3. First order logic

3.1. Motivation

Why PL is not enough

Consider the argument:

> *"Every integer number is the difference of two natural numbers. -1 is an integer. Therefore -1 is the difference of two naturals."*

If we examine the argument from the PL perspective, setting

Variable	Interpretation
x	Every integer is the difference of two naturals.
y	-1 is an integer.
z	-1 is the difference of two naturals.

we find that the argument translates into

$$x, y \vDash z$$

which is false: if $v(x) = v(y) = 1$ and $v(z) = 0$, v satisfies the premises though not the conclusion.

Why PL is not enough (continued)

To prove correctness of an argument using PL:

1. we replace atomic sentences with variables;
2. we replace connective of the natural language with propositional connectives;
3. we replace the original argument with the more general $\Gamma \models \varphi$;
4. if the propositional argument is correct, we infer correctens of the original argument.

However, if the more general propositional argument is not correct, that does not mean that the given special case is also not correct.

3.2. Syntax

Structures

Recall: given a set A,

- An **operation of arity** n on A is a function $f : A^n \to A$.
- A **relation of arity** n on A is a subset $R \subseteq A^n$.

In particular, a nullary operation is an element of A.

Definition 3.1. A **(first order) structure** is assigned by:

1. a set A, the **support** (or **universe**) of the structure,
2. a sequence $(R_1, R_2, ...)$ of relations on A,
3. a sequence $(f_1, f_2, ...)$ of operations on A.

- We represent a structure with a sequence $(A, R_1, R_2, \dots, f_1, f_2, \dots)$
- When the rest of the structure is understood, we abbreviate the sequence with the support A.

Examples of structures

1. The **group of integers** is the structure $(\mathbf{Z}, 0, -, +)$ where $\mathbf{Z} = \{\ldots, -1, 0, 1, \ldots\}$ is the set of integers and the remaining symbols are defined in the table below.

Symbol	Type	Arity	Description
0	operation	0	the element 0
$-$	operation	1	the opposite
$+$	operation	2	addition

2. The **group of plane rotations** is the structure $(S^1, 0, -, +)$ where S^1 is unit circle in the plane and the remaining symbols are defined in the table below.

Symbol	Type	Arity	Description
0	operation	0	the point $(1, 0)$, which corresponds to the 0 angle
$-$	operation	1	the simmetric point w.r.t. the x-axis, i.e. the point that corresponds to the opposite angle
$+$	operation	2	the point obtained by adding the angles

Examples of structures (continued)

3. The **ordered ring of integers** is $(\mathbf{Z}, \leq, 0, 1, -, +, \times)$ where **Z** is the set of integers and

Symbol	Type	Arity	Description
$\leq$	relation	2	order relation
0	operation	0	the element 0
1	operation	0	the element 1
$-$	operation	1	the opposite
$+$	operation	2	addition
$\times$	operation	2	multiplication

4. The **ordered field of real numbers** is $(\mathbf{R}, \leq, 0, 1, -, +, \times)$ where **R** is the set of real numbers

Symbol	Type	Arity	Description
$\leq$	relation	2	order relation
0	operation	0	the element 0
$\vdots$	$\vdots$	$\vdots$	$\vdots$

First order signatures

Definition 3.2. A **(first order) signature** is assigned by:

1. a sequence $(R_1, R_2, ...)$ of **relation symbols** (or **predicates**)
2. a sequence $(f_1, f_2, ...)$ of **function symbols**
3. an **arity function** assigning to each symbol a natural number, its arity.

Function symbols of arity 0 are also called **constants**

Every structure has an associated signature:

1. the signature of the group of integers is $\{0, -, +\}$; all symbols are function symbols and their arities are, respectively, 0,1 and 2. It is the same as the signature of the group of plane rotations. This is called the signature of **abelian groups**.
2. the signature of the ordered ring of integers is $\{\leq, 0, 1, -, +, \times\}$; the first symbol is a relation symbol, all others are function symbols; the arities are 2, 0, 0, 1, 2 and 2. It is the same as the signature of the field of real numbers. This is called the signature of **ordered rings**

We tend to use as symbols of the signature the symbol of the original relations and operations, although this is not necessary.

Terms

Definition 3.3. The set of **terms** generated by a signature S and by a set $X = \{x_0, x_1, ...\}$ of variables is the smallest set T whose elements are recursively defined by a finite application of the following formation rules.

1. Every variable is a term.
2. If $f \in S$ is a function symbol of arity n and $t_1, \ldots, t_n \in T$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

A term is **closed** it it contains no variables.

1. Function symbols of arity 0 are called **constants**
2. If c is a constant, we write c instead of $c()$.
3. If $\Box$ is a function symbol of arity 2, we write $t_1 \Box t_2$ instead of $\Box(t_1, t_2)$.

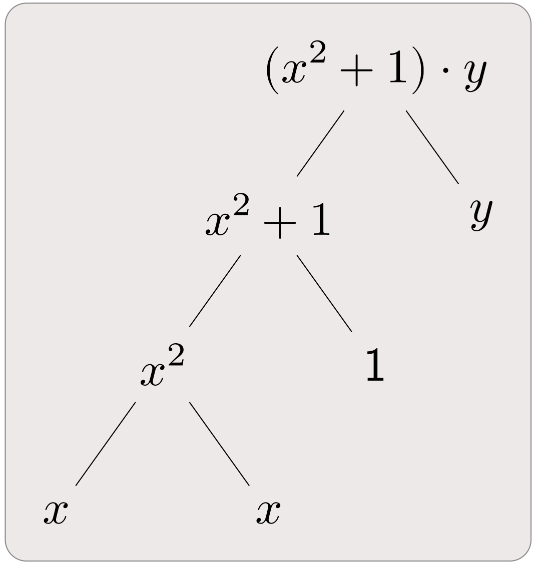
Terms, example

Let $S = \{\leq, 0, 1, -, +, \cdot\}$ be the signature of ordered rings. We claim that

$$(x^2 + 1) \cdot y$$

is a term of S. This is either proved using a formation sequence or a formation tree:

Step	Term	Formation rule
1	x	variable
2	x^2	1 (twice), product
3	1	constant
4	$x^2 + 1$	2, 3, sum
5	y	variable
6	$(x^2 + 1) \cdot y$	4, 5, product



We are using some standard abbreviations: xy instead of $x \cdot y$ and x^2 instead of xx.

Formulas

Definition 3.4. The **language** generated by S and X is the smallest set L whose elements, called **formulas**, are recursively defined by a finite application of the following formation rules.

1. $\top$ and $\bot$ are formulas.
2. if R is a relation symbol of arity n and $t_1, \dots, t_n$ are terms, then $R(t_1, \dots, t_n)$ is a formula.
3. If c is a connective of arity n and $\varphi_1, \dots, \varphi_n$ are formulas, then $c(\varphi_1, \dots, \varphi_n)$ is a formula.
4. If φ is a formula and x is a variable then $((\forall x)\varphi)$ and $((\exists x)\varphi)$ are formulas.

A language **with equality** has the additional formation rule

5. if t_1 and t_2 are terms, then $t_1 = t_2$ is a formula.

- Formulas of type 1, 2 and 5 are called **atomic**.
- The symbols $\exists$ (there exists) and $\forall$ (for all) are the existential and universal **quantifiers**.
- If Q is a quantifier, the formula φ in $((Qx)\varphi)$ is the **scope** of the quantifier Q.
- We drop parentheses as in PL agreeing that quantifiers bind more strongly than any connective.
- We collapse quantifiers: if Q is a fixed quantifier, we write $Qx_1 \dots x_n$ instead of $Qx_1 \dots Qx_n$.

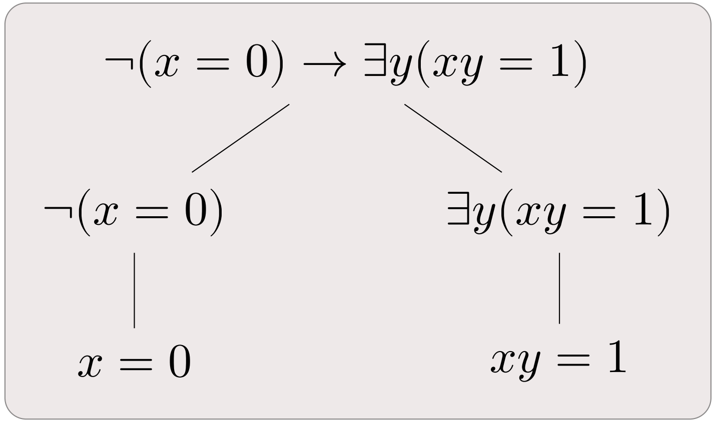
Formulas, example

Let $S = \{\leq, 0, 1, -, +, \cdot\}$ be the signature of ordered rings. We claim that

$$x \neq 0 \to \exists y(xy = 1)$$

is a formula of the first order language (with equality) generated by S. This is again proved using a formation sequence or a formation tree:

Step	Formula	Formation rule
1	$x = 0$	equality
2	$\neg(x = 0)$	1, negation
3	$xy = 1$	equality
4	$\exists y(xy = 1)$	3, existential quantifier
5	$(x \neq 0) \to \exists y(xy = 1)$	2, 5, implication



Note that we are using $t_1 \neq t_2$ as an abbreviation for $\neg(t_1 = t_2)$.

Proposition 3.5. (Proof by induction on terms) Let L be a first order language and let P be a property that terms of L may or may not have. Write $t \in P$ when the term t has the property P. Assume that

1. $x \in P$ for every variable x
2. if f is a function symbol of arity n and $t_1, \dots, t_n \in P$, then $f(t_1, \dots, t_n) \in P$.

Then $t \in P$ for all terms of L. $\square$

Proposition 3.6. (Proof by induction on formulas) Let L be a first order language and let P be a property that formulas of L may or may not have. Write $\varphi \in P$ when the formula φ has the property P. Assume that

1. $\varphi \in P$ for every atomic formula φ.
2. If $\varphi_1, \dots, \varphi_n \in P$ then $c(\varphi_1, \dots, \varphi_n) \in P$
3. If $\varphi \in P$, then $Qx.\varphi \in P$.

Then $\varphi \in P$ for all formulas φ of L. $\square$

Proposition 3.7. Assume L is a first order language and $h_0 : X \to S$ is a function from the set of variables of L to any set S. Assume that for every functional symbol f of arity n we are given a function $f_S : S^n \to S$. Then h extends uniquely to a function $h : T \to S$ satisfying the condition

$$h(f(t_1, \dots, t_n)) = f_s(h(t_1), \dots, h(t_n))\,.$$

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "h_0"'] & T \arrow[d, "h"] & T^n \arrow[l, "f"'] \arrow[d, "h^n"] \\
& S & S^n \arrow[l, "f_S"]
\end{tikzcd}$$

Definition by recursion on formulas

Proposition 3.8. Assume $h : A \to S$ is a function from the set A of atomic formulas of L to any set S. Assume further that for every propositional connective c of arity n and for every quantifier Q we are given functions

$$c_S : S^n \to S, \qquad Q_S : \kappa \times S \to S,$$

where $\kappa = |X|$. Then h extends uniquely to a function $L \to S$ such that

$$h(c(\varphi_1, \ldots, \varphi_n)) = c_s(h(\varphi_1), \ldots, h(\varphi_n)), \qquad h(Qx_i.\varphi) = Q_s(i, h(\varphi))$$

Free variables

Definition 3.9. **Free variable occurrences** in a formula φ are defined recursively as follows:

1. All variable occurrences in atomic formulas are free.
2. The free variable occurrences in $c(\varphi_1, \ldots, \varphi_n)$ are all the free variable occurrences in $\varphi_1, \ldots, \varphi_n$
3. The free variable occurrences of $Qx.\varphi$ are all free variable occurrences of φ except for all occurrences of x in φ.

A formula with no free occurrences of variables is called a **sentence** (or a **closed** formula). A variable is **free** in a formula if it has at least one free occurrence.

Example Let L be the language of the ordered field of real numbers. Consider the formulas

1. $\forall y(x \leq y) \to \exists x(x \leq y)$
2. $\forall x(x \geq 0 \to \exists y(x = y^2))$

In the first formula, the first occurrence of x is free, the second is bound; conversely, the first occcurrence of y is bound and the second is free. Therefore, both x and y are free variables in the formula.
In the second formula all occurrences of x and y are bound; the formula is closed.

Substitution in terms

Definition 3.10. A **substitution** is a function $\sigma : T \to T$ on the set of terms satisfying the condition

$$[f(t_1, \dots, t_n)]\sigma = f(t_1\sigma, \dots, t_n\sigma).$$

- We write substitution multiplicatively ($t\sigma$) rather than functionally ($\sigma(t)$).
- By the recursive definition theorem, a substitution is determined by its value on variables.
- We can define a product of substitutions as functions and $(t\sigma)\tau = t(\sigma\tau)$ by the definition of product function.
- The product of substitutions, like any product of functions, is associative: $(\sigma\tau)\upsilon = \sigma(\tau\upsilon)$

Example Assume $X = \{x, y, z\}$ and

$$x\sigma = f(x, y), \qquad y\sigma = h(a), \qquad z\sigma = g(c, h(x)).$$

Then

$$j(k(x), y)\sigma = j(k(x)\sigma, y\sigma) = j(k(x\sigma), y\sigma) = j(k(f(x, y)), h(a)).$$

Definition 3.11. The **support** of a substitution σ is the set of variables x for which $x\sigma \neq x$. If σ has finite support $\{x_1, \dots, x_n\}$ and $x_i\sigma = t_i$ we write $\sigma = [t_1/x_1, \dots, t_n/x_n]$.

Proposition 3.12. The product of substitution with finite support has finite support. Moreover, if

$$\sigma = [s_1/x_1, \dots, s_m/x_m], \qquad \tau = [t_1/y_1, \dots, t_n/y_n],$$

then

$$\sigma\tau = [s_1\tau/x_1, \dots, s_m\tau/x_m, z_1\tau/z_1, \dots, z_p\tau/z_p]$$

where the z_i's are the variables in the list $y_1, \dots, y_n$ which are not in the list $x_1, \dots, x_m$.

Example Suppose

$$\sigma = [f(x, y)/x, h(a)/y, g(c, h(x))/z], \qquad \tau = [b/x, g(a, x)/y, z/w].$$

Then

$$\sigma\tau = [f(b, g(a, x))/x, h(a)/y, g(c, h(b))/z, z/w].$$

Substitution in formulas

Definition 3.13. Assume σ is a substitution and x a variable. We write σ_x for the substitution which coincides with σ except that it fixes x.

$$y\sigma_x = \begin{cases} y\sigma & \text{if } y \neq x \\ x & \text{if } y = x \end{cases}$$

Definition 3.14. Substitutions can be extended recursively to formulas as follows:

1. $\top\sigma := \top$
2. $\bot\sigma := \bot$
3. $R(s_1, \ldots, s_n)\sigma := R(s_1\sigma, \ldots, s_n\sigma)$
4. $(s_1 = s_2)\sigma := (s_1\sigma = s_2\sigma)$
5. $c(\varphi_1, \ldots, \varphi_n)\sigma := c(\varphi_1\sigma, \ldots, \varphi_n\sigma)$
6. $(Qx.\varphi)\sigma := Qx(\varphi\sigma_x)$

Examples of substitution in formulas

Example Suppose $\sigma = [a/x, b/y]$. Then

$$\begin{aligned}(\forall x.R(x,y) \to \exists y.R(x,y))\,\sigma &= (\forall x.R(x,y))\,\sigma \to (\exists y.R(x,y))\,\sigma \\ &= \forall x(R(x,y)\,\sigma_x) \to \exists y(R(x,y)\,\sigma_y) \\ &= \forall x.R(x\sigma_x, y\sigma_x) \to \exists y.R(x\sigma_y, y\sigma_y) \\ &= \forall x.R(x,b) \to \exists y.R(a,y)\end{aligned}$$

Example Recall that $(t\sigma)\tau = t(\sigma\tau)$ for terms. This is not true for formulas: suppose $\sigma = [y/x]$ and $\tau = [c/y]$, where c is a constant, so that $\sigma\tau = [c/x, c/y]$. If If $\varphi = \forall y.R(x,y)$, then

$$\begin{aligned}(\varphi\sigma)\tau = [(\forall y.R(x,y))\,\sigma]\,\tau = [\forall y(R(x,y)\,\sigma_y)]\,\tau &= [\forall y.R(y,y)]\,\tau \\ = \forall y(R(y,y)\,\tau_y) = \forall y.R(y,y)\,.\end{aligned}$$

$$\varphi(\sigma\tau) = (\forall y.R(x,y))\,[c/x, c/y] = \forall y(R(x,y)\,[c/x]) = \forall y.R(c,y)$$

Free substitutions

Definition 3.15. We define recursively what it means for a substitution σ to be **free** for a formula φ:

1. σ is free for every atomic formula φ
2. σ is free for $c(\varphi_1, \dots, \varphi_n)$ if it is free for $\varphi_1, \dots, \varphi_n$.
3. σ is free for $Qx.\varphi$ if
   - σ_x is free for φ
   - If $y \neq x$ occurs free in φ, then $y\sigma$ does not contain x

- The second condition in 3 means that Qx can not capture extra variables in $\varphi\sigma$.
- Being free is not restrictive if we have enough variables: we can change the quantified variable.
- When we perform a substitution σ in φ we will **always assume that it is free** because :

Theorem 3.16. If σ is free for φ and τ is free for $\varphi\sigma$, then

$$(\varphi\sigma)\tau = \varphi(\sigma\tau).$$

3.3. Semantics

Definition 3.17. Let L be a first order language generated by a signature S and by a set X of variables. An L**-structure** is assigned by the following data:

1. A set M, the **support** (or **carrier**) of the structure.
2. For every relation symbol $R \in S$ of arity n a relation $[\![R]\!] \subseteq M^n$.
3. For every function symbol $f \in S$ of arity n a function $[\![f]\!] : M^n \to M$.

We use just M to indicate the structure when this does not cause ambiguity.

Example Let L be the language generated by the signature $S = \{\leq, 0, -, +\}$. The following are examples of L-structures.

1. The **ordered group of integers** $(\mathbf{Z}, \leq, 0, -, +)$ where $[\![\leq]\!]$ is the usual order relation $\leq$ on **Z**, $[\![0]\!]$ is the integer 0, etc.
2. The **ordered multiplicative group of the rationals**, $(\mathbf{Q}^\times, \leq, 1, (\_)^{-1}, \times)$, where $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$ is the set of nonzero rationals, $[\![0]\!] = 1$, $[\![-]\!]$ is the the function $(\_)^{-1}$ assigning to every nonzero rational its multiplicative inverse and $[\![+]\!]$ is the multiplication between rationals.

Valuations

Definition 3.18. If M is an L-structure, a **valuation** in M is a function $v : T \to M$ associating to every term an element of M in such a way that for every function symbol f of arity n and terms $t_1, \dots, t_n$ we have

$$v(f(t_1, \dots, t_n)) = [\![f]\!] \left(v(t_1), \dots, v(t_n)\right).$$

$$\begin{tikzcd} T^n \arrow[r, "v^n"] \arrow[d, "f"'] & M^n \arrow[d, "{[\![f]\!]}"] \\ T \arrow[r, "v"'] & M \end{tikzcd}$$

By the recursive definition theorem 3.7, v is uniquely determined once its value on the set X of variables has been assigned. Also, if $t \in T$ is closed, $v(t)$ does not depend on v and we write $[\![t]\!]$ instead.

Valuations, example

Let L be the first order language generated by the signature $S = (0, 1, +, \cdot, \leq)$ of arithmetic and let $\mathbf{N} = (\mathbf{N}, 0, 1, +, \cdot, \leq)$ be the L-structure of natural numbers. Note that that we are interpreting the symbols of the signature with the operation of the same name, i.e. $[\![0]\!] = 0$, $[\![1]\!] = 1$, $[\![+]\!] = +$ and so on. Consider the term

$$t = (x + 1)\, y$$

and the valuation defined by $v(x) = 3$, $v(y) = 2$. Then

$$\begin{aligned} v(t) &= v((x+1)\, y) \\ &= v(x+1) \cdot v(y) \\ &= (v(x) + v(1)) \cdot v(y) \\ &= (3+1) \cdot 2 \\ &= 8. \end{aligned}$$

Variants

Definition 3.19. Assume M is an L-structure and x is a variable. Two valuations $u, v : T \to M$ are **x-variants** if $u(y) = v(y)$ for every variable $y \neq x$.

In particular, given a valuation $v : T \to M$ and an element $a \in M$, we define the x-variant $v[a/x]$ setting

$$v[a/x]\,(y) = \begin{cases} a & \text{if } y = x \\ v(y) & \text{if } y \neq x \end{cases}$$

Evaluating formulas

Definition 3.20. Given a valuation $v : T \to M$ we define recursively what it means for v to **satisfy** (or to be a **model** of) a formula φ, in symbols $v \models \varphi$, as follows:

Formula	**Condition**
$v \models \top$	always
$v \models \bot$	never
$v \models R(t_1, \dots, t_n)$	if $(v(t_1), \dots, v(t_n)) \in [\![R]\!]$
$v \models t_1 = t_2$	if $v(t_1) = v(t_2)$
$v \models \neg\varphi$	if $v \not\models \varphi$
$v \models \varphi \wedge \psi$	if $v \models \varphi$ and $v \models \psi$
$v \models \varphi \vee \psi$	if $v \models \varphi$ or $v \models \psi$ or both
$v \models \varphi \to \psi$	if $v \models \psi$ whenever $v \models \varphi$
$v \models \varphi \leftrightarrow \psi$	if $v \models \varphi$ if and only if $v \models \psi$
$v \models \forall x.\varphi$	if $u \models \varphi$ for every x-variant u of v
$v \models \exists x.\varphi$	if $u \models \varphi$ for at least one x-variant u of v

Evaluating formulas, an example

Consider the language L generated by the signature $(\leq, 0, 1, -, +, \cdot)$, the L-structure $M = (\mathbf{Q}, \leq, 0, 1, -, +, \cdot)$ and the formula $\varphi := \exists x(x^2 = y)$.

1. If v is any valuation such that $v(y) = 4$, then $v \vDash \varphi$:

$$\begin{aligned} v \vDash \varphi &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } v[a/x] \vDash x^2 = y \\ &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } v[a/x]\,(x^2) = v[a/x]\,(y) \\ &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } a^2 = 4 \end{aligned}$$

   and the last condition is satisfied if we take $a = 2$.
2. If v is any valuation such that $v(y) = 2$, then $v \nvDash \varphi$:

$$\begin{aligned} v \vDash \varphi &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } v[a/x] \vDash x^2 = y \\ &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } v[a/x]\,(x^2) = v[a/x]\,(y) \\ &\Leftrightarrow \text{there exists } a \in \mathbf{Q} \text{ such that } a^2 = 2 \end{aligned}$$

   and the last condition is not satisfied as there is no rational number whose square is 2.

Models and substitution

Proposition 3.21. Assume φ is a formula, t is a term and v a valuation. Then

$$v \models \varphi[t/x] \Leftrightarrow v[v(t)/x] \models \varphi.$$

By induction.

Definition 3.22. Assume L is a first order language, $\varphi \in L$ is a formula and M is an L-structure.

1. φ is **satisfiable in M** if it has a model in M.
2. φ is **valid in M** if all valuations in M are models of φ.
3. φ is **unsatisfiable in M** if it has no models in M.

When φ is valid in M we write $M \models \varphi$ and call M a **model** of φ. Moreover, we say that

4. φ is **satisfiable** if it is satisfiable in some L-structure.
5. φ is **valid** if all valuations in all L-structures are models of φ.
6. φ is **unsatisfiable** if it has no models at all.

When φ is valid we write $\models \varphi$. Similar definitions can be given for a set Γ of formulas of L.

Satisfiability and validity, example 1

Consider the first order language of the ring of integers $(\mathbf{Z}, 0, 1, -, +, \cdot)$ and the formula

$$\forall x(x \neq 0 \to \exists y(xy = 1)).$$

1. $\mathbf{Q} \vDash \varphi$. In fact, for any valuation v, we have

$$\begin{aligned} v \vDash \varphi \Leftrightarrow\ & \text{for every } a \in \mathbf{Q}\ , v[a/x] \vDash x \neq 0 \to \exists y(xy = 1) \\ \Leftrightarrow\ & \text{for every } a \in \mathbf{Q}, \text{ if } v[a/x] \vDash \neg(x = 0), \text{ then } v[a/x] \vDash \exists y(xy = 1) \\ \Leftrightarrow\ & \text{for every } a \in \mathbf{Q}, \text{ if } v[a/x] \nvDash x = 0, \text{ then there exists } b \in \mathbf{Q} \text{ s.t. } v[a/x, b/y] \vDash xy = 1 \\ \Leftrightarrow\ & \text{for every } a \in \mathbf{Q}, \text{ if } a \neq 0 \text{ then there exists } b \in \mathbf{Q} \text{ such that } ab = 1 \end{aligned}$$

   And indeed, given any rational number $a \neq 0$ we can pick $b = a^{-1}$.
2. $\mathbf{Z} \nvDash \varphi$. In fact, arguing exactly as above, we see that when $a = 2$, for example, there is no $b \in \mathbf{Z}$ such that $ab = 1$.

In particular, the formula φ is not valid.

Satisfiability and validity, example 2

Consider the first order language L generated by the signature $\{<\}$ consisting of a single relation symbol of arity two. Let φ be the following formula of L:

$$\exists x(x < y)\,.$$

1. φ is satisfiable but not valid in $(\mathbf{N}, <)$. In fact any valuation v with $v(y) = 1$ satisfies φ:

$$\begin{aligned} v \models \exists x(x < y) &\Leftrightarrow \text{there exists } a \in \mathbf{N} \text{ such that } v[a/x] \models x < y \\ &\Leftrightarrow \text{there exists } a \in \mathbf{N} \text{ such that } v[a/x]\,(x) < v[a/x]\,(y) \\ &\Leftrightarrow \text{there exists } a \in \mathbf{N} \text{ such that } a < 1 \end{aligned}$$

   and we can take $a = 0$. Instead, if $v(y) = 0$, then $v \not\models \varphi$.
2. φ is valid in $(\mathbf{Z}, <)$

Hence φ is not valid.

Existential and universal closure

Definition 3.23. Assume $\varphi(x_1, \ldots, x_n)$ is a formula whose only free variables are $x_1, \ldots, x_n$. The formulas

$$\exists x_1 \ldots x_n \varphi(x_1, \ldots, x_n), \qquad \forall x_1 \ldots x_n \varphi(x_1, \ldots, x_n)$$

are called, respectively, the **existential** and the **universal closure** of φ.

Note:

1. Both the existential and the universal closure are closed formulas.
2. φ is satisfiable in M iff its existential closure is valid in M
3. φ is valid in M iff its universal closure is valid in M.
4. Thus, when satisfiability and validity are involved, we may always assume that our formulas are closed.

Definition 3.24. Assume $\Gamma \subseteq L$ is set of formulas of a first order language. A formula $\varphi \in L$ is a **consequence** of Γ if every model of Γ is also a model of φ. In this case we write $\Gamma \models \varphi$ and say that Γ **satisfies** φ.

Exactly as in PL one proves the following theorems:

Proposition 3.25. (Deduction theorem) Assume $\Gamma \subseteq L$ is set of formulas and $\varphi, \psi \in L$ are formulas. Then

$$\Gamma, \varphi \models \psi \quad \Leftrightarrow \quad \Gamma \models \varphi \to \psi.$$

Proposition 3.26. If Γ is a set of formulas in a first order language and φ is a formula of L, then

$$\Gamma \models \varphi \Leftrightarrow \Gamma \cup \{\neg\varphi\} \text{ is unsatisfiable.}$$

Equivalence

Definition 3.27. Two formulas $\varphi, \psi \in L$ of a first order language are **equivalent** if they have the same models; in this case we write $\varphi \equiv \psi$.

Proposition 3.28. $\varphi \equiv \psi \Leftrightarrow\ \models \varphi \leftrightarrow \psi$.

Proof. It suffices to observe that

$$\begin{aligned}
\models \varphi \leftrightarrow \psi &\Leftrightarrow \text{for all valuations } v \text{ we have } v \models \varphi \leftrightarrow \psi && \text{definition of validity} \\
&\Leftrightarrow \text{for all valuations } v \text{ we have } v \models \varphi \text{ iff } v \models \psi && \text{definition } (\triangleright 3.20) \\
&\Leftrightarrow \varphi \equiv \psi. && \text{definition of equivalence}
\end{aligned}$$

Basic equivalences involving quantifiers

Proposition 3.29. The following equivalences hold in any first order language L.

1. $\forall xy.\varphi \equiv \forall yx.\varphi$ $\quad$ $\exists xy.\varphi \equiv \exists yx.\varphi$
2. $\forall x(\varphi \wedge \psi) \equiv \forall x.\varphi \wedge \forall x.\psi$ $\quad$ $\exists x(\varphi \vee \psi) \equiv \exists x.\varphi \vee \exists x.\psi$
3. $\forall x.\varphi \equiv \varphi$ $\quad$ $\exists x.\varphi \equiv \varphi$ $\quad$ if x does not occur free in φ
4. $\neg\forall x.\varphi \equiv \exists x.\neg\varphi$ $\quad$ $\neg\exists x.\varphi \equiv \forall x.\neg\varphi$

Prof of 1 for the universal quantifier. Let v be any valuation into an L-structure M.

$$\begin{aligned}
v \vDash \forall xy.\varphi &\Leftrightarrow \text{for every } a \in M \;\; v[a/x] \vDash \forall y.\varphi \\
&\Leftrightarrow \text{for every } a, b \in M \;\; v[a/x, b/y] \vDash \varphi \\
&\Leftrightarrow \text{for every } a, b \in M \;\; v[b/y, a/x] \vDash \varphi \\
&\Leftrightarrow v \vDash \forall yx.\varphi
\end{aligned}$$

1. In general, the universal quantifier does not commute with the existential quantifier.

$$\forall x \exists y.\varphi(x, y) \not\equiv \exists y \forall x.\varphi(x, y)$$

For example:

$$\mathbf{N} \models \forall x \exists y(x < y), \qquad \mathbf{N} \not\models \exists y \forall x(x < y)$$

2. The universal quantifier does not distribute over disjunction and the existential quantifier does not distribute over conjunction, in general.

$$\forall x(\varphi \vee \psi) \not\equiv \forall x.\varphi \vee \forall x.\psi \qquad\qquad \exists x(\varphi \wedge \psi) \not\equiv \exists x.\varphi \wedge \exists x.\psi.$$

For example, if we interpret in $\mathbf{N}$ the formulas

$$\varphi := \exists y(x = 2y), \qquad \psi := \exists y(x = 2y + 1)$$

then the first asserts that x is even, the second that x is odd. Then

$$\mathbf{N} \models \forall x(\varphi \vee \psi) \qquad \mathbf{N} \not\models \forall x.\varphi \vee \forall x.\psi$$

Uniform notation

Besides α and β-formulas, we define formulas of **universal type**, which we also call γ-**formulas** and formulas of **existential type**, which we also call δ-**formulas**, in the tables below. We also define, for every term t, what is an instance of the formula.

γ	$\gamma(t)$
$\forall x \varphi$	$\varphi[t/x]$
$\neg \exists x \varphi$	$\neg \varphi[t/x]$

δ	$\delta(t)$
$\exists x \varphi$	$\varphi[t/x]$
$\neg \forall x \varphi$	$\neg \varphi[t/x]$

Notice that

$$\gamma \equiv \forall y.\gamma(y) \qquad\qquad \delta \equiv \exists y.\delta(y)\,.$$

where y is a variable not appearing neither in γ nor in δ.

Proposition 3.30. (Proof by structural induction) Every formula φ has a property P provided:

1. $\varphi \in P$ and $\neg\varphi \in P$ for every atomic φ.
2. If $\varphi \in P$ then $\neg\neg\varphi \in P$.
3. If both $\alpha_1 \in P$ and $\alpha_2 \in P$, then $\alpha \in P$.
4. If both $\beta_1 \in P$ and $\beta_2 \in P$, then $\beta \in P$.
5. If $\gamma(t) \in P$ for every term t, then $\gamma \in P$.
6. If $\delta(t) \in P$ for every term t, then $\delta \in P$.

Proposition 3.31. (Definition by recursion on formulas) A function f defined on atomic formulas extends uniquely to the language provided:

1. $f(\neg\neg\varphi)$ is specified in terms of $f(\varphi)$
2. $f(\alpha)$ is specified in terms of $f(\alpha_1)$ and $f(\alpha_2)$
3. $f(\beta)$ is specified in terms of $f(\beta_1)$ and $f(\beta_2)$
4. $f(\gamma)$ is specified in terms of $f(\gamma(t))$
5. $f(\delta)$ is specified in terms of $f(\delta(t))$

Separating variables

Definition 3.32. A formula φ has **separated variables** if

1. No two quantifiers in φ bind the same variable
2. No bound variables occur also free.

Every formula is equivalent to one with separated variables.

Quantifier rewrite rules

Proposition 3.33. Assuming all formulas have separated variables, the following equivalences hold.

1. $\neg(\forall x.\varphi) \equiv \exists x.\neg\varphi)$ $\qquad$ $\neg(\exists x.\varphi) \equiv \forall x.\neg\varphi$
2. $(\forall x.\varphi) \wedge \psi \equiv \forall x(\varphi \wedge \psi)$ $\qquad$ $(\exists x.\varphi) \wedge \psi \equiv \exists x(\varphi \wedge \psi)$
3. $(\forall x.\varphi) \vee \psi \equiv \forall x(\varphi \vee \psi)$ $\qquad$ $(\exists x.\varphi) \vee \psi \equiv \exists x(\varphi \vee \psi)$
4. $(\forall x.\varphi) \to \psi \equiv \exists x(\varphi \to \psi)$ $\qquad$ $(\exists x.\varphi) \to \psi \equiv \forall x(\varphi \to \psi)$
5. $\varphi \to (\forall x.\psi) \equiv \forall x(\varphi \to \psi)$ $\qquad$ $\varphi \to (\exists x.\psi) \equiv \exists x(\varphi \to \psi)$

Quantifier rewrite rules (continued)

Proof of 1. Let v be any valuation in an L-structure M.

$$\begin{aligned} v \models \neg(\forall x.\varphi) &\Leftrightarrow v \not\models \forall x.\varphi \\ &\Leftrightarrow v[a/x] \not\models \varphi \text{ for some } a \in M \\ &\Leftrightarrow v[a/x] \models \neg\varphi \text{ for some } a \in M \\ &\Leftrightarrow v \models \exists x.\neg\varphi \end{aligned}$$

Proof of 2 for the universal quantifier.

$$\begin{aligned} v \models (\forall x.\varphi) \wedge \psi &\Leftrightarrow v \models \forall x.\varphi \text{ and } v \models \psi \\ &\Leftrightarrow v[a/x] \models \varphi \text{ and } v[a/x] \models \psi \text{ for all } a \in M \\ &\Leftrightarrow v[a/x] \models (\varphi \wedge \psi) \ \text{ for all } a \in M \\ &\Leftrightarrow v \models \forall x(\varphi \wedge \psi) \end{aligned}$$

Notice that in the second line of the proof of 2 we can replace $v \models \psi$ with $v[a/x] \models \psi$ as x does not occur in ψ because of the assumption on separated variables. The other proofs are similar.

Prenex form

Definition 3.34. A formula is in **prenex form** if it is of type $Q_1 x_1 \cdots Q x_n\ \varphi$ where φ is quantifier-free.

From proposition (3.33) and using structural induction we immediately have

Corollary 3.35. Every formula of a first order language L is equivalent to a formula of L in prenex form. $\square$

Prenex form, example

We compute a prenex form. Note that we separate variables, first.

$$\begin{aligned}
\forall x \exists y\ \varphi(x, y, z) \to \forall x \exists y\ \psi(x, y, z) &\equiv \forall x \exists y\ \varphi(x, y, z) \to \forall u \exists v\ \psi(u, v, z) \\
&\equiv \exists x (\exists y \varphi(x, y, z) \to \forall u \exists v\ \psi(u, v, z)) \\
&\equiv \exists x \forall y (\varphi(x, y, z) \to \forall u \exists v\ \psi(u, v, z)) \\
&\equiv \exists x \forall y \forall u (\varphi(x, y, z) \to \exists v \psi(u, v, z)) \\
&\equiv \exists x \forall y \forall u \exists v (\varphi(x, y, z) \to \psi(u, v, z))
\end{aligned}$$

We can also move the variables in the consequence first, and obtain an equivalent formula:

$$\begin{aligned}
\forall x \exists y\ \varphi(x, y, z) \to \forall x \exists y\ \psi(x, y, z) &\equiv \forall x \exists y\ \varphi(x, y, z) \to \forall u \exists v\ \psi(u, v, z) \\
&\equiv \forall u \exists v (\forall x \exists y . \varphi(x, y, z) \to \psi(u, v, z)) \\
&\equiv \forall u \exists v \exists x \forall y (\varphi(x, y, z) \to \psi(u, v, z))
\end{aligned}$$

Definition 3.36.

1. A signature S' is an **expansion** of a signature S if $S' \supseteq S$. A first order language L' is an **expansion** of L if it is generated using an expansion of the signature of L and the same set of variables.
2. If M is an L-structure and M' an L'-strucure, we say that M' is an **expansion** of M (or that M is a **reduct** of M') if
   - M and M' have the same support
   - the interpretation in M' of every symbol of L coincides with the interpretation in M.

Example The ordered field of real numbers $(\mathbf{R}, \leq, 0, 1, -, +, \cdot)$ is an expansion of the ordered group of real numbers $(\mathbf{R}, \leq, 0, -, +)$.

Skolemization

Definition 3.37. A formula is **universal** if it is in prenex form and all its quantifiers are universal. Given a formula in prenex form

$$Q_1 x_1 \cdots Q_n x_n \varphi(x_1, \dots, x_n)$$

its **skolemization** is the universal formula obtained by eliminating all existential quantifiers through an application of the following procedure:

1. Identify the first existential quantifier Q_i occurring in the formula.
2. Expand L by adding a new function symbol f of arity $i-1$.
3. Replace the original formula with

$$(Q_1 x_1) \cdots (Q_{i-1} x_{i-1})\,(Q_{i+1} x_{i+1}) \cdots (Q_n x_n)\, \varphi[f(x_1, \dots, x_{i-1})/x_i]$$

Example We Skolemize the following formula

$$\begin{aligned} \exists x \forall y \forall u \exists v(\varphi(x, y, z) \to \psi(u, v, z)) &\mapsto \forall y \forall u \exists v(\varphi(c, y, z) \to \psi(u, v, z)) \\ &\mapsto \forall y \forall u(\varphi(c, y, z) \to \psi(u, f(y, u), z)) \end{aligned}$$

Some remarks on skolemization

1. Any formula φ of L is equivalent to a formula ψ in prenex form by corollary ($\triangleright$3.35); the skolemization of ψ is a called a skolemization of φ and is denoted by φ_S. Mind that it is not unique.
2. φ and φ_S belong to different languages, so it makes no sense to ask whether they are equivalent, in general. But they may even be not equivalent in structures that can interpret both languages.

Example In the language of arithmetic, consider the formula $\exists y(x < y)$. Its skolemization is $x < c$. Both formulas can be interpreted in $\mathbf{N}$; however the first formula is valid in $\mathbf{N}$, whereas the second is not.

Theorem 3.38. φ is satisfiable iff φ_S is.

Proof. By corollary 3.35 we may assume that φ is in prenex form. Taking $y = f(x_1, \dots, x_n)$, we have

$$\forall x_1 \dots x_n \ \psi(x_1, \dots, x_n, f(x_1, \dots, x_n)) \vDash \forall x_1 \dots x_n \exists y \ \psi(x_1, \dots, x_n, y).$$

Thus, if $M \vDash \varphi_S$, then $M \vDash \varphi$. Conversely:

1. Suppose $M \vDash \forall x_1 \dots x_n \exists y \ \psi(x_1, \dots, x_n, y)$.
2. Then, given $(a_1, \dots, a_n) \in M^n$, there exists $b \in M$ such that $M \vDash \psi[a_1/x_1, \dots, a_n/x_n, b/y]$.
3. Let M_f be the expansion of M by f, where $[\![f]\!](a_1, \dots, a_n) = b$.
4. By 2, given $(a_1, \dots, a_n) \in M_f^n$, $M_f \vDash \psi[a_1/x_1, \dots, a_n/x_n, f(a_1, \dots, a_n)/y]$
5. Hence $M_f \vDash \forall x_1 \dots x_n \ \psi(x_1, \dots, x_n, f(x_1, \dots, x_n))$

Thus, if $M \vDash \varphi$, then $M_f \vDash \varphi_S$.

3.4. Completeness

Definition 3.39. A **Herbrand structure** for L is a structure M for which

1. M is the set of closed terms of L
2. $[\![f]\!](t_1, \dots, t_n) = f(t_1, \dots, t_n)$

- There is no provision as to how to interpret relation symbols in a Herbrand structure
- If t is a closed term and v a valuation then $v(t) = t$ does not depend on v. For this reason we write $[\![t]\!]$ to indicate the constant value in M.

Example Suppose the function symbols of L are the constants a and b and a binary function symbol f. Then the support of any Herbrand L-structure is

$$M = \{a, b, f(a, a), f(a, b), f(b, b), f(f(a, a), a), f(f(a, a), b), f(f(a, b), a), \dots\}$$

The interpretation of the function symbols is

$$[\![a]\!] = a, \quad [\![b]\!] = b, \quad [\![f]\!](t_1, t_2) = f(t_1, t_2).$$

For example, $[\![f]\!](a, f(a, b)) = f(a, f(a, b))$.

Definition 3.40. A **Hintikka set** is a set of closed formulas $H \subseteq L$ satisfying the following conditions:

1. If φ is atomic and $\varphi \in H$ then $\neg\varphi \notin H$.
2. $\bot, \neg\top \notin H$.
3. If $\neg\neg\varphi \in H$, then $\varphi \in H$.
4. If $\alpha \in H$, then $\alpha_1, \alpha_2 \in H$.
5. If $\beta \in H$, then $\beta_1 \in H$ or $\beta_2 \in H$.
6. If $\gamma \in H$, then $\gamma(t) \in H$ for every closed term t.
7. If $\delta \in H$, then $\delta(t) \in H$ for some closed term t.

Lemma 3.41. Assume L has closed terms. If H is Hintikka for L, then H has a Herbrand model.

Proof. Let M be the Herbrand L-structure in which relation symbols are interpreted as follows:

$$(t_1, \ldots, t_n) \in [\![R]\!] \Leftrightarrow R(t_1, \ldots, t_n) \in H$$

We prove by structural induction that $\varphi \in H \Rightarrow M \models \varphi$.

1. Atomic formulas. if $R(t_1, \ldots, t_n) \in H$ then the t_i's must be closed because H consists of closed formulas; thus, $(t_1, \ldots, t_n) \in [\![R]\!]$ by definition and $M \models R(t_1, \ldots, t_n)$.
2. Connectives. As in the propositional case.
3. γ-formulas. Suppose $\gamma(t) \in H \Rightarrow M \models \gamma(t)$ for every closed term t and suppose $\gamma \in H$. Then $\gamma(t) \in H$ for every closed term t, because H is Hintikka. By the inductive hypothesis, $M \models \gamma(t)$ for every closed t. Since M is Herbrand and contains only closed terms, $M \models \gamma$.
4. δ-formulas. Suppose $\delta(t) \in H \Rightarrow M \models \delta(t)$ for every closed term t and suppose $\delta \in H$. Then $\delta(t) \in H$ for some closed term t, because H is Hintikka. By the inductive hypothesis, $M \models \delta(t)$. Since M is Herbrand, $t \in M$ and therefore $M \models \delta$.

Parameters

Definition 3.42. If L is a first order language and P is an infinite set of constant symbols not appearing in L, we write L_P for the expansion of L by P and call the elements of P **parameters**.

A function $\pi : P \to P$ is called a **parameter substitution** and can be extend to a function $\pi : L_P \to L_P$ setting $\varphi\pi := \varphi[p\pi/p]$

Definition 3.43. A **consistency class** for L is a set C of subsets $S \subseteq L_P$ of closed formulas such that:

1. $\bot, \neg\top \notin S$.
2. if $\varphi \in S \in C$ is atomic, then $\neg\varphi \notin S$
3. If $\neg\neg\varphi \in S$, then $S \cup \{\varphi\} \in C$.
4. If $\alpha \in S$ is a conjunctive formula, then $S \cup \{\alpha_1, \alpha_2\} \in C$.
5. If $\beta \in S$ is a disjunctive formula, then $S \cup \{\beta_1\} \in C$ or $S \cup \{\beta_2\} \in C$.
6. If $\gamma \in S$ then $S \cup \{\gamma(t)\} \in C$ for every closed term of L_P.
7. If $\delta \in S$ then $S \cup \{\delta(p)\} \in C$ for some parameter $p \in P$.

A consistency class is **stable** if condition 6 is replaced by

8. If $\delta \in S$ then $S \cup \{\delta(p)\} \in C$ for every parameter $p \in P$ not appearing in S.

Extending consistency classes

1. Every consistency class C is contained in a downward closed consistency class D: declare that $T \in D \Leftrightarrow T \subseteq S \in C$ for some S.
2. However not every downward closed consistency class D is contained in a locally finite consistency class E. For setting $U \in E \Leftrightarrow T \in D$ for all finite $T \subseteq U$ (which is the only possible definition) does not satisfy condition 7. For suppose $\delta \in U \in E$; if p is a parameter and $V \subseteq U \cup \{\delta(p)\}$ is finite, then $V \subseteq W \cup \{\delta(p)\}$ where $W \subseteq U$ is finite and contains δ. Now $W \in D$ and since D is a consistency class, $W \cup \{\delta(q)\} \in D$ for some parameter q; if $q = p$ we would then have that $V \in D$, because D is downward closed; however, there is no guarantee that the condition $p = q$ is fulfilled.
3. Every consistency class C which is subset closed is contained in a stable consistency class C' which is subset closed: declare that $S \in C' \Leftrightarrow S\pi \in C$ for some parameter substitution π.
4. Every stable consistency class which is subset closed is contained in a stable consistency class which is locally finite.

Theorem 3.44. If C is a consistency class for L and $S \in C$ is a set of sentences of L, then S is satisfiable.

Proof. By the previous remark, we may assume that C is a locally finite, stable class. If $\{\varphi_0, \varphi_1, \ldots\}$ is the set of sentencesof L_P, construct a sequence $S_0 \subseteq S_1 \subseteq \ldots$ of elements of C as follows.

1. $S_0 = S$
2. $S_{i+1} = \begin{cases} S_i & \text{if } S_i \cup \{\varphi_i\} \notin C \\ S_i \cup \{\varphi_i\} & \text{if } S_i \cup \{\varphi_i\} \in C \text{ and } \varphi_i \text{ is not a } \delta\text{-formula} \\ S_i \cup \{\varphi_i\} \cup \{\delta(p)\} & \text{if } S_i \cup \{\varphi_i\} \in C \text{ and } \varphi_i = \delta \text{ and } p \in P \setminus (S_i \cup \{\varphi_i\}) \end{cases}$
3. If i is a limit ordinal, then $S_i = \bigcup S_j : j < i$.

Set $H = \bigcup S_i$. Then

1. $H \in C$
2. H is maximal in C
3. H is Hintikka w.r.t. L_P

By Hintikka's lemma, $S \subseteq H$ is satisfiable in a Herbrand model for L_P. □

3.5. Resolution

The resolution calculus

Recall that for resolution we write $\psi = \psi_1 \vee \ldots \vee \psi_n = \{\psi_1, \ldots, \psi_n\}$.

Definition 3.45. The following are the derivation rules for the resolution calculus.

$\dfrac{\varphi \in \Gamma}{\varphi}$	Assumption	$\dfrac{\bot \in \varphi}{\varphi \setminus \{\bot\}}$	Falsehood
$\dfrac{\alpha \in \varphi}{\varphi \setminus \{\alpha\} \cup \{\alpha_i\}}$	α-rule	$\dfrac{\beta \in \varphi}{\varphi \setminus \{\beta\} \cup \{\beta_1, \beta_2\}}$	β-rule
$\dfrac{\neg\neg\psi \in \varphi}{\varphi \setminus \{\neg\neg\psi\} \cup \{\psi\}}$	Negation	$\dfrac{\psi \in \varphi_1, \quad \neg\psi \in \varphi_2}{(\varphi_1 \setminus \{\psi\}) \cup (\varphi_2 \setminus \{\neg\psi\})}$	Resolution
$\dfrac{\gamma}{\gamma(t)}$	γ-rule	$\dfrac{\delta}{\delta(p)}$	δ-rule

where $t \in L_P$ is a closed term and p is a new parameter.

Resolution, an example

We prove that $\forall x(Rx \vee Sx) \vdash \exists x Rx \vee \forall x.Sx$ by showing that $\{\forall x(Rx \vee Sx), \ \neg(\exists x Rx \vee \forall x.Sx)\}$ has a closed expansion.

Step	Formula	Reason
1	$\{\forall x(Rx \vee Sx)\}$	assumption
2	$\{\neg(\exists x Rx \vee \forall x.Sx)\}$	assumption
3	$\{\neg\exists x Rx\}$	2, α-rule
4	$\{\neg\forall x.Sx\}$	2, α-rule
5	$\{\neg Sc\}$	4, δ-rule
6	$\{\neg Rc\}$	3, γ-rule
7	$\{Rc \vee Sc\}$	1, γ-rule
8	$\{Rc, Sc\}$	7, β-rule
9	$\{Sc\}$	8, 6, resolution
10	$\varnothing$	9, 5, resolution

> Theorem 3.46. The resolution calculus is sound.

We show that γ and δ rules preserve satisfiability of (closed) formulas.

1. Suppose $M \models \gamma$. Since t is closed, there exists $c \in M$ such that $v(t) = c$ for all valuations $v : X \to M$. Observe first that

$$v \models \gamma(t) \Leftrightarrow v \models \gamma[t/x] \Leftrightarrow v[c/x] \models \gamma(x)\,.$$

Then

$$\begin{aligned} M \models \gamma &\Rightarrow M \models \forall x.\gamma(x) \\ &\Rightarrow \text{for all valuations } v : X \to M,\ v \models \forall x.\gamma(x) \\ &\Rightarrow \text{for all valuations } v : X \to M \text{ and all } a \in M,\ v[a/x] \models \gamma(x) \\ &\Rightarrow \text{for all valuations } v : X \to M,\ v[c/x] \models \gamma(x) \\ &\Rightarrow \text{for all valuations } v : X \to M,\ v \models \gamma(t) \\ &\Rightarrow M \models \gamma(t) \end{aligned}$$

Soundness (continued)

2. Observe that since p does not appear in δ, we do not need to interpret it yet.

$$\begin{aligned} M \vDash \delta \Rightarrow M \vDash \exists x.\delta(x) & \\ &\Rightarrow \text{there exists a valuation } v : X \to M,\ v \vDash \exists x.\delta(x) \\ &\Rightarrow \text{there exists a valuation } u : X \to M,\ u \vDash \delta(x) \end{aligned}$$

where u is an x-variant of v. Define the expansion M_p of M setting $[\![p]\!] := u(x)$. Then

$$\begin{aligned} &\Rightarrow \text{there exists a valuation } u : X \to M_p,\ u \vDash \delta(x) \\ &\Rightarrow \text{there exists a valuation } u : X \to M_p,\ u \vDash \delta(p) \\ &\Rightarrow M_p \vDash \delta(p) \end{aligned}$$

Since all rules are sound,

$$\begin{aligned} F \vdash \varphi \Rightarrow \bot \in \mathrm{Res}(F \cup \{\neg\varphi\}) \Rightarrow \forall v \in M^X.\ v \nvDash \mathrm{Res}(F \cup \{\neg\varphi\}) \\ \Rightarrow \forall v \in M^X.\ v \nvDash F \cup \{\neg\varphi\} \Rightarrow F \cup \{\neg\varphi\} \vDash \bot \Rightarrow F \vDash \varphi \end{aligned}$$

> Lemma 3.47. The class C consisting of finite sets $S \subseteq L_P$ of sentences which have no closed resolution expansion is a consistency class.

We only need to add the proof for γ and δ-rules

Step	Claim	Reason
1	$\gamma \in S$	assumption
2	$\exists t. S \cup \{\gamma(t)\} \notin C$	assumption
3	$\exists t. \bot \in \mathrm{Res}(S \cup \{\gamma(t)\})$	2
4	$\forall t. \{\gamma(t)\} \in \mathrm{Res}(S)$	1
5	$\bot \in \mathrm{Res}(S)$	3, 4
6	$S \notin C$	5

Step	Claim	Reason
1	$\delta \in S$	assumption
2	$\forall p. S \cup \{\delta(p)\} \notin C$	assumption
3	$\forall p. \bot \in \mathrm{Res}(S \cup \{\delta(p)\})$	2
4	$\exists p. \{\delta(p)\} \in \mathrm{Res}(S)$	1
5	$\bot \in \mathrm{Res}(S)$	3, 4
6	$S \notin C$	5

Thus,

$$\gamma \in S \in C \Rightarrow \forall t S \cup \{\gamma(t)\} \in C, \qquad \delta \in S \in C \Rightarrow \exists p. S \cup \{\delta(p)\} \in C$$

Completeness (continued)

Corollary 3.48. The resolution calculus is complete, i.e.

$$F \vDash \varphi \Rightarrow F \vdash \varphi.$$

□

- By the lemma and PL, consistent sets forms a consistency class
- Therefore every consistent set is satisfiable
- Therefore the inference is complete

Unification

A **literal** is either an atomic formula or the negation of an atomic formula

Definition 3.49. A set E of literals is **unifiable** if there exists a substitution s such that Es has a single element; s is called a **unifier** for E. A **most general unifier** for E is a unifier u such that for every unifier s of E there exists a substitution t such that $s = ut$.

Theorem 3.50. Let E be a finite set of literals. Define recursively two sequences $\{E_n\}$ of sets of literals and $\{s_n\}$ of substitutions as follows:

1. $E_0 = E$ and $s_0 = \varnothing$.
2. If E_n contains at least two distinct literals L_i and L_j, then there exists a smallest natural number n such that the n-th symbols of L_i and L_j are different. If one of the two symbols is a variable x and the other is the first symbol of a term t not containing x, then set $s_{n+1} := [t/x]$ and $E_{n+1} := E_n[t/x]$.

If there exists an index k such that E_k is a singleton then E is unifiable and a most general unifier is

$$s = \prod_{i=1}^{k} s_i,$$

otherwise E is not unifiable.

Unification, example 1

The following set of literal is not unifiable.

$$E = \{R(f(g(a)), a, b), R(f(y), a, z), R(f(g(x)), a, x)\}.$$

We form the sequence of the Robinson theorem:

Substitution	Set
	$E_0 = \{R(f(g(a)), a, b), R(f(y), a, z), R(f(g(x)), a, x)\}$
$s_1 = [g(a)/y]$	$E_1 = \{R(f(g(a)), a, b), R(f(g(a)), a, z), R(f(g(x)), a, x)\}$
$s_2 := [b/z]$	$E_2 = \{R(f(g(a)), a, b), R(f(g(x)), a, x)\}$
$s_3 := [a/x]$	$E_3 = \{R(f(g(a)), a, b), R(f(g(a)), a, a)\}$

1. at stage 0, L_1 and L_2 differ at $n = 7$ where L_2 has y and L_1 has the first symbol of $g(a)$ which does not contain y.
2. at stage 1, L_1 and L_2 differ at $n = 13$, where L_2 has z and L_1 has b which does not contain z.
3. at stage 2, L_1 and L_2 differ at $n = 7$ where L_2 has x and L_1 has a
4. at stage 3, L_1 and L_2 differ at $n = 13$; this time, however, none of them has a variable in that position.

Unification, example 2

The set

$$E = \{P(x, y),\ P(x, f(y))\}\,.$$

can not be unified: the two literals differ at $n = 5$ where L_1 has a variable y and L_2 has the first symbol of the term $f(y)$. Since the term contains the variable the algorithm stops and E can not be unified.

Unification, example 3

The set $E = \{P(g(y), f(x, h(x), y)),\ P(x, f(g(z), w, z))\}$ can be unified:

Substitution	**Set**
	$E_0 = \{P(g(y), f(x, h(x), y)),\ P(x, f(g(z), w, z))\}$
$s_1 = [g(y)/x]$	$E_1 = \{P(g(y), f(g(y), h(g(y)), y),\ P(g(y), f(g(z), w, z))\}$
$s_2 := [y/z]$	$E_2 = \{P(g(y), f(g(y), h(g(y)), y),\ P(g(y), f(g(y), w, y))\}$
$s_3 := [h(g(y))/w]$	$E_3 = \{P(g(y), f(g(y), h(g(y)), y)\}$

A most general unifier is

$$u = s_1 s_2 s_3 = [g(y)/x, y/z, h(g(y))/w].$$

Resolution with unification

Definition 3.51. A formula φ is in **Skolem normal form** if it is a closed universal formula of type $\forall x_1 \ldots x_n.\psi$ where ψ is open (i.e. quantifier free) and in conjunctive normal form, i.e. a conjunction of disjunctions of literals. We write $C(\varphi)$ to indicate the set of clauses of ψ.

Notice that $C(\varphi)$ determines φ up to equivalence; therefore we do not distinguish between φ and $C(\varphi)$. The resolution calculus can be generalized adding the following inference rule:

Definition 3.52. Let C_1 and C_2 be two clauses with no common variables. Suppose there exist subsets $E_1 \subseteq C_1$ and $E_2 \subseteq C_2$ such that $E = \bar{E}_1 \cup E_2$ can be unified. If u is a most general unifier of E, then we can derive from C_1 and C_2 the **resolvent**

$$R := [(C_1 \setminus E_1) \cup (C_2 \setminus E_2)]\, u$$

The assumption that C_1 and C_2 have no variables in common is not restrictive: if they do, we can find substitutions s_1 and s_2 such that $C_1 s_1$ and $C_2 s_2$ have no common variables.

Resolution with unification, example

Consider the two clauses

$$C_1 = \{Q(x,y), P(f(x),y)\}, \qquad C_2 = \{R(x,c), \neg P(f(c),x), \neg P(f(y),h(z))\}\,.$$

Since the clauses have common variables, we redefine the first clause setting

$$C_1 := C_1[u/x, v/y] = \{Q(u,v), P(f(u),v)\}\,.$$

If we now let $E_1 = \{P(f(u),v)\} \subseteq C_1$ and $E_2 = \{\neg P(f(c),x), \neg P(f(y),h(z))\} \subseteq C_2$, then the set

$$E = E_1 \cup \bar{E}_2 = \{P(f(u),v), P(f(c),x), P(f(y),h(z))\}$$

is unifiable with a most general unifier $u = [c/u, c/y, h(z)/v, h(z)/x]$. A resolvent for C_1 and C_2 is therefore

$$R = \{Q(u,v), R(x,c)\}\,u = \{Q(c,h(z)), R(h(z),c)\}$$

Resolution with unification, example for consequence

We prove that $\forall x(Rx \vee Sx) \vdash \exists x.Rx \vee \forall x.Sx$. First we obtain the clausal form

$$\forall x(Rx \vee Sx) \equiv \{\{Rx, Sx\}\}$$

$$\neg(\exists x.Rx \vee \forall x.Sx) \equiv \forall x.\neg Rx \wedge \exists x.\neg Sx \equiv \exists y \forall x(\neg Rx \wedge \neg Sy) \equiv \forall x(\neg Rx \wedge \neg Sc) \equiv \{\{\neg Rx\}, \{\neg Sc\}\}$$

Then we derive the empty clause

Step	Clause	Rule
1	$\{Rx, Sx\}$	assumption
2	$\{\neg Rx\}$	assumption
3	$\{\neg Sc\}$	assumption
4	$\{Sx\}$	1, 2, resolution
5	$\varnothing$	3, 4, resolution

3.6. The Hilbert calculus

The Hilbert calculus

Definition 3.53. The following are the axiom schemes of the Hilbert calculus:

1. $\varphi \to (\chi \to \varphi)$
2. $(\varphi \to (\chi \to \psi)) \to ((\varphi \to \chi) \to (\varphi \to \psi))$
3. $\bot \to \varphi$
4. $\varphi \to \top$
5. $\neg\neg\varphi \to \varphi$
6. $\varphi \to (\neg\varphi \to \chi)$
7. $\alpha \to \alpha_i$
8. $(\beta_1 \to \varphi) \to ((\beta_2 \to \varphi) \to (\beta \to \varphi))$
9. $\gamma \to \gamma(t)$

where t is a closed term of L_P. The inference rules of the calculus are modus ponens and **generalization**:

$$\frac{\varphi \qquad \varphi \to \chi}{\chi} \qquad\qquad \frac{\varphi \to \gamma(p)}{\varphi \to \gamma}$$

where p does not occur neither in φ nor in γ.

Hilbert calculus, an example

We prove that

$$\vdash \forall x(Rx \wedge Sx) \rightarrow \forall x.Rx$$

is a theorem of the Hilbert calculus.

Step	Formula	Reason
1	$\forall x(Rx \wedge Sx) \rightarrow (Rp \wedge Sp)$	axiom scheme 9
2	$(Rp \wedge Sp) \rightarrow Rp$	propositional Hilbert calculus
3	$\forall x(Rx \wedge Sx) \rightarrow Rp$	1, 2, propositional Hilbert calculus
4	$\forall x(Rx \wedge Sx) \rightarrow \forall x.Rx$	3, generalization

A variation on generalization

The generalization inference rule can be replaced by the simpler version

$$\frac{\gamma(p)}{\gamma}$$

where p can not occur in the premises of the derivation.

	Statement	Reason
1.	$\gamma(p)$	hypothesis
2.	$\gamma(p) \to (\top \to \gamma(p))$	axiom scheme 1
3.	$\top \to \gamma(p)$	1, 2, MP
4.	$\top \to \gamma$	3, generalization
5.	$\top$	Hilbert calculus in PL
6.	γ	4, 5, MP

	Statement	Reason
1.	$\varphi \to \gamma(p)$	hypothesis
2.	$\gamma(p) \to \gamma$	theorem
3.	$\varphi \to \gamma$	1, 2, PL

Weak generalization yields a new derivation rule: if $\Gamma \vdash \varphi(p)$, then $\Gamma \vdash \varphi$ if p does not occur in Γ and φ.

Theorem 3.54. (Deduction theorem) Assume L is a first order language, $\Gamma \subseteq L$ is a set of formulas and $\varphi, \psi \in L$ are formulas. Then

$$\Gamma, \varphi \vdash \chi \Leftrightarrow \Gamma \vdash \varphi \to \chi$$

Proof. We only need to prove that the claim applies to generalization. Suppose $(\chi_1, \dots, \chi_n)$ is a derivation of $\Gamma, \varphi \vdash \chi$ and χ_n comes from χ_i, with $i < n$, by generalization (we are using the weak version of generalization, here). This means that $\chi_n = \gamma$ and $\chi_i = \gamma(p)$. We proceed as follows:

Step	Statement	Reason
1	$\Gamma \vdash \varphi \to \gamma(p)$	induction hypothesis
2	$\Gamma \vdash \varphi \to \gamma$	generalization

Deduction theorem, example

We prove that

$$\forall x(Px \to Qx) \to (\forall x.Px \to \forall x.Qx)$$

is a theorem of the Hilbert calculus. We can use the deduction theorem and prove instead that

$$\forall x(Px \to Qx), \forall x.Px \vdash \forall x.Qx$$

The proof is as follows:

Step	Statement	Reason
1	$\forall x(Px \to Qx)$	assumption
2	$Pp \to Qp$	1, axiom scheme 9, MP
3	$\forall x.Px$	assumption
4	Pp	2, axiom scheme 9, MP
5	Qp	2, 4, MP
6	$\forall x.Qx$	5, generalization

Soundness

Theorem 3.55. (Soundness) Assume L is a first order language, $\Gamma \subseteq L$ and $\varphi \in L$ is a formula. Then $\Gamma \vdash \varphi \Rightarrow \Gamma \vDash \varphi$

Proof. We prove that axiom 9 is sound

1.	$v \vDash \forall x.\varphi$	assumption
2.	$v[a/x] \vDash \varphi$ for all $a \in M$	1, $\forall$ semantics
3.	$v[v(t)/x] \vDash \varphi$	2, specialization
4.	$v \vDash \varphi[t/x]$	3, proposition 3.21

Generalization is sound: suppose $\vDash \gamma(p)$. If v is a valuation in M and $a \in M$, construct the structure N which only differs from M for $[\![p]\!] = a$. Then $v[a/x] \vDash \gamma(x)$ in N and hence in M. Since a is arbitrary, $v \vDash \forall x.\gamma(x)$. $\square$

Consistency for the Hilbert calculus

Lemma 3.56. If L is a propositional language. For any formula $\varphi \in L$, the class

$$C_\varphi := \{S \subseteq L : S \nvdash_H \varphi\}$$

of sets from which φ is not derivable in the Hilbert calculus is a consistency class.

Assume $S \in C_\varphi$

1. If $x, \neg x \in S$ we obtain a contradiction as follows:

	Statement	Reason
1.	$S \vdash x$	assumption
2.	$S \vdash \neg x$	assumption
3.	$S \vdash x \to (\neg x \to \varphi)$	axiom 6
4.	$S \vdash \neg x \to \varphi$	1, 3, modus ponens
5.	$S \vdash \varphi$	2, 4, modus ponens

Consistency for the Hilbert calculus (continued)

2. If $\bot \in S$ or $\neg\top \in S$, we obtain contradictions

	Statement	Reason
1.	$S \vdash \bot$	assumption
2.	$S \vdash \bot \to \varphi$	axiom 3
3.	$S \vdash \varphi$	1, 2, MP

	Statement	Reason
1.	$S \vdash \neg\top$	assumption
2.	$S \vdash \neg\top \to \top$	axiom 4
3.	$S \vdash \top$	1, 2, MP
4.	$S \vdash \top \to (\neg\top \to \varphi)$	axiom 6
5.	$S \vdash \neg\top \to \varphi$	3, 4, MP
6.	$S \vdash \varphi$	1, 5, MP

Consistency for the Hilbert calculus (continued)

3. If $\neg\neg\psi \in S$ and $S \cup \{\psi\} \notin C_\varphi$, i.e. $S, \psi \vdash \varphi$, we obtain a contradiction

	Statement	Reason
1.	$S, \psi \vdash \varphi$	hypothesis
2.	$S \vdash \neg\neg\psi$	assumption
3.	$S \vdash \neg\neg\psi \to \psi$	axiom 5
4.	$S \vdash \psi$	2, 3, MP
5.	$S \vdash \psi \to \varphi$	1, deduction theorem
6.	$S \vdash \varphi$	4, 5, MP

Consistency for the Hilbert calculus (continued)

4. If $\alpha \in S$ and $S \cup \{\alpha_1, \alpha_2\} \notin C_\varphi$we obtain a contradiction.

	Statement	Reason
1.	$S, \alpha_1, \alpha_2 \vdash \varphi$	hypothesis
2.	$S \vdash \alpha_1 \rightarrow (\alpha_2 \rightarrow \varphi)$	1, DT
3.	$S \vdash \alpha$	assumption
4.	$S \vdash \alpha \rightarrow \alpha_i$	axiom 7
5.	$S \vdash \alpha_i$	3, 4, MP
6.	$S \vdash \varphi$	2, 5, MP

Consistency for the Hilbert calculus (continued)

5. If $\beta \in S$ but $S \cup \{\beta_i\} \notin C_\varphi$we obtain a contradiction.

	Statement	Reason
1.	$S, \beta_i \vdash \varphi$	hypothesis
2.	$S \vdash \beta_i \to \varphi$	1, DT
3.	$S{\vdash}(\beta_1 \to \varphi) \to ((\beta_2 \to \varphi) \to (\beta \to \varphi))$	axiom
4.	$S \vdash \beta \to \varphi$	2, 3, MP
5.	$S \vdash \beta$	assumption
6.	$S \vdash \varphi$	4, 5, MP

Consistency for the Hilbert calculus (continued)

6. Suppose $\gamma \in S$ and $S \cup \gamma(t) \notin C_\varphi$ for some t; then $S \cup \gamma(t) \vdash \varphi$ and we obtain the contradiction $S \vdash \varphi$ as follows.

	Statement	Reason
1.	$S \vdash \gamma$	assumption
2.	$S \vdash \gamma \to \gamma(t)$	axiom 9, weakening
3.	$S \vdash \gamma(t)$	1, 2, MP
4.	$S, \gamma(t) \vdash \varphi$	hypothesis
5.	$S \vdash \gamma(t) \to \varphi$	4, deduction theorem
6.	$S \vdash \varphi$	3, 5, MP

7. Suppose $\delta \in S$ and $S \cup \delta(p) \notin C_\varphi$ for every p; then $S \cup \delta(p) \vdash \varphi$ and we obtain the contradiction $S \vdash \varphi$ as above (replace γ with δ and $\gamma(t)$ with $\delta(p)$.

A basic lemma

Lemma 3.57. The following formula is a theorem.

$$(\neg\varphi \to \varphi) \to \varphi$$

	Statement	Reason
1.	$(\neg\neg\varphi \to \varphi) \to ((\varphi \to \varphi) \to ((\neg\varphi \to \varphi) \to \varphi))$	axiom 8
2.	$\neg\neg\varphi \to \varphi$	axiom 5
3.	$(\varphi \to \varphi) \to ((\neg\varphi \to \varphi) \to \varphi)$	1, 2, MP
4.	$\varphi \to \varphi$	part 1
5.	$(\neg\varphi \to \varphi) \to \varphi$	3, 4, MP

Theorem 3.58. The Hilbert caculus is complete. That is, given $\mathit{\Gamma} \subseteq L$ and $\varphi \in L$ we have that

$$\mathit{\Gamma} \vDash \varphi \Rightarrow \mathit{\Gamma} \vdash \varphi.$$

Proof. We first prove that $\mathit{\Gamma} \in C_\varphi \Rightarrow \mathit{\Gamma} \cup \{\neg\varphi\} \in C_\varphi$. For suppose $\mathit{\Gamma} \cup \{\neg\varphi\} \notin C_\varphi$; we then obtain $\mathit{\Gamma} \notin C_\varphi$ as follows.

	Statement	Reason
1.	$\mathit{\Gamma}, \neg\varphi \vdash \varphi$	hypothesis
2.	$\mathit{\Gamma} \vdash \neg\varphi \to \varphi$	1, DT
3.	$\mathit{\Gamma} \vdash (\neg\varphi \to \varphi) \to \varphi$	lemma 3.57
4.	$\mathit{\Gamma} \vdash \varphi$	2, 3, MP

Suppose now that $\mathit{\Gamma} \nvdash \varphi$. Then $\mathit{\Gamma} \in C_\varphi$ and hence $\mathit{\Gamma} \cup \{\neg\varphi\} \in C_\varphi$. Thus $\mathit{\Gamma} \cup \{\neg\varphi\}$ is satisfiable and hence $\mathit{\Gamma} \nvDash \varphi$. $\square$