Foundations of Programming Languages and Software Engineering

Jan-Georg Smaus (Peter Thiemann)

Universität Freiburg

July 2011

Overview

- Basics
  - Relations
  - Induction
- Terms and All That
  - Syntax
  - Semantics

Binary Relations

Definition

- A binary relation on sets M_1 and M_2 is a set $R \subseteq M_1 \times M_2$ of pairs of elements from M_1 and M_2, respectively. If $M_1 = M_2 = M$, we simply call R a binary relation on M.
- We say that $m_1 \in M_1$ and $m_2 \in M_2$ are related by R iff $(m_1, m_2) \in R$.
- We often write $m_1 \; R \; m_2$ instead of $(m_1, m_2) \in R$.

Properties of Binary Relations (1)

Definition

Let R be a binary relation on M.

- R is reflexive iff $m \; R \; m$ for all $m \in M$.
- R is symmetric iff $m \; R \; m'$ implies $m' \; R \; m$.
- R is transitive iff $m_1 \; R \; m_2$ and $m_2 \; R \; m_3$ imply $m_1 \; R \; m_3$.
- R is an equivalence relation iff it is reflexive, symmetric, and transitive.

Properties of Binary Relations (2)

Definition

Let R be a binary relation on M.

- The reflexive closure of R is the smallest reflexive relation R' such that $R \subseteq R'$.
- The transitive closure of R is the smallest transitive relation R' such that $R \subseteq R'$. It is often written R^+.
- The reflexive and transitive closure of R is the smallest reflexive and transitive relation R' such that $R \subseteq R'$. It is often written R^*.

Induction Principles

Suppose P is some property on natural numbers.

Principle of ordinary induction on natural numbers

If $P(0)$	Base case
and, for all $i \in \mathbb{N}$, $P(i)$ implies $P(i+1)$,	Induction step
then $P(n)$ holds for all $n \in \mathbb{N}$.	Conclusion

The assumption "$P(i)$" in the induction step is called the induction hypothesis (IH for short).

Principle of complete induction on natural numbers

If, for each $n \in \mathbb{N}$,
given $P(i)$ for all $i < n$
we can show $P(n)$,
then $P(n)$ holds for all $n \in \mathbb{N}$.

Example

Lemma

For all $n \in \mathbb{N}$, $\Sigma_{i=1}^{n}(2i-1) = n^2$.

Proof. The proof is by ordinary induction on n.

- If $n = 0$, then both sides of the equation are 0.
- Suppose the lemma holds for some $k \in \mathbb{N}$. We then have:

$$\Sigma_{i=1}^{k+1}(2i-1) = \Sigma_{i=1}^{k}(2i-1) + (2(k+1)-1)$$
$$\overset{\text{(IH)}}{=} k^2 + 2k + 1$$
$$= (k+1)^2 \quad \square$$

Signatures

Definition

- A signature Σ is a set of function symbols, where each $f \in \Sigma$ is associated with a natural number n called the arity of f.
- $\Sigma^{(n)}$ denotes the set of all n-ary elements of Σ.
- The elements of $\Sigma^{(0)}$ are also called constant symbols.

Example

Signature Σ_{prop} for propositional logic

$$\Sigma_{prop} = \{\mathbf{T}^{(0)}, \mathbf{F}^{(0)}, \neg^{(1)}, \wedge^{(2)}, \vee^{(2)}\}$$
$$\Sigma_{prop}^{(0)} = \{\mathbf{T}, \mathbf{F}\}$$
$$\Sigma_{prop}^{(1)} = \{\neg\}$$
$$\Sigma_{prop}^{(2)} = \{\wedge, \vee\}$$

Terms

Definition

Let Σ be a signature and X a set of variables such that $\Sigma \cap X = \emptyset$. The set $T(\Sigma, X)$ of all Σ-terms over X is inductively defined as

- $X \subseteq T(\Sigma, X)$,
- for all $n \in \mathbb{N}$, all $f \in \Sigma^{(n)}$, and all $t_1, \ldots, t_n \in T(\Sigma, X)$, we have $f(t_1, \ldots, t_n) \in T(\Sigma, X)$

Note:

- For a constant symbol $f \in \Sigma^{(0)}$, we often write the term $f()$ as f.
- From now on, we leave the variable set $X = \{x, x_1, x_2, \ldots, y, y_1, y_2, \ldots, z, z_1, z_2 \ldots\}$ implicit

Example

Suppose $\Sigma = \Sigma_{prop}$. Then

$$\vee(\neg(x_{42}), \wedge(\mathbf{T}, x_3)) \in T(\Sigma, X)$$

Alternative notation

Infix notation (with implicit operator precedence order):
$\neg x_{42} \vee \mathbf{T} \wedge x_3$

Unique Decomposition of Terms

- In our current view, equality of terms means syntactic equality.
- Therefore, if $t, s \in T(\Sigma, X)$ and $t = f(t_1, \ldots, t_n)$ and $s = g(s_1, \ldots, s_m)$, and $t = s$, then $f = g$, $n = m$, and $t_i = s_i$ for all $i \in \{1, \ldots, n\}$.
- Later, we consider a kind of semantic equality: $+(1, 3)$ might be equal to $+(2, 2)$.

Positions and Size of Terms

Definition

Suppose $t \in T(\Sigma, X)$.

- The set of positions of term t is a set $Pos(t)$ of strings over the alphabet of natural numbers. It is inductively defined as follows:
  - If $t = x \in X$, then $Pos(t) := \{\epsilon\}$
  - If $t = f(t_1, ..., t_n)$, then

$$Pos(t) := \{\epsilon\} \cup \bigcup_{i=1}^{n} \{ip \mid p \in Pos(t_i)\}$$

- The position ϵ is called the root position of t, the function or variable at this position is called the root symbol of t.
- The size $|t|$ of t is the cardinality of $Pos(t)$.

Subterms and Replacing

Definition (Subterm)

For $p \in Pos(t)$, the subterm of t at position p, denoted by $t|_p$, is defined by induction on the length of p:

$$t|_\epsilon := t$$
$$f(t_1, \ldots, t_n)|_{ip} := t_i|_p$$

($ip \in Pos(t)$ implies that $t = f(t_1, \ldots, t_n)$ with $0 \leq i \leq n$.)

Definition (Replacing)

For $p \in Pos(t)$, we denote by $t[s]_p$ the term that is obtained from t by replacing the subterm at position p by s, i.e.

$$t[s]_\epsilon := s$$
$$f(t_1, \ldots, t_n)[s]_{ip} := f(t_1, ..., t_i[s]_p, \ldots, t_n)$$

Examples

Suppose $t = \vee(\neg(x_{42}), \wedge(\mathbf{T}, x_3))$

- $Pos(t) = \{\epsilon, 1, 12, 2, 21, 22\}$
- $|t| = 6$ (number of nodes in the tree)
- $t|_2 = \wedge(\mathbf{T}, x_3)$
- $t[\neg(\mathbf{F})]|_2 = \vee(\neg(x_{42}), \neg(\mathbf{F}))$

An Induction Principle for Terms

Term Induction

To prove that a property P holds for all $t \in T(\Sigma, X)$, we have to show the following properties:

- Base case
  $P(x)$ holds for all $x \in X$ and $P(f)$ holds for all $f \in \Sigma^{(0)}$.
- Induction step
  Suppose $n > 0$, $f \in \Sigma^{(n)}$, and $t_1, \ldots, t_n \in T(\Sigma, X)$.
  Then $P(f(t_1, \ldots, t_n))$ holds assuming $P(t_1), \ldots, P(t_n)$.

Example for Term Induction

Lemma

For all terms t, the set $Pos(t)$ is prefix closed, i.e. if $wv \in Pos(t)$ then $w \in Pos(t)$.

Substitutions

Definition

Let Σ be a signature.

- A $T(\Sigma, X)$-substitution is a function $\sigma : X \to T(\Sigma, X)$ such that $\sigma(x) \neq x$ for only finitely many xs.
- The domain of σ is $Dom(\sigma) := \{x \in X \mid \sigma(x) \neq x\}$.
- We write $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ for a substitution that maps x_i to t_i and has domain $Dom(\sigma) = \{x_1, \ldots, x_n\}$.
- A $T(\Sigma, X)$-substitution σ is extended to a mapping $\sigma : T(\Sigma, X) \to T(\Sigma, X)$ on arbitrary terms as follows: $\sigma(f(t_1, \ldots, t_n)) := f(\sigma(t_1), \ldots, \sigma(t_n))$

Substitutions. Explanation

Note

Applying the extension of a substitution σ to a term simultaneously replaces all occurrences of a variable by their respective σ-image.

Example

A substitution on terms from $T(\Sigma_{prop}, X)$

$$\begin{aligned} \Sigma &= \Sigma_{prop} \\ \sigma &= \{x \mapsto \neg z, y \mapsto x \vee \mathbf{F}\} \\ t &= x \vee y \wedge z \\ \sigma(t) &= \neg z \vee (x \vee \mathbf{F}) \wedge z \end{aligned}$$

Composing Substitutions

Definition

The composition $\sigma\tau$ of two substitutions σ and τ is defined as $\sigma\tau(x) := \sigma(\tau(x))$.

Lemma

Composition of substitutions is an associative operation where the identity substitution is the unit.

Σ-Algebras

Definition

Let Σ be a signature. A Σ-algebra $\mathcal{A} = (A, \mathcal{J})$ consists of

- a carrier set A, and
- an interpretation function $\mathcal{J}$ that associates with each function symbol $f \in \Sigma^{(n)}$ a function $\mathcal{J}(f) : A^n \to A$.

Example

The Σ_{prop}-Algebra $\mathcal{A}_{prop}$

$$\begin{aligned}
\mathcal{A}_{prop} &= (A_{prop}, \mathcal{J}_{prop}) \\
A_{prop} &= \{0, 1\} \\
\mathcal{J}_{prop}(\mathbf{F}) &= 0 \\
\mathcal{J}_{prop}(\mathbf{T}) &= 1 \\
\mathcal{J}_{prop}(\neg)(x) &= 1 - x \\
\mathcal{J}_{prop}(\vee)(x, y) &= \max(x, y) \\
\mathcal{J}_{prop}(\wedge)(x, y) &= \min(x, y)
\end{aligned}$$

Term Interpretation

Definition

Let $\mathcal{A} = (A, \mathcal{J})$ be a Σ-algebra.

- A variable assignment is a function $\alpha : X \to A$ that assigns every variable a value in the carrier set.
- Given a variable assignment α, the interpretation function $\mathcal{J}$ is extended to a function on terms, $\mathcal{J}_\alpha : T(\Sigma, X) \to A$, as follows:
$$\begin{aligned}
\mathcal{J}_\alpha(x) &= \alpha(x) && (x \in X) \\
\mathcal{J}_\alpha(f(t_1, \ldots, t_n)) &= \mathcal{J}(f)(\mathcal{J}_\alpha(t_1), \ldots, \mathcal{J}_\alpha(t_n))
\end{aligned}$$
- The restriction of $\mathcal{J}_\alpha$ to variable free-terms, $\mathcal{J}_\alpha : T(\Sigma, \emptyset) \to A$, is usually denoted by $\mathcal{J}$ since the α does not matter.

Example

Interpretation of $\vee(\neg(x_{42}), \wedge(\mathbf{T}, x_3)) \in T(\Sigma_{prop}, X)$

Suppose $\alpha : X \to A_{prop}$ is a function such that

$$\begin{aligned} \alpha(x_{42}) &= 0 \\ \alpha(x_3) &= 1 \end{aligned}$$

Then we have

$$\begin{aligned} \mathcal{J}_\alpha(\vee(\neg(x_{42}), \wedge(\mathbf{T}, x_3))) &= \mathcal{J}(\vee)(\mathcal{J}_\alpha(\neg(x_{42})), \mathcal{J}_\alpha(\wedge(\mathbf{T}, x_3))) \\ &= \max(\mathcal{J}(\neg)(\mathcal{J}_\alpha(x_{42})), \\ &\qquad \mathcal{J}(\wedge)(\mathcal{J}_\alpha(\mathbf{T}), \mathcal{J}_\alpha(x_3))) \\ &= \max(1 - \alpha(x_{42}), \min(\mathcal{J}(\mathbf{T}), \alpha(x_3))) \\ &= \max(1 - 0, \min(1, 1)) = 1 \end{aligned}$$