldots [R(t_{m,1}, \ldots, t_{m,n})]_{p_m} \Rightarrow_{\mathrm{IE}} \chi[f_R(t_{1,1}, \ldots, t_{1,n}) \approx \mathrm{true}]_{p_1} \ldots [f_R(t_{m,1}, \ldots, t_{m,n}) \approx \mathrm{true}]_{p_m}$

provided R is a predicate occurring in χ, $\{p_1, \ldots, p_m\}$ are all positions of atoms with predicate R in χ and f_R is new with appropriate sorting

Proposition 3.3.1. Let $\chi \Rightarrow_{\mathrm{IE}}^* \chi'$ then χ is satisfiable (valid) iff χ' is satisfiable (valid).

Proof. (Sketch) The basic proof idea is to establish the relation $(t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) \in R^{\mathcal{A}}$ iff $f_R^{\mathcal{A}}(t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) = \mathrm{true}^{\mathcal{A}}$. Furthermore, the sort of true is fresh to χ and the equations $f_R(t_1, \ldots, t_n) \approx \mathrm{true}$ do not interfere with any term t_i because the f_R are all fresh and only occur on top level of the equations. □

When removing equality from a formula it needs to be axiomatized. For simplicity, I assume here that the considered formula χ is one-sorted, i.e., there is only one sort occurring for functions, relations in χ. The extension to formulas with many sorts is straightforward and discussed below.

RemEq $\chi[l_1 \approx r_1]_{p_1} \ldots [l_m \approx r_m]_{p_m} \Rightarrow_{\mathrm{RE}} \chi[E(l_1, r_1)]_{p_1} \ldots [E(l_m, r_m)]_{p_m} \wedge \mathrm{def}(\chi, E)$

provided $\{p_1, \ldots, p_m\}$ are all positions of equations $l_i = r_i$ in χ and E is a new binary predicate

The formula $\mathrm{def}(\chi, E)$ is the axiomatization of equality for χ and it consists of a conjunction of the equivalence relation axioms for E

$\forall x.E(x,x)$
$\forall x,y.(E(x,y) \rightarrow E(y,x))$
$\forall x,y,z.((E(x,y) \wedge E(x,z)) \rightarrow E(x,z))$

plus the congruence axioms for E for every n-ary function symbol f

$\forall x_1, y_1, \ldots, x_n, y_n.((E(x_1,y_1) \wedge \ldots \wedge E(x_n,y_n)) \rightarrow E(f(x_1,\ldots,x_n), f(y_1,\ldots,y_n)))$

plus the congruence axioms for E for every m-ary predicate symbol P

$\forall x_1, y_1, \ldots, x_m, y_m.((E(x_1,y_1) \wedge \ldots \wedge E(x_m,y_m) \wedge P(x_1,\ldots,x_m)) \rightarrow P(y_1,\ldots,y_m)$

Proposition 3.3.2. Let $\chi \Rightarrow_{\mathrm{RE}} \chi'$ then χ is satisfiable iff χ' is satisfiable.

Proof. (Sketch) The identity on an algebra (see Definition 3.2.2) is a congruence relation proving the direction from left to right. The direction from right to left is more involved. □

Note that $\Rightarrow_{\mathrm{RE}}$ is not validity preserving. Consider the simple example formula $a \approx a$ which is valid for any constant a. Its translation $E(a,a) \wedge \mathrm{def}(a \approx a, E)$ is not valid, e.g., consider an algebra with $E^{\mathcal{A}} = \emptyset$.

Now in case χ has many different sorts then for each sort S one new fresh predicate E_S is needed for the translation. For each of these predicates equivalence relation and congruence axioms need to be generated where for every function f only one axiom using E_S is needed, where S is the range sort of S. Similar for the domain sorts of f and accordingly for predicates.

3.4 Substitution and Unifier

Definition 3.4.1 (Substitution)**.** A *substitution* is a mapping $\sigma : \mathcal{X} \rightarrow T(\Sigma, \mathcal{X})$ so that

1. $\sigma(x) \neq x$ for only finitely many variables x and
2. $sort(x) = sort(t)$ for every variable $x \in \mathcal{X}$ that is mapped to a term $t \in T_S(\Sigma, \mathcal{X})$.

The application $\sigma(x)$ of a substitution σ to a variable x is often written in postfix notation as $x\sigma$. The variable set $\mathrm{dom}(\sigma) := \{x \in \mathcal{X} \mid x\sigma \neq x\}$ is called the *domain* of σ. The term set $\mathrm{codom}(\sigma) := \{x\sigma \mid x \in \mathrm{dom}(\sigma)\}$ is called the *codomain* of σ. From the above definition of substitution it follows that $\mathrm{dom}(\sigma)$ is finite for any substitution σ. The composition of two substitutions σ and τ is written as a juxtaposition $\sigma\tau$, i.e., $t\sigma\tau = (t\sigma)\tau$. A substitution σ is called *idempotent* if $\sigma\sigma = \sigma$. σ is idempotent iff $\mathrm{dom}(\sigma) \cap \mathrm{vars}(\mathrm{codom}(\sigma)) = \emptyset$.

Substitutions are often written as $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ if $dom(\sigma) = \{x_1, \ldots, x_n\}$ and $x_i\sigma = t_i$ for every $i \in \{1, \ldots, n\}$. The *modification*of a substitution σ at a variable x is defined as follows:

$$\sigma[x \mapsto t](y) = \begin{cases} t & \text{if } y = x \\ \sigma(y) & \text{otherwise} \end{cases}$$

A substitution σ is identified with its extension to expression and defined as following:

1. $\bot\sigma = \bot$,
2. $\top\sigma = \top$,
3. $(f(t_1, \ldots, t_n))\sigma = f(t_1\sigma, \ldots, t_n\sigma)$,
4. $(P(t_1, \ldots, t_n))\sigma = P(t_1\sigma, \ldots, t_n\sigma)$,
5. $(s \approx t)\sigma = (s\sigma \approx t\sigma)$,
6. $(\neg\phi)\sigma = \neg(\phi\sigma)$,
7. $(\phi \circ \psi)\sigma = \phi\sigma \circ \psi\sigma$ where $\circ \in \{\vee, \wedge\}$,
8. $(Qx\phi)\sigma = Qz(\phi\sigma[x \mapsto z])$ where $Q \in \{\forall, \exists\}$, z and x are of the same sort and z is a fresh variable.

The result $e\sigma$ of applying a substitution σ to an expression e is called an *instance* of e. The substitution σ is called *ground* if it maps every domain variable to a ground term. If the application of a substitution σ to an expression e produces a ground expression $e\sigma$ then $e\sigma$ is called *ground instance* of e. A ground substitution σ is called *grounding for an expression* e if $e\sigma$ is ground. A substitution σ is called *variable renaming* if $im(\sigma) \subseteq \mathcal{X}$ and for any $x, y \in \mathcal{X}$, if $x \neq y$ then $x\sigma \neq y\sigma$.

Definition 3.4.2 (Unifier)**.** Two terms s and t are said to be *unifiable* if there exists a substitution σ so that $s\sigma = t\sigma$, the substitution σ is then called a *unifier* of s and t. The unifier σ is called *most general unifier*, written $\sigma = mgu(s, t)$, if any other unifier τ of s and t can be represented as $\tau = \sigma\tau'$, for some substitution τ'.

3.5 Unification Calculi

The first calculus is the naive standard unification calculus that is typically found in the (old) literature on automated reasoning. A state of the naive standard unification calculus is a set of equations E or $\bot$, where $\bot$ denotes that no unifier exists. The set E is also called a *unification problem*. The start state for checking whether two terms s, t with $\text{sort}(s) = \text{sort}(t)$ (or atoms A, B) are unifiable is the set $E = \{s = t\}$. A variable x is solved in E if $E = \{x = t\} \uplus E'$, $x \notin \text{vars}(t)$ and $x \notin \text{vars}(E)$.

Tautology $\quad E \uplus \{t = t\} \;\Rightarrow_{\text{SU}}\; E$

Decomposition $E \uplus \{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)\} \Rightarrow_{\mathrm{SU}} E \cup \{s_1 = t_1, \ldots, s_n = t_n\}$

Clash $E \uplus \{f(s_1, \ldots, s_n) = g(s_1, \ldots, s_m)\} \Rightarrow_{\mathrm{SU}} \bot$
if $f \neq g$

Substitution $E \uplus \{x = t\} \Rightarrow_{\mathrm{SU}} E\{x \mapsto t\} \cup \{x = t\}$
if $x \in vars(E)$ and $x \notin vars(t)$

Occurs Check $E \uplus \{x = t\} \Rightarrow_{\mathrm{SU}} \bot$
if $x \neq t$ and $x \in vars(t)$

Orient $E \uplus \{t = x\} \Rightarrow_{\mathrm{SU}} E \cup \{x = t\}$
if $t \notin \mathcal{X}$

Theorem 3.5.1 (Soundness, Completeness and Termination of $\Rightarrow_{\mathrm{SU}}$)**.** If s, t are two terms with $\mathrm{sort}(s) = \mathrm{sort}(t)$ then

1. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} E$ then any equation $(s' = t') \in E$ is well-sorted, i.e., $\mathrm{sort}(s') = \mathrm{sort}(t')$.
2. $\Rightarrow_{\mathrm{SU}}$ terminates on $\{s = t\}$.
3. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} E$ then σ is a unifier (mgu) of E iff σ is a unifier (mgu) of $\{s = t\}$.
4. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} \bot$ then s and t are not unifiable.
5. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} \{x_1 = t_1, \ldots, x_n = t_n\}$ and this is a normal form, then $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ is an mgu of s, t.

Proof. 1. by induction on the length of the derivation and a case analysis for the different rules.
2. for a state $E = \{s_1 = t_1, \ldots, s_n = t_n\}$ take the measure $\mu(E) := (n, M, k)$ where n is the number of unsolved variables, M the multiset of all term depths of the s_i, t_i and k the number of equations $t = x$ in E where t is not a variable. The state $\bot$ is mapped to $(0, \emptyset, 0)$. Then the lexicographic combination of $>$ on the naturals and its multiset extension shows that any rule application decrements the measure.
3. by induction on the length of the derivation and a case analysis for the different rules. Clearly, for any state where Clash, or Occurs Check generate $\bot$ the respective equation is not unifiable.
4. a direct consequence of 3.
5. if $E = \{x_1 = t_1, \ldots, x_n = t_n\}$ is a normal form, then for all $x_i = t_i$ we have $x_i \notin \mathrm{vars}(t_i)$ and $x_i \notin \mathrm{vars}(E \setminus \{x_i = t_i\})$, so $\{x_1 = t_1, \ldots, x_n = t_n\}\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\} = \{t_1 = t_1, \ldots, t_n = t_n\}$ and hence $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ is an mgu of $\{x_1 = t_1, \ldots, x_n = t_n\}$. By 3. it is also an mgu of s, t. □

Example 3.5.2 (Size of Standard Unification Problems)**.** Any normal form of the unification problem E given by

$\{f(x_1, g(x_1, x_1), x_3, \ldots, g(x_n, x_n)) = f(g(x_0, x_0), x_2, g(x_2, x_2), \ldots, x_{n+1})\}$

with respect to $\Rightarrow_{\mathrm{SU}}$ is exponentially larger than E.

The second calculus, polynomial unification, prevents the problem of exponential growth by introducing an implicit representation for the mgu. For this calculus the size of a normal form is always polynomial in the size of the input unification problem.

Tautology $E \uplus \{t = t\} \Rightarrow_{\mathrm{PU}} E$

Decomposition $E \uplus \{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)\} \Rightarrow_{\mathrm{PU}} E \uplus \{s_1 = t_1, \ldots, s_n = t_n\}$

Clash $E \uplus \{f(t_1, \ldots, t_n) = g(s_1, \ldots, s_m)\} \Rightarrow_{\mathrm{PU}} \bot$
if $f \neq g$

Occurs Check $E \uplus \{x = t\} \Rightarrow_{\mathrm{PU}} \bot$
if $x \neq t$ and $x \in vars(t)$

Orientation $E \uplus \{t = x\} \Rightarrow_{\mathrm{PU}} E \uplus \{x = t\}$
if $t \notin \mathcal{X}$

Substitution $E \uplus \{x = y\} \Rightarrow_{\mathrm{PU}} E\{x \mapsto y\} \uplus \{x = y\}$
if $x \in vars(E)$ and $x \neq y$

Cycle $E \uplus \{x_1 = t_1, \ldots, x_n = t_n\} \Rightarrow_{\mathrm{PU}} \bot$
if there are positions p_i with $t_i|_{p_i} = x_{i+1}, t_n|_{p_n} = x_1$ and some $p_i \neq \epsilon$

Merge $E \uplus \{x = t, x = s\} \Rightarrow_{\mathrm{PU}} E \uplus \{x = t, t = s\}$
if $t, s \notin \mathcal{X}$ and $|t| \leq |s|$

Theorem 3.5.3 (Soundness, Completeness and Termination of $\Rightarrow_{\mathrm{PU}}$)**.** If s, t are two terms with $\mathrm{sort}(s) = \mathrm{sort}(t)$ then

1. if $\{s = t\} \Rightarrow^*_{\mathrm{PU}} E$ then any equation $(s' = t') \in E$ is well-sorted, i.e., $\mathrm{sort}(s') = \mathrm{sort}(t')$.
2. $\Rightarrow_{\mathrm{PU}}$ terminates on $\{s = t\}$.
3. if $\{s = t\} \Rightarrow^*_{\mathrm{PU}} E$ then σ is a unifier (mgu) of E iff σ is a unifier (mgu) of $\{s = t\}$.
4. if $\{s = t\} \Rightarrow^*_{\mathrm{PU}} \bot$ then s and t are not unifiable.

Theorem 3.5.4 (Unifier generated by $\Rightarrow_{\mathrm{PU}}$)**.** Let $\{s = t\} \Rightarrow^*_{\mathrm{PU}} \{x_1 = t_1, \ldots, x_n = t_n\}$. Then

γ	Descendant $\gamma(t)$
$\forall x_S.\psi$	$\psi\{x_S \mapsto t\}$
$\neg\exists x_S.\psi$	$\neg\psi\{x_S \mapsto t\}$
	for any ground term $t \in T_S(\Sigma)$

δ	Descendant $\delta(c)$
$\exists x_S.\psi$	$\psi\{x_S \mapsto c\}$
$\neg\forall x_S.\psi$	$\neg\psi\{x_S \mapsto c\}$
	for some fresh Skolem constant $c \in T_S(\Sigma)$

Figure 3.1: γ- and δ-Formulas

1. $x_i \neq x_j$ for all $i \neq j$ and without loss of generality $x_i \notin \mathrm{vars}(t_{i+k})$ for all i, k, $1 \leq i < n$, $i + k \leq n$.
2. the substitution $\{x_1 \mapsto t_1\}\{x_2 \mapsto t_2\}\ldots\{x_n \mapsto t_n\}$ is an mgu of $s = t$.

Proof. 1. If $x_i = x_j$ for some $i \neq j$ then Merge is applicable. If $x_i \in \mathrm{vars}(t_i)$ for some i then Occurs Check is applicable. If the x_i cannot be ordered in the described way, then either Substitution or Cycle is applicable.
2. Since $x_i \notin \mathrm{vars}(t_{i+k}$ the composition yields the mgu. □

3.6 First-Order Tableaux

The different versions of tableaux for first-order logic differ in particular in the treatment of variables by the tableaux rules. The first variant is standard first-order tableaux where variables are instantiated by ground terms.

Definition 3.6.1 (γ-,δ-Formulas)**.** A formula ϕ is called a γ-formula if ϕ is a formula $\forall x_S.\psi$ or $\neg\exists x_S.\psi$. A formula ϕ is called a δ-formula if ϕ is a formula $\exists x_S.\psi$ or $\neg\forall x_S.\psi$.

Definition 3.6.2 (Direct Standard Tableaux Descendant)**.** Given a γ- or δ-formula ϕ, Figure 3.1 shows its direct descendants.

For the standard first-order tableaux rules to make sense "enough" Skolem constants are needed in the signature, e.g., countably infinitely many for each sort. A δ formula ϕ occurring in some sequence is called *open* if no direct descendant of it is part of the sequence. In general, the number of γ descendants cannot be limited for a successful tableaux proof.

γ-Expansion $\quad N \uplus \{(\phi_1, \ldots, \psi, \ldots, \phi_n)\} \Rightarrow_{\mathrm{FT}} N \uplus \{(\phi_1, \ldots, \psi, \ldots, \phi_n, \psi')\}$
provided ψ is a γ-formula, ψ' a $\gamma(t)$ descendant where t is an arbitrary ground term in the signature of the sequence (branch) and the sequence is not closed.

δ-Expansion $\quad N \uplus \{(\phi_1, \ldots, \psi, \ldots, \phi_n)\} \Rightarrow_{\mathrm{FT}} N \uplus \{(\phi_1, \ldots, \psi, \ldots, \phi_n, \psi')\}$

provided ψ is an open δ-formula, ψ' a $\delta(c)$ descendant where c is fresh to the sequence and the sequence is not closed.

The standard first-order tableaux calculus consists of the rules α-, and β-expansion (see Section 2.4) and the above two rules γ-Expansion and δ-Expansion.

Theorem 3.6.3 (Standard First-Order Tableaux is Sound and Complete)**.** A formula ϕ (without equality) is valid iff standard tableaux computes a closed state out of $\{(\neg\phi)\}$.

Skolem *constants* are sufficient: In a δ-formula $\exists x\,\phi$, $\exists$ is the outermost quantifier and x is the only free variable in ϕ. The γ rule has to be applied several times to the same formula for tableaux to be complete. For instance, constructing a closed tableau for

$$\{\forall x\,(P(x) \to P(f(x))),\ P(b),\ \neg P(f(f(b)))\}$$

is impossible without applying γ-expansion twice on one path.

The main disadvantage of standard first-order tableau is that the γ ground term instances need to be guessed. The whole complexity of the problem lies in this guessing as for otherwise tableaux terminates. A natural idea is to guess ground terms that can eventually be used to close a branch. This is the idea of free-variable first-order tableaux. Instead of guessing a ground term for a γ formula the variable remains, the instantiation is delayed until a branch is closed for two literals via unification. As a consequence, for δ formulas no longer constants are introduced but Skolem terms in the formerly universally quantified variables that had the δ formula in their scope.

The new calculus suggests to keep track of scopes of variables, so I move from a state as a set of sequences of formulas to a set of sequences of pairs $l_i = (\phi_i, X_i)$ where X_i is a set of variables.

Definition 3.6.4 (Direct Free-Variable Tableaux Descendant)**.** Given a γ- or δ-formula ϕ, Figure 3.2 shows its direct descendants.

γ-Expansion $N \uplus \{(l_1, \ldots, (\psi, X), \ldots, l_n)\} \Rightarrow_{\mathrm{FT}} N \uplus \{(l_1, \ldots, (\psi, X), \ldots, l_n, (\psi', X \cup \{y\}))\}$
provided ψ is a γ-formula, ψ' a $\gamma(y)$ descendant where y is fresh to the sequence (branch) and the sequence is not closed.

δ-Expansion $N \uplus \{(l_1, \ldots, (\psi, X), \ldots, l_n)\} \Rightarrow_{\mathrm{FT}} N \uplus \{(l_1, \ldots, (\psi, X), \ldots, l_n, (\psi', X))\}$
provided ψ is an open δ-formula, ψ' a $\delta(f(y_1, \ldots, y_n))$ descendant where f is fresh to the sequence, $X = \{y_1, \ldots, y_n\}$ and the sequence is not closed.

Branch-Closing $N \uplus \{(l_1, \ldots, (L, X), \ldots, (K, X'), \ldots, l_n)\} \Rightarrow_{\mathrm{FT}} N\sigma \uplus \{(\phi_1, \ldots, (L, X), \ldots, (K, X'), \ldots, \phi_n, \}\sigma$

γ	Descendant $\gamma(y)$
$\forall x_S.\psi$	$\psi\{x_S \mapsto y\}$
$\neg\exists x_S.\psi$	$\neg\psi\{x_S \mapsto y\}$
	for a fresh variable $y, \mathrm{sort}(y) = S$

δ	Descendant $\delta(f(y_1, \ldots, y_n))$
$\exists x_S.\psi$	$\psi\{x_S \mapsto f(y_1, \ldots, y_n)\}$
$\neg\forall x_S.\psi$	$\neg\psi\{x_S \mapsto f(y_1, \ldots, y_n)\}$
	for some fresh Skolem function f
	where $f(y_1, \ldots, y_n) \in T_S(\Sigma)$

Figure 3.2: γ- and δ-Formulas

provided K and L are literals and there is an mgu σ such that $K\sigma = \neg L\sigma$ and the sequence is not closed.

The standard first-order tableaux calculus consists of the rules α-, and β-expansion (see Section 2.4) which are adapted to pairs and the above three rules γ-Expansion, δ-Expansion and Branch-Closing.

Theorem 3.6.5 (Free-variable First-Order Tableaux is Sound and Complete)**.** A formula ϕ (without equality) is valid iff free-variable tableaux computes a closed state out of $\{(\neg\phi)\}$.

Example 3.6.6.

1.	$\neg[\exists w \forall x R(x, w, f(x, w)) \to \exists w \forall x \exists y R(x, w, y)]$	
2.	$\exists w \forall x\ R(x, w, f(x, w))$	1_1 $[\alpha]$
3.	$\neg\exists w \forall x \exists y\ R(x, w, y)$	1_2 $[\alpha]$
4.	$\forall x\ R(x, c, f(x, c))$	$2(c)$ $[\delta]$
5.	$\neg\forall x \exists y\ R(x, v_1, y)$	$3(v_1)$ $[\gamma]$
6.	$\neg\exists y\ R(g(v_1), v_1, y)$	$5(g(v_1))$ $[\delta]$
7.	$R(v_2, c, f(v_2, c))$	$4(v_2)$ $[\gamma]$
8.	$\neg R(g(v_1), v_1, v_3)$	$6(v_3)$ $[\gamma]$

7. and 8. are complementary (modulo unification):

$$v_2 = g(v_1),\ c = v_1,\ f(v_2, c) = v_3$$

is solvable with an mgu $\sigma = \{v_1 \mapsto c, v_2 \mapsto g(c), v_3 \mapsto f(g(c), c)\}$, and hence, $T\sigma$ is a closed (linear) tableau for the formula in 1.

Problem: Strictness for γ is still incomplete. For instance, constructing a closed tableau for

$$\{\forall x\,(P(x) \to P(f(x))),\ P(b),\ \neg P(f(f(b)))\}$$

is impossible without applying γ-expansion twice on one path.

Semantic Tableau vs. Resolution

1. Tableau: global, goal-oriented, "backward".
2. Resolution: local, "forward".
3. Goal-orientation is a clear advantage if only a small subset of a large set of formulas is necessary for a proof. (Note that resolution provers saturate also those parts of the clause set that are irrelevant for proving the goal.)
4. Resolution can be combined with more powerful redundancy elimination methods; because of its global nature this is more difficult for the tableau method.
5. Resolution can be refined to work well with equality; for tableau this seems to be impossible.
6. On the other hand tableau calculi can be easily extended to other logics; in particular tableau provers are very successful in modal and description logics.

3.7 First-Order CNF Transformation

Similar to the propositional case, first-order superposition operates on clauses. In this section I show how any first-order sentence can be efficiently transformed into a CNF, preserving satisfiability. To this end all existentially quantified variables are replaced with so called Skolem functions. Similar to renaming this replacement only preserves satisfiability. Eventually, all variables in clauses are implicitly universally quantified.

As usual, the CNF transformation is done by a set of rules. All rules known from the propositional case apply. Further rules deal with the quantifies $\forall$, $\exists$ and some of the propositional rules need an extension in order to cope with first-order variables.

The first set of rules eliminates $\top$ and $\bot$ from a first-order formula.

ElimTB1 $\chi[(\phi \wedge \top)]_p \Rightarrow_{\mathrm{CNF}} \chi[\phi]_p$

ElimTB2 $\chi[(\phi \wedge \bot)]_p \Rightarrow_{\mathrm{CNF}} \chi[\bot]_p$

ElimTB3 $\chi[(\phi \vee \top)]_p \Rightarrow_{\mathrm{CNF}} \chi[\top]_p$

ElimTB4 $\chi[(\phi \vee \bot)]_p \Rightarrow_{\mathrm{CNF}} \chi[\phi]_p$

ElimTB5 $\chi[\neg\bot]_p \Rightarrow_{\mathrm{CNF}} \chi[\top]_p$

ElimTB6 $\chi[\neg\top]_p \Rightarrow_{\mathrm{CNF}} \chi[\bot]_p$

ElimTB7 $\chi[\{\forall,\exists\}x.\top]_p \Rightarrow_{\text{CNF}} \chi[\top]_p$

ElimTB8 $\chi[\{\forall,\exists\}x.\bot]_p \Rightarrow_{\text{CNF}} \chi[\bot]_p$

where the expression $\{\forall,\exists\}x.\phi$ covers both cases $\forall x.\phi$ and $\exists x.\phi$. The next step is to rename all variable such that different quantifiers bind different variables. This step is necessary to prevent a later on confusion of variables.

RenVar $\phi \Rightarrow_{\text{CNF}} \phi\sigma$
for $\sigma = \{\}$

Once the variable renaming is done, renaming of beneficial subformulas is the next step. The mechanism of renaming and the concept of a beneficial subformula is exactly the same as in propositional logic. The only difference is that renaming does introduce an atom in the free variables of the respective subformula. When some formula ψ is renamed at position p an atom $P(\vec{x_n})$, $\vec{x_n} = x_1,\ldots,x_n$ replaces $\psi|_p$ where $\text{fvars}(\psi|_p) = \{x_1\ldots,x_n\}$. The respective definition of $P(\vec{x_n})$ becomes

$$\text{def}(\psi,p,P(\vec{x_n})) := \begin{cases} \forall\vec{x_n}.(P(\vec{x_n}) \rightarrow \psi|_p) & \text{if } \text{pol}(\psi,p) = 1 \\ \forall\vec{x_n}.(\psi|_p \rightarrow P(\vec{x_n})) & \text{if } \text{pol}(\psi,p) = -1 \\ \forall\vec{x_n}.(P(\vec{x_n}) \leftrightarrow \psi|_p) & \text{if } \text{pol}(\psi,p) = 0 \end{cases}$$

and the rule SimpleRenaming is changed accordingly.

SimpleRenaming $\phi \Rightarrow_{\text{CNF}} \chi[A_1]_{p_1}[A_2]_{p_2}\ldots[A_n]_{p_n} \wedge \text{def}(\phi,p_1,A_1) \wedge \ldots \wedge \text{def}(\chi[A_1]_{p_1}[A_2]_{p_2}\ldots[A_{n-1}]_{p_{n-1}},p_n,A_n)$
provided $\{p_1,\ldots,p_n\} \subset \text{pos}(\phi)$ and for all $i, i+j$ either $p_i \parallel p_{i+j}$ or $p_i > p_{i+j}$ and the $A_i = P_i(x_{i,1},\ldots,x_{i,k_i})$ where $\text{fvars}(\phi|_{p_i}) = \{x_{i,1},\ldots,x_{i,k_i}\}$ and all P_i are different and new to ϕ

Negation normal form is again done as in the propositional case with additional rules for the quantifiers.

ElimEquiv $\chi[(\phi \leftrightarrow \psi)]_p \Rightarrow_{\text{CNF}} \chi[(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)]_p$

ElimImp $\chi[(\phi \rightarrow \psi)]_p \Rightarrow_{\text{CNF}} \chi[(\neg\phi \vee \psi)]_p$

PushNeg1 $\chi[\neg(\phi \vee \psi)]_p \Rightarrow_{\text{CNF}} \chi[(\neg\phi \wedge \neg\psi)]_p$

PushNeg2 $\chi[\neg(\phi \wedge \psi)]_p \Rightarrow_{\text{CNF}} \chi[(\neg\phi \vee \neg\psi)]_p$

PushNeg3 $\chi[\neg\neg\phi]_p \Rightarrow_{\mathrm{CNF}} \chi[\phi]_p$

PushNeg4 $\chi[\neg\forall x.\phi]_p \Rightarrow_{\mathrm{CNF}} \chi[\exists x.\neg\phi]_p$

PushNeg5 $\chi[\neg\exists x.\phi]_p \Rightarrow_{\mathrm{CNF}} \chi[\forall x.\neg\phi]_p$

In propositional logic after NNF, the CNF can be generated using distributivity. In first-order logic the existential quantifiers are eliminated first by the introduction of Skolem functions. In order to receive Skolem functions with few arguments, the quantifiers are first moved inwards as far as passible. This step is called *mini-scoping*.

MiniScope1 $\chi[\forall x.(\psi_1 \circ \psi_2)]_p \Rightarrow_{\mathrm{CNF}} \chi[(\forall x.\psi_1) \circ \psi_2]_p$
provided $\circ \in \{\wedge, \vee\}$, $x \notin \mathrm{fvars}(\psi_2)$

MiniScope2 $\chi[\exists x.(\psi_1 \circ \psi_2)]_p \Rightarrow_{\mathrm{CNF}} \chi[(\exists x.\psi_1) \circ \psi_2]_p$
provided $\circ \in \{\wedge, \vee\}$, $x \notin \mathrm{fvars}(\psi_2)$

MiniScope3 $\chi[\forall x.(\psi_1 \wedge \psi_2)]_p \Rightarrow_{\mathrm{CNF}} \chi[(\forall x.\psi_1) \wedge (\forall x.\psi_2)\sigma]_p$
where $\sigma = \{\}$, $x \in (\mathrm{fvars}(\psi_1) \cap \mathrm{fvars}(\psi_2))$

MiniScope4 $\chi[\exists x.(\psi_1 \vee \psi_2)]_p \Rightarrow_{\mathrm{CNF}} \chi[(\exists x.\psi_1) \vee (\exists x.\psi_2)\sigma]_p$
where $\sigma = \{\}, x \in (\mathrm{fvars}(\psi_1) \cap \mathrm{fvars}(\psi_2))$

The rules MiniScope1, MiniScope2 are applied modulo the commutativity of $\wedge$, $\vee$. Once the quantifiers are moved inwards Skolemization can take place.

Skolemization $\chi[\exists x, \psi]_p \Rightarrow_{\mathrm{CNF}} \chi[\psi\{x \mapsto f(y_1, \ldots, y_n)\}]_p$
provided there is no q, $q < p$ with $\phi|_q = \exists x'.\psi'$, $\mathrm{fvars}(\exists x.\psi) = \{y_1, \ldots, y_n\}$, $\mathrm{arity}(f) = n$ is a new function symbol to ϕ matching the respective sorts of the y_i with range sort $\mathrm{sort}(x)$

Example 3.7.1 (Mini-Scoping and Skolemization)**.** Consider the simple formula $\forall x.\exists y.(R(x,x) \wedge P(y)$. Applying Skolemization directly to this formula, without mini-scoping results in

$$\forall x.\exists y.(R(x,x) \wedge P(y)) \Rightarrow_{\mathrm{CNF,Skolemization}} \forall x.(R(x,x) \wedge P(g(x))$$

for a unary Skolem function g because $\mathrm{fvars}(\exists y.(R(x,x) \wedge P(y))) = \{x\}$. Applying mini-scoping and then Skolemization generates

$$\begin{array}{lll} \forall x.\exists y.(R(x,x) \wedge P(y)) & \Rightarrow^*_{\mathrm{CNF,MiniScope2,1}} & \forall x.R(x,x) \wedge \exists y.P(y) \\ & \Rightarrow_{\mathrm{CNF,Skolemization}} & \forall x.R(x,x) \wedge P(a) \end{array}$$

for some Skolem constant a because $\mathrm{fvars}(\exists y.P(y)) = \emptyset$. Now the former formula after Skolemization is seriously more complex than the latter. The former belongs to an undecidable fragment of first-order logic while the latter belongs to a decidable one (see Section 3.14).

Finally, the universal quantifiers are removed. In a first-order logic CNF any variable is universally quantified by default. Furthermore, the variables of two different clauses are always assumed to be different.

RemForall $\chi[\forall x.\psi]_p \Rightarrow_{\mathrm{CNF}} \chi[\psi]_p$

The actual CNF is then done by distributivity.

PushDisj $\chi[(\phi_1 \wedge \phi_2) \vee \psi]_p \Rightarrow_{\mathrm{CNF}} \chi[(\phi_1 \vee \psi) \wedge (\phi_2 \vee \psi)]_p$

Algorithm 6: $\mathrm{cnf}(\phi)$

Input : A first-order formula ϕ.
Output: A formula ψ in CNF satisfiability preserving to ϕ.

```
1  whilerule (ElimTB1(φ),...,ElimTB8(φ)) do ;
2  RenVar(φ);
3  SimpleRenaming(φ) on obvious positions;
4  whilerule (ElimEquiv1(φ),ElimEquiv2(φ)) do ;
5  whilerule (ElimImp(φ)) do ;
6  whilerule (PushNeg1(φ),...,PushNeg5(φ)) do ;
7  whilerule (MiniScope1(φ),...,MiniScope4(φ)) do ;
8  whilerule (Skolemization(φ)) do ;
9  whilerule (RemForall(φ)) do ;
10 whilerule (PushDisj(φ)) do ;
11 return φ;
```

Theorem 3.7.2 (Properties of the CNF Transformation)**.** Let ϕ be a first-order sentence, then

1. $\mathrm{cnf}(\phi)$ terminates
2. ϕ is satisfiable iff $\mathrm{cnf}(\phi)$ is satisfiable

Proof. (Idea) 1. is a straightforward extension of the propositional case. It is easy to define a measure for any line of Algorithm 6.
2. can also be established separately for all rule applications. The rules SimpleRenaming and Skolemization need separate proofs, the rest is straightforward or copied from the propositional case. □