First Order Predicate Logic

Formal Definitions and Specifications

Wolfgang Schreiner and Wolfgang Windsteiger
Wolfgang.(Schreiner|Windsteiger)@risc.jku.at

Research Institute for Symbolic Computation (RISC)
Johannes Kepler University (JKU), Linz, Austria
http://www.risc.jku.at

Defining and Specifying

Specifying problems and domains is a core activity of computer science.

- Goal: the adequate specification of a certain "problem" or "type".
  - A computation to be performed.
  - A domain of values to be represented.
  - Specification is to be expressed using the notions of some "model".
- Given: a "model", i.e., a collection of notions (functions/predicates).
  - For example, the model "set" with the usual set operations.
  - The interpretation of these notions is universally understood.
- Issue: the given model is not up to the task.
  - Its notions are on a too low level of abstraction.
  - The specification would become too cumbersome to write and too difficult to understand.

We need a model that is on an appropriate level of abstraction.

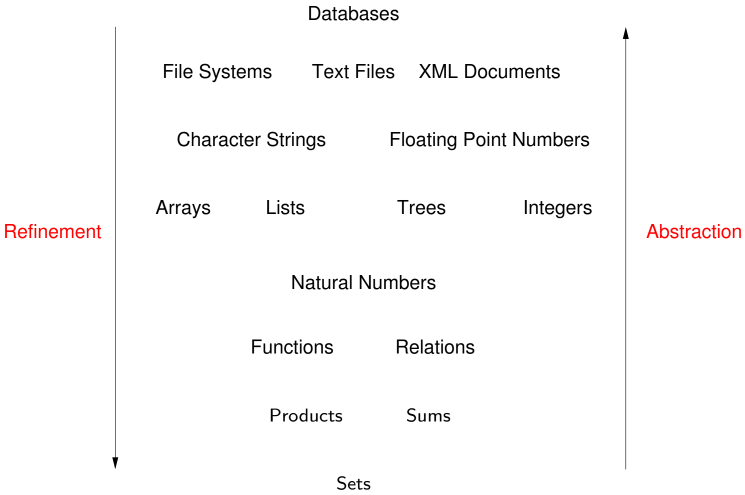
Refinement and Abstraction

How to overcome the gap between the given model and the intended one?

- Top-down (↓): refinement.
  - Start with the intended model.
  - Reduce its notions to lower-level notions.
  - Iterate, until the lowest level of the given notions is reached.
- Bottom-up (↑): abstraction.
  - Start with the given model.
  - Iteratively combine the given notions to higher-level notions.
  - Iterate, until the highest level of the intended notions is reached.
- Bottom-up and top-down (↕):
  - Combination of refinement and abstraction steps.
  - Iterate, until the refined notions "meet" the abstracted ones.

With the help of newly defined notions, problems and types may be adequately specified.

Illustration



Some Standard Models

- Products: $T_1 \times \ldots \times T_n$
  - Let $x_1 \in T_1, \ldots, x_n \in T_n, t \in T_1 \times \ldots \times T_n$.
  - Tuple construction: $(x_1, \ldots, x_n) \in T_1 \times \ldots \times T_n$.
  - Element selection: $t.1 \in T_1, \ldots, t.n \in T_n$ (or: $t_1 \in T_1, \ldots, t_n \in T_n$).
- Functions: $T_1 \times \ldots \times T_n \to T$
  - Let $x_1 \in T_1, \ldots, x_n \in T_n, f \in T_1 \times \ldots \times T_n \to T$.
  - Function definition: see later.
  - Function application: $f(x_1, \ldots, x_n) \in T$.
  - $domain(f) = T_1 \times \ldots \times T_n$, $range(f) \subseteq T$.
- Relations/Predicates: $\mathcal{P}(T_1 \times \ldots \times T_n)$

  $$\mathcal{P}(T) : \textit{the powerset (the set of all subsets) of } T.$$

  - Let $x_1 \in T_1, \ldots, x_n \in T_n, p \in \mathcal{P}(T_1 \times \ldots \times T_n)$ $(p \subseteq T_1 \times \ldots \times T_n)$.
  - Predicate definition: see later.
  - Predicate application: $p(x_1, \ldots, x_n)$ denotes a truth value.
  - $domain(p) = T_1 \times \ldots \times T_n$.

Can be reduced to set-theoretic notions.

Some Standard Models

- Infinite Sequences: $T^\omega = \mathbb{N} \to T$
  - Let $s \in T^\omega, i \in \mathbb{N}$.
  - Element access $s(i) \in T$ (or: $s_i \in T$).
- Sequences of Length n: $T^n = \mathbb{N}_n \to T$
  - Index domain: $\mathbb{N}_n = \{i \in \mathbb{N} \mid i < n\}$.
  - Let $s \in T^n, i \in \mathbb{N}_n$.
  - Element access: $s(i) \in T$ (or: $s_i \in T$).
- Finite Sequences: $T^* = \bigcup_{n \in \mathbb{N}} T^n$
  - Let $s \in T^*$, i.e., $s \in T^n$ for some $n \in \mathbb{N}$, let $i \in \mathbb{N}_n$.
  - Sequence length: $length(s) = n$.
  - Element access: $s(i) \in T$ (or: $s_i \in T$).

Sequences (arrays, lists, ...) of arbitrary length can be modeled as functions over an index domain.

Formal Definitions and Specifications

- Explicit Function Definitions.
- Explicit Predicate Definitions.
- Implicit Function Definitions.
- Proving with Definitions.
- Problem Specifications.

Explicit Function Definitions

A new function my be introduced by describing its value.

- An explicit function definition

  $$f : T_1 \times \ldots \times T_n \to T$$
  $$f(x_1, \ldots, x_n) := t$$

  consists of

  - a new n-ary function constant f,
  - a type signature $T_1 \times \ldots \times T_n \to T$ withs sets $T_1, \ldots, T_n, T$,
  - a list of variables $x_1, \ldots, x_n$ (the parameters), and
  - a term t (the body) whose free variables occur in $x_1, \ldots, x_n$;
  - case $n = 0$: the definition of a value constant $f : T, f := t$.

- We have to show for the newly introduced function f

  $$\forall x_1 \in T_1, \ldots, x_n \in T_n : t \in T$$

  and then know

  $$\forall x_1 \in T_1, \ldots, x_n \in T_n : f(x_1, \ldots, x_n) = t$$

The body of an explicit function definition may only refer to *previously* defined functions (no recursion).

Examples

$$sqrtsum : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$$
$$sqrtsum(x, y) := \sqrt{x} + \sqrt{y}$$

$$sumsquared : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$sumsquared(x, y) := \textbf{let } z = x + y \textbf{ in } z^2$$

$$sqrtsumsquared : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$$
$$sqrtsumsquared(x, y) := sqrtsum(x, y)^2$$

$$sqrtsumset : \mathbb{N} \to \mathcal{P}(\mathbb{R})$$
$$sqrtsumset(n) := \{sqrtsum(x, y) \mid x, y \in \mathbb{N} \wedge 1 \leq x, y \leq n\}$$

Explicit Predicate Definitions

A new predicate my be introduced by describing its truth value.

- An explicit predicate definition

$$p \subseteq T_1 \times \ldots \times T_n$$
$$p(x_1, \ldots, x_n) :\Leftrightarrow F$$

  consists of

  - a new n-ary predicate constant p,
  - a type signature $T_1 \times \ldots \times T_n$ with sets $T_1, \ldots, T_n$
  - a list of variables $x_1, \ldots, x_n$ (the parameters), and
  - a formula F (the body) whose free variables occur in $x_1, \ldots, x_n$.
  - case $n = 0$: definition of a truth value constant $p :\Leftrightarrow F$.

- We then know for the newly introduced predicate p:

$$\forall x_1 \in T_1, \ldots, x_n \in T_n : p(x_1, \ldots, x_n) \leftrightarrow F$$

The body of an explicit predicate definition may only refer to *previously* defined predicates (no recursion).

Examples

$$| \subseteq \mathbb{N} \times \mathbb{N}$$
$$x|y :\Leftrightarrow \exists z \in \mathbb{N} : x \cdot z = y$$

$$\mathit{isprime} \subseteq \mathbb{N}$$
$$\mathit{isprime}(x) :\Leftrightarrow x \geq 2 \land \forall y \in \mathbb{N} : 1 < y \land y < x \rightarrow \neg(y|x)$$

$$\mathit{isprimefactor} \subseteq \mathbb{N} \times \mathbb{N}$$
$$\mathit{isprimefactor}(p, n) :\Leftrightarrow \mathit{isprime}(p) \land p|n$$

Definitions with Side Conditions

- A definition may occur in the context of a side condition.

  Let $x_1 \in T_1, \ldots, x_n \in T_n$ *be such that* $c(x_1, \ldots, x_n)$*. We define*

$$f(x_1, \ldots, x_n) := t$$
$$p(x_1, \ldots, x_n) :\Leftrightarrow F$$

- We then know for the newly introduced function/predicate

$$\forall x_1 \in T_1, \ldots, x_n \in T_n : c(x_1, \ldots, x_n) \rightarrow f(x_1, \ldots, x_n) = t$$
$$\forall x_1 \in T_1, \ldots, x_n \in T_n : c(x_1, \ldots, x_n) \rightarrow (p(x_1, \ldots, x_n) \leftrightarrow F)$$

Applications of the function/predicate to arguments that violate the side condition are meaningless.

Implicit Function Definitions

We may also introduce a new function by describing what condition its result must satisfy.

- An implicit function definition

$$
\begin{aligned}
&f : T_1 \times \ldots \times T_n \to T \\
&f(x_1, \ldots, x_n) := \textbf{such } y : F
\end{aligned}
$$

  consists of
  - a new n-ary function constant f,
  - a type signature $T_1 \times \ldots \times T_n \to T$ withs sets $T_1, \ldots, T_n, T$,
  - a list of variables $x_1, \ldots, x_n$ (the parameters),
  - a variable y (the result variable),
  - a formula F (the result condition) whose free variables occur in $x_1, \ldots, x_n, y$.
- We then know for the newly introduced function f

$$
\begin{aligned}
&\forall x_1 \in T_1, \ldots, x_n \in T_n : \\
&\quad (\exists y \in T : F) \to (\exists y \in T : F \wedge y = f(x_1, \ldots, x_n))
\end{aligned}
$$

If there is some value that satisfies the result condition, the function result is one such value (otherwise, it is undefined).

Examples

$quotient : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ // undefined for n=0, otherwise unique

$quotient(m,n) :=$ **such** $q : \exists r \in \mathbb{N} : m = n \cdot q + r \wedge r < n$

$root : \mathbb{R} \to \mathbb{R}$ // defined for non-negative x, but not unique

$root(x) :=$ **such** $r : r^2 = x$

$someprimefactor : \mathbb{N} \to \mathbb{N}$ // may be undefined; if defined, may not be unique

$someprimefactor(n) :=$ **such** $p : isprimefactor(p,n)$

$maxprime : \mathbb{N} \to \mathbb{N}$ // may be undefined; if defined, it is unique

$maxprime(n) :=$ **such** $p : isprime(p) \wedge p \leq n \wedge$
$(\forall q \in \mathbb{N} : isprime(q) \wedge q \leq n \to q \leq p)$

The result of an implicitly specified function is not necessarily uniquely defined (and may be also completely undefined).

Implicit Unique Function Definitions

But sometimes the result is uniquely defined by an implicit definition.

- An implicit unique function definition

$$
\begin{aligned}
&f : T_1 \times \ldots \times T_n \rightarrow T\\
&f(x_1, \ldots, x_n) := \textbf{the } y : F
\end{aligned}
$$

  consists of the same elements as an unique function definition.

- We have to prove that the function result is defined and unique

$$
\begin{aligned}
&\forall x_1 \in T_1, \ldots, x_n \in T_n :\\
&\quad (\exists y \in T : F) \wedge\\
&\quad (\forall y_1 \in T, y_2 \in T : F[y_1/y] \wedge F[y_2/y] \rightarrow y_1 = y_2)
\end{aligned}
$$

  from which we know for the newly introduced function f

$$
\begin{aligned}
&\forall x_1 \in T_1, \ldots, x_n \in T_n :\\
&\quad (\exists y \in T : F \wedge y = f(x_1, \ldots, x_n)) \wedge\\
&\quad (\forall y \in T : F \rightarrow y = f(x_1, \ldots, x_n))
\end{aligned}
$$

The function result is the only value that satisfies the result condition.

Examples

$quot : \mathbb{R}_{\geq 0} \times \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ // defined and unique

$quot(a, b) :=$ **the** $q : a = b \cdot q$

$posroot : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ // defined and unique

$posroot(x) :=$ **the** $r : r^2 = x \wedge r \geq 0$

$minimum : \mathcal{P}(\mathbb{N}) \backslash \{\emptyset\} \to \mathbb{N}$ // defined and unique

$minimum(S) :=$ **the** $m : m \in S \wedge \forall m' \in S : m' \geq m$

Predicates versus Functions

A predicate gives also rise to functions.

- A predicate:

$$\begin{aligned} &\mathit{isprimefactor} \subseteq \mathbb{N} \times \mathbb{N} \\ &\mathit{isprimefactor}(p, n) :\Leftrightarrow \mathit{isprime}(p) \wedge p|n \end{aligned}$$

- An implicitly defined function:

$$\begin{aligned} &\mathit{someprimefactor} : \mathbb{N} \to \mathbb{N} \\ &\mathit{someprimefactor}(n) := \textbf{such } p : \mathit{isprime}(p) \wedge p|n \end{aligned}$$

- A function whose result is a set:

$$\begin{aligned} &\mathit{allprimefactors} : \mathbb{N} \to \mathcal{P}(\mathbb{N}) \\ &\mathit{allprimefactors}(n) := \{p \in \mathbb{N} \mid \mathit{isprime}(p) \wedge p|n\} \end{aligned}$$

The preferred style of definition is a matter of taste and purpose.

Informal Definitions

- Definition: A *tomcat* is a male cat.

$$tomcat(x) :\Leftrightarrow cat(x) \wedge male(x).$$

- Definition: Let x, y be positive integers. Then $gcd(x, y)$ denotes the greatest positive integer that divides both x and y.

$$gcd : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$$
$$gcd(x, y) := \textbf{the } z : z|x \wedge z|y \wedge \forall z' \in \mathbb{Z}_{>0} : z'|x \wedge z'|y \to z' \leq z$$

- Definition: A *prime factorization* of $n > 1$ is a product $p_1^{e_1} \cdots p_l^{e_l} = n$ with primes $p_1 < \ldots < p_l$ and exponents $e_i > 0$.

$$isPrimeFactorization \subseteq \mathbb{N} \times (\mathbb{N} \times \mathbb{N})^*$$
$$isPrimeFactorization(n, p) :\Leftrightarrow$$
$$\textbf{let } l = length(p) \textbf{ in}$$
$$n = \prod_{i=0}^{l-1} (p(i).1)^{(p(i).2)} \wedge$$
$$(\forall i \in \mathbb{N}_l : prime(p(i).1)) \wedge$$
$$(\forall i \in \mathbb{N}_{l-1} : p(i).1 < p(i+1).1)$$

It is important to recognize the formal content of informal definitions.

Proving with Definitions

- Given definitions

$$f : A \to B,\ f(x) := \ldots$$
$$p \subseteq A,\ p(x) :\Leftrightarrow \ldots$$
$$\ldots$$

we wish to prove some goal G which involves $f, p, \ldots$.

- We extract the knowledge provided by the definitions:

$$\forall x \in A : f(x) = \ldots \qquad (K_1)$$
$$\forall x \in A : p(x) \leftrightarrow \ldots \qquad (K_2)$$
$$\ldots$$

- We prove

$$(K_1), (K_2), \ldots \vdash G$$

The proof is performed with the knowledge provided by the definitions.

Example

If a divides b then it also divides every multiple of b.

Definition: a divides $b :\Leftrightarrow \exists t \in \mathbb{N} : b = t \cdot a$

Knowledge (K): $\forall a \in \mathbb{N}, b \in \mathbb{N} : a \text{ divides } b \leftrightarrow \exists t \in \mathbb{N} : b = t \cdot a$

$$\downarrow$$

$$(K) \vdash \forall a, b, s \in \mathbb{N} : a \text{ divides } b \rightarrow a \text{ divides } s \cdot b$$

P-$\forall$:

$$(K) \vdash \bar{a}, \bar{b}, \bar{s} \in \mathbb{N} \rightarrow (\bar{a} \text{ divides } \bar{b} \rightarrow \bar{a} \text{ divides } \bar{s} \cdot \bar{b})$$

P-$\rightarrow$:

$$(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N} \vdash \bar{a} \text{ divides } \bar{b} \rightarrow \bar{a} \text{ divides } \bar{s} \cdot \bar{b}$$

P-$\rightarrow$:

$$(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b} \vdash \bar{a} \text{ divides } \bar{s} \cdot \bar{b}$$

G-Def:

$$(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a}$$

A-Def:

$$(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \exists t \in \mathbb{N} : \bar{b} = t \cdot \bar{a} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a}$$

A-$\exists$, A-$\wedge$:

$$(K), \bar{a}, \bar{b}, \bar{s}, \bar{t} \in \mathbb{N}, \bar{b} = \bar{t} \cdot \bar{a} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a}$$

A-$=$:

$$(K), \bar{a}, \bar{b}, \bar{s}, \bar{t} \in \mathbb{N}, \bar{b} = \bar{t} \cdot \bar{a} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{t} \cdot \bar{a} = t \cdot \bar{a}$$

P-$\exists$:

$$(K), \bar{a}, \bar{b}, \bar{s}, \bar{t} \in \mathbb{N}, \bar{b} = \bar{t} \cdot \bar{a} \vdash \bar{s} \cdot \bar{t} \in \mathbb{N} \wedge \bar{s} \cdot \bar{t} \cdot \bar{a} = \bar{s} \cdot \bar{t} \cdot \bar{a}$$

P-$\wedge$:

$$\begin{array}{ll} (K), \ldots, \bar{s}, \bar{t} \in \mathbb{N} \vdash \bar{s} \cdot \bar{t} \in \mathbb{N} & (K), \ldots \vdash \bar{s} \cdot \bar{t} \cdot \bar{a} = \bar{s} \cdot \bar{t} \cdot \bar{a} \\ \text{ValidAssum:} & \text{P-=:} \\ \ldots \vdash \ldots & \\ \text{GoalAssum:} & \end{array}$$

Example: Explanation

- Derivation of G-Def:

$$
\begin{array}{rc}
 & (K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b} \vdash \bar{a} \text{ divides } \bar{s} \cdot \bar{b} \\
\text{A-}\forall\text{:} & \overline{(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b}, \bar{a} \text{ divides } \bar{s} \cdot \bar{b} \leftrightarrow \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a} \vdash \bar{a} \text{ divides } \bar{s} \cdot \bar{b}} \\
\text{A-}\leftrightarrow\text{:} & \overline{(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b}, \bar{a} \text{ divides } \bar{s} \cdot \bar{b} \leftrightarrow \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a}} \\
\text{AnyAssum:} & \overline{(K), \bar{a}, \bar{b}, \bar{s} \in \mathbb{N}, \bar{a} \text{ divides } \bar{b} \vdash \exists t \in \mathbb{N} : \bar{s} \cdot \bar{b} = t \cdot \bar{a}}
\end{array}
$$

- Analogous derivation of A-Def.

Definitions can be “expanded” in goal and knowledge.

Specifying Problems

An important role of logic in computer science is to specify problems.

- The specification of a (computational) problem

$$\textbf{Input: } x_1 \in T_1, \ldots, x_n \in T_n \quad \textbf{where } I$$
$$\textbf{Output: } y_1 \in U_1, \ldots, y_m \in U_m \ \textbf{where } O$$

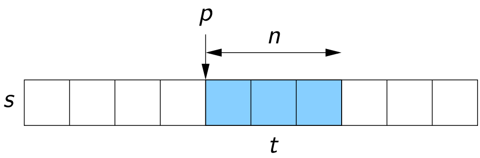
  consists of

  - a list of input variables $x_1, \ldots, x_n$ with types $T_1, \ldots, T_n$,
  - a formula I (the input condition) whose free variables occur in $x_1, \ldots, x_n$,
  - a list of output variables $y_1, \ldots, y_m$ with types $U_1, \ldots, U_m$, and
  - a formula O (the output condition) whose free variables occur in $x_1, \ldots, x_n, y_1, \ldots, y_m$.

The specification is expressed with the help of functions and predicates that have been previously defined to describe the problem domain.

Example

Extract from a finite sequence s of natural numbers a subsequence of length n starting at position p.



Input: $s \in \mathbb{N}^*, n \in \mathbb{N}, p \in \mathbb{N}$ **where**

$$n + p \leq length(s)$$

Output: $t \in \mathbb{N}^*$ **where**

$$length(t) = n \land$$
$$\forall i \in \mathbb{N}_n : t(i) = s(i + p)$$

The resulting sequence must have appropriate length and content.

Implementing Problem Specifications

The ultimate goal of computer science is to implement specifications.

- The specifications demands the definition of a function $f : T_1 \times \ldots \times T_n \to U_1 \times \ldots \times U_m$ such that

$$\forall x_1 \in T_1, \ldots, x_n \in T_n : I \to \\ \textbf{let } (y_1, \ldots, y_m) = f(x_1, \ldots, x_n) \textbf{ in } O$$

  - For all arguments $x_1, \ldots, x_n$ that satisfy the input condition,
  - the result $(y_1, \ldots, y_m)$ of f satisfies the output condition.
- The specification itself already implicitly defines such a function:

$$f(x_1, \ldots, x_n) := \textbf{such } y_1, \ldots, y_m : I \to O$$

- However, the specification is actually implemented only by an explicitly defined function (computer program).

  The correctness of the implementation with respect to the specification has to be verified (e.g. by a formal proof).

Our goal is to adequately specify informal problems, to implement formal specifications, and to verify the correctness of the implementations.

The Java Modeling Language (JML)

A language for specifying the contracts of Java functions.

```
/*@ requires s != null && 0 <= p && 0 <= n && p+n <= s.length;
  @ ensures  \result != null && \result.length == n &&
  @          (\forall int i; 0 <= i && i < n;
  @             \result[i] == s[i+p]);
  @*/
/*@ pure @*/ static int[] subarray(int[] s, int p, int n) {
  int[] t = new int[n];
  for (int i=0; i<n; i++)
    t[i] = s[i+p];
  return t;
}
```

The Java function implements the specified contract.