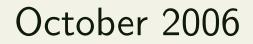
## Software specification in CASL -Logic

#### Till Mossakowski, Lutz Schröder





### Signatures (vocabularies)

- sort symbols s, t, Nat, List, Tree
- function symbols  $f: s \longrightarrow t$ , \_\_\_ + \_\_:  $Nat \times Nat \longrightarrow Nat$ , \_\_\_ + +\_\_:  $List \times List \longrightarrow List$
- predicate symbols p: t, \_\_\_  $\leq$  \_\_\_ :  $Nat \times Nat$

### Terms

Terms denote values, like natural numbers, data values, etc.



$$\phi ::= p(t_1, \dots, t_n)$$

$$| false \quad (\bot)$$

$$| true \quad (\top)$$

$$| not \phi \quad (\neg \phi)$$

$$| (\phi_1 \land \dots \land \phi_n)$$

$$| (\phi_1 \lor \dots \lor \phi_n)$$

$$| (\phi_1 \Rightarrow \phi_2)$$

$$| (\phi_1 \Leftrightarrow \phi_2)$$

$$| (\phi_1 \Leftrightarrow \phi_2)$$

$$| \forall x : s \cdot \phi$$

$$| \exists x : s \cdot \phi$$

### Formulas

application of predicate symbols contradiction always true negation conjunction disjunction implication equivalence universal quantification existential quantification

In single-sorted logic:  $\forall x . \phi$ ,  $\exists x . \phi$ .



### Free and bound variables

An occurrence of a variable in a formula that is not bound is said to be free.

$\exists y \ LeftOf(x,y)$	x is free, $y$ is bound
$ \begin{array}{c} (Cube(x) \land Small(x)) \\ \rightarrow \exists y \ LeftOf(x,y) \end{array} \end{array} $	x is free, $y$ is bound
$\exists x \ (Cube(x) \land Small(x))$	Both occurrences of $x$ are
	bound
$ (\exists x \ Cube(x)) \land Small(x) $	The first occurrence of $x$ is
	bound, the second one is
	free



### Models

- each sort is interpreted with a carrier set
- each function symbol is interpreted with a (set-theoretic) function
- each predicate symbol is interpreted with a (set-theoretic) relation (= subset of cartesian product)

### Variable valuations . . .

. . . are just maps from a set of variables into the carrier sets of a model. The sorting has to respected.



# Denotation of a term in a model w.r.t. a variable valuation

is defined inductively over the structure of the term

- the interpretation of a variable is determined by the variable valuation
- the intepretation of constant c is determined by the corresponing element of the carrier set
- the interpretation of  $f(t_1, \ldots, t_n)$  is the interpretation of f, applied to the interpretations of  $t_1, \ldots, t_n$



# Satisfaction of a formula in a model w.r.t. a variable valuation

- $p(t_1, \ldots, t_n)$  is satisfied iff the tuple formed by the interpretations of  $t_1, \ldots, t_n$  is element of the relation that is the interpretation of p
- the logical connectives are interpreted in the well-known way
- $\forall x:s. \phi$  is satisfied if for all valuations that may modify the given one on x,  $\phi$  is satisfied
- $\exists x:s. \phi$  is satisfied if for some valuation that may modify the given one on x,  $\phi$  is satisfied



### Satisfaction of a formula in a model

A formula is satisfied in a model iff it is satisfied for all valuations.

Notation:  $M \models \varphi$ .



### The axiomatic method

Try to capture the intended meaning of data sets, functions and predicates by specifying their properties using axioms (=formulas).

Axioms restrict the possible interpretation of sorts, functions and predicates.

Axioms may be used as premises within arguments/proofs.

A basic specification consists of a signature together with a collection of axioms.

### **Semantics of specifications**

- The (loose) semantics of a basic specification is the class of those models that satisfy all the specified formulas.
- A specification is said to be **consistent** when there are some models that satisfy all the formulas, and
- inconsistent when there are no such models.
- A formula is a logical consequence of a basic specification if it is satisfied in all the models of the specification.

### The four Aristotelian forms

All P's are Q's.  $\forall x(P(x) \rightarrow Q(x))$ Some P's are Q's.  $\exists x(P(x) \land Q(x))$ No P's are Q's.  $\forall x(P(x) \rightarrow \neg Q(x))$ Some P's are not Q's.  $\exists x(P(x) \land \neg Q(x))$ 

#### Note:

 $\forall x(P(x) \rightarrow Q(x)) \text{ does not imply that there are some } P's.$  $\exists x(P(x) \land Q(x)) \text{ does not imply that not all } P's \text{ are } Q's.$