
Term Algebras

Signatures and finite terms

Σ : Set of **function symbols** having an **arity** $n \in \mathbb{N}$.

\mathcal{X} : Set of **variables**.

$\mathcal{T}(\mathcal{X}, \Sigma)$: Set of **terms** over \mathcal{X} and Σ :

f has arity n

$$\frac{x \in \mathcal{X}}{x \in \mathcal{T}(\mathcal{X}, \Sigma)} \quad \frac{t_1, \dots, t_n \in \mathcal{T}(\mathcal{X}, \Sigma) \quad f/n \in \Sigma}{f(t_1, \dots, t_n) \in \mathcal{T}(\mathcal{X}, \Sigma)}$$

We note $Var(t)$ the set of variables of the term t . A term t is **closed** if $Var(t) = \emptyset$.

Example :

Signature :

z :	arity 0	s :	arity 1
$+$:	arity 2	eq :	arity 2
$true$:	arity 0	$false$:	arity 0

Terms :

$eq(s(x + z), z)$ $eq(true, false)$ $eq(s(x + z), false)$

closed

Positions of terms

\mathbb{N}^* : positions over \mathbb{N}

$$\frac{}{\Lambda \in \mathbb{N}^*} \qquad \frac{i \in \mathbb{N} \text{ and } p \in \mathbb{N}^*}{ip \in \mathbb{N}^*}$$

$Pos(t)$: positions of a term t

$$\frac{}{\Lambda \in Pos(t)} \qquad \frac{p \in Pos(t_i) \text{ and } 1 \leq i \leq n}{ip \in Pos(f(t_1, \dots, t_n))}$$

Example :

$$Pos(f(g(a, h(b)), x, c)) = \{\Lambda, 1, 2, 3, 11, 12, 121\}$$

The relation \leq_{pref} over positions

Concatenation of positions :
$$\begin{cases} \Lambda.q & = & q \\ (ip).q & = & i(p.q) \end{cases}$$

Comparing positions : $p \leq_{pref} q$ iff $\exists r \in \mathbb{N}^* p.r = q$

Example :

1	\leq_{pref}	1211	"1 is a prefix of 1211"
231	\geq_{pref}	23	"231 is a suffix of 23"
12	$\not\leq_{pref}$	2	"12 is parallel to 2"

12 $\not\leq_{pref}$ 2 & 2 $\not\leq_{pref}$ 12

Sub-terms

$v \sqsubseteq t$: v is a **subterm/subtree** of t :

$$\frac{}{t \sqsubseteq t} \qquad \frac{v \sqsubseteq t_i}{v \sqsubseteq f(t_1, \dots, t_n)}$$

$v \triangleleft t$: v is a **strict** subterm of t .

$ST(t)$: All the subterms of t .

Example : $g(x, y) \triangleleft f(g(x, y), a)$ and $a \triangleleft f(g(x, y), a)$ but $f(x, a) \not\triangleleft f(g(x, y), a)$.

Sub-term X at position Y

$t|_p$: subterm of t at position p

$$\frac{}{t|_{\Lambda} = t} \quad \frac{t_i|_q = v}{f(t_1, \dots, t_n)|_{iq} = v}$$

Example : $f(g(a, h(b)), x, c)|_{11} = a$ but $f(g(a, h(b)), x, c)|_{21}$ is not defined.

Exercise : Show that $p.q \in Pos(t)$ implies $t|_{p.q} = (t|_p)_q$.

Replacement

$t[p//v]$: **replacement** of the subterm $t|_p$ by the term v

– $t[\Lambda//v] = v$

– $f(t_1, \dots, t_n)[ip//v] = f(t_1, \dots, t_i[p//v], \dots, t_n)$

Other notations : $t[v]_p$ or $t[v]$ if p is clear from the context.

Example : $f(h(x, y), a)[12//b] = f(h(x, b), a)$ and
 $f(h(x, y), a)[1//b] = f(b, a)$.

Exercise : Show the following properties :

- If $p \in Pos(s)$ and $q \in Pos(t)$, then $(s[t]_p)|_{p.q} = t|_q$ and $(s[t]_p)[r]_{p.q} = s[t[r]_q]_p$.
- If $p.q \in Pos(s)$, then $(s[t]_{p.q})|_p = (s|_p)[t]_q$ and $(s[t]_{p.q})[r]_p = s[r]_p$.
- If $p, q \in Pos(s)$ and $p \bowtie q$, then $(s[t]_p)|_q = s|_q$ and $(s[t]_p)[r]_q = (s[r]_q)[t]_p$.

Σ -algebras

A Σ -algebra \mathcal{A} is defined by :

- A non-empty domain \mathbf{A} .
- An interpretation function $f^{\mathcal{A}} : \mathbf{A}^n \mapsto \mathbf{A}$, for each f/n .

Example : Let $\Sigma = \{z, s, p\}$.

1. \mathbf{A} is the set \mathbb{N} , $z^{\mathcal{A}} = 0$, $s^{\mathcal{A}}(n) = n + 1$ and $p^{\mathcal{A}}(n, m) = n + m$.
2. \mathbf{A} is the set \mathbb{Z} , $z^{\mathcal{A}} = -5$, $s^{\mathcal{A}}(n) = n * 13$ and $p^{\mathcal{A}}(n, m) = n * m$.
3. **Syntactic Algebra** : \mathbf{A} is the set of all the terms over \mathcal{X} and $\Sigma = \{z, s, p\}$ such that $z^{\mathcal{A}} = z$, $s^{\mathcal{A}}(t) = s(t)$ and $p^{\mathcal{A}}(t, u) = p(t, u)$.

Congruence

The symbol $f \in \Sigma$ is **monotonic** w.r.t the relation R iff

$a_i R b_i$ implies $f.A(a_1, \dots, a_n) R f.A(b_1, \dots, b_n)$.
reflexive, symmetric, transitive

A **congruence** \sim is an equivalence relation, s.t. every symbol $f \in \Sigma$ is monotonic w.r.t. \sim .

Example : $\sim = \{(x, y) \mid 4 \text{ divides } x - y\}$ is a congruence.

Notation : \mathcal{A}/\sim is the set of equivalence classes of a \mathcal{A} modulo the congruence \sim .

The quotient algebra

Quotient algebra \mathcal{A}^\sim over \mathcal{A} :

- Domain \mathcal{A}/\sim
- Interpretations $f^{\mathcal{A}^\sim}([a_1], \dots, [a_n]) = [f^{\mathcal{A}}(a_1, \dots, a_n)]$.

Example : Let $\Sigma = \{z, suc, pred, add\}$ and let \mathcal{A} be the Σ -algebra given by $\mathbf{A} = \mathbf{Z}$, $suc^{\mathcal{A}}(n) = n + 1$, $pred^{\mathcal{A}}(n) = n - 1$ and $add^{\mathcal{A}}(n, m) = n + m$.

Let $\sim = \{(x, y) \mid 4 \text{ divides } x - y\}$.

We have $A/\sim = \{[0], [1], [2], [3]\}$, where

$$[0] = \{\dots, -4, 0, 4, 8, \dots\}$$

$$[1] = \{\dots, -3, 1, 5, 9, \dots\}$$

$$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$[3] = \{\dots, -5, -1, 3, 7, \dots\}$$

We have $z^{A/\sim} = [0]$, $suc^{A/\sim}(n) = [n + 1]$, $pred^{A/\sim}(n) = [n - 1]$
and $add^{A/\sim}(n, m) = [n + m]$.

Homomorphism, endomorphism, isomorphism

Let \mathcal{A} and \mathcal{B} be two Σ -algebras. A **morphism** is a function $\Phi : \mathcal{A} \rightarrow \mathcal{B}$ s.t. for all $n \geq 0$, for all $f/n \in \Sigma$ and for all $a_1, \dots, a_n \in \mathcal{A}$ we have

$$\Phi(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(\Phi(a_1), \dots, \Phi(a_n))$$

An **endomorphism** over a Σ -algebra \mathcal{A} is a morphism from \mathcal{A} to itself. An **isomorphism** is a bijective morphism.

Exercise : Let $\Sigma = \{a, s, g, h\}$. Define a Σ -algebra \mathcal{B} and a morphism Φ between the syntactic Σ -algebra and \mathcal{B} .

Let \mathcal{B} be the Σ -algebra defined by :

- The domain $\mathbf{B} = \{n \in \mathbb{N} \mid n \geq 2\}$
- The interpretations :

$$\begin{aligned} a^{\mathcal{B}} &= 2 & g^{\mathcal{B}}(t) &= t + 1 \\ s^{\mathcal{B}}(t) &= t & h^{\mathcal{B}}(u, t) &= u + t \end{aligned}$$

Let Φ be the following function :

$$\begin{aligned} \Phi(a) &= 2 & \Phi(g(t)) &= \Phi(t) + 1 \\ \Phi(s(t)) &= \Phi(t) & \Phi(h(u, t)) &= \Phi(u) + \Phi(t) \end{aligned}$$

One verifies $\Phi(f^{\mathcal{A}}(t_1, \dots, t_n)) = f^{\mathcal{B}}(\Phi(t_1), \dots, \Phi(t_n))$ for every f/n in Σ .

Valuations

Let \mathcal{A} be a Σ -algebra and let \mathcal{X} be a set of variables.

A \mathcal{A} -valuation is an application $\sigma : \mathcal{X} \rightarrow \mathcal{A}$.

Theorem : For every \mathcal{A} -valuation $\sigma : \mathcal{X} \rightarrow \mathcal{A}$, there is a **unique morphism** $\hat{\sigma} : \mathcal{T}(\mathcal{X}, \Sigma) \rightarrow \mathcal{A}$, s.t.

$$\begin{aligned}\hat{\sigma}(x) &= \sigma(x) \\ \hat{\sigma}(f(t_1, \dots, t_n)) &= f^{\mathcal{A}}(\hat{\sigma}(t_1), \dots, \hat{\sigma}(t_n))\end{aligned}$$

Remarque : We usually do not distinguish σ and $\hat{\sigma}$

Substitutions as valuations

the set of all the terms

having a finite domain

A substitution from \mathcal{X} to the syntactic algebra.

Finite substitutions are denoted $\theta = \{x_1/t_1, \dots, x_n/t_n\}$.

A **Renaming** is an isomorphic substitution.

Example :

- $\theta_1 = \{x/y, y/x\}$ and $\theta_2 = \{x/y, y/z, z/w\}$ are renamings.
- Given $t = f(x, g(y))$ and $\theta = \{x/g(a), y/f(x, x)\}$ we have $\theta(t) = f(g(a), g(f(x, x)))$.

Semantical equational reasoning

A Σ -equation is a pair of terms denoted $s \doteq t$.

A Σ -algebra \mathcal{A} is a **model** of a **set of Σ -equations** \mathcal{E} , noté $\mathcal{A} \models \mathcal{E}$, iff \mathcal{A} is a model of every equation of \mathcal{E} (e.g. $\sigma(s) = \sigma(t)$ holds for every \mathcal{A} -valuation).

Example : The first Σ -algebra on slide (Σ -algebras) is a model of the equation $x + y = y + x$.

The equation $s \doteq t$ is a **semantic consequence** of a set of equations \mathcal{E} , written $\mathcal{E} \models s \doteq t$, iff every model of \mathcal{E} is also a model of $s \doteq t$ iff $\mathcal{A} \models \mathcal{E}$ implies $\mathcal{A} \models s \doteq t$.

Syntactic rules for equational reasoning

$$\frac{s \doteq t \in \mathcal{E}}{s \doteq t} \quad (\text{axiome}) \qquad \frac{}{s \doteq s} \quad (\text{r\'eflexivit\'e})$$

$$\frac{s \doteq t}{t \doteq s} \quad (\text{sym\'etrie}) \qquad \frac{s \doteq t \quad t \doteq u}{s \doteq u} \quad (\text{transitivit\'e})$$

$$\frac{s \doteq t}{\sigma(s) \doteq \sigma(t)} \quad (\text{substitution}) \qquad \frac{s \doteq t}{u[s]_p \doteq u[t]_p} \quad (\text{contexte})$$

Derivation of $s \doteq t$ from the set \mathcal{E} is denoted by $\mathcal{E} \vdash s \doteq t$.

Example

Let $\mathcal{E} = \{0 + n \doteq n, s(n) + m \doteq s(n + m)\}$.

We derive $s(0) + 3 \doteq 4$ from \mathcal{E} as follows :

$$\frac{\frac{s(n) + m \doteq s(n + m)}{s(0) + 3 \doteq s(0 + 3)} \text{ (subst)}}{\frac{\frac{0 + n \doteq n}{0 + 3 \doteq 3} \text{ (subst)}}{s(0 + 3) \doteq s(3)} \text{ (ctxt)}} \text{ (tran)}$$
$$s(0) + 3 \doteq s(3)$$

Birkhoff's Theorem (1933)

Let \mathcal{E} be a set of Σ -equations.

(Soundness) If $\mathcal{E} \vdash s \doteq t$, then $\mathcal{E} \models s \doteq t$.

(Completeness) If $\mathcal{E} \models s \doteq t$, then $\mathcal{E} \vdash s \doteq t$.

Unification

Unification

Two terms s and t are **unifiable** iff there exists a substitution (called **unifier**) s.t. $\theta(s) = \theta(t)$.

Example :

- $f(x, g(x, a))$ and $f(f(a), y)$ are unifiable with
 $\theta = \{x/f(a), y/g(f(a), a)\}$

$$f(x, g(x, a)) \quad \doteq \quad f(f(a), y)$$

$$f(f(a), g(f(a), a)) \quad = \quad f(f(a), g(f(a), a))$$

- $f(x, g(x, a))$ and $f(f(a), f(b, a))$ are not unifiable.

Principal substitutions

Let θ and τ be two substitutions and \mathcal{S} be a set of substitutions.

- The **composition** of θ and τ is $(\theta \circ \tau)(x) = \widehat{\theta}(\tau(x))$ for every variable $x \in \mathcal{X}$.
- θ is an **instance** of τ (or τ is **more general** than θ) iff there exists a substitution ρ s.t. for every variable $x \in \mathcal{X}$, $(\rho \circ \tau)(x) = \theta(x)$.
- $\tau \in \mathcal{S}$ is **principal** (or **most general**) iff every substitution $\theta \in \mathcal{S}$ is an instance of τ .

Example : Let $\sigma_1 = \{y/b, z/h(c)\}$ and $\sigma_2 = \{x/f(y), y/z\}$.

$$\sigma_1 \circ \sigma_2 = \{x/f(b), y/h(c), z/h(c)\}.$$

σ_2 is more general than $\sigma_1 \circ \sigma_2$.

Principal unifier

Theorem : Let \mathcal{S} be a non-empty set of unifiers of s and t . Then, there exists a **principal unifier** $\theta \in \mathcal{S}$ s.t. for every $\tau \in \mathcal{S}$, θ is more general than τ . Moreover, this principal unifier is **unique** modulo renaming.

Idempotent unifiers

A substitution θ is **idempotent** iff $\theta \circ \theta = \theta$.

Example : $\{y/b, z/h(c)\}$ is idempotent.

$\{x/f(y), y/z\}$ is not idempotent.

Theorem : If s and t are unifiable, then there exists a **principal unifier** of s and t which is **idempotent**.

How we can construct this unifier?

Equational systems

An (Σ) equational system is a set of (Σ) equations of the form $s \doteq t$.

An equational system E is **unifiable** iff there exists a unifier (called **solution**) for all the equations of E .

Finite equational systems are denoted $\{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$.

Solved forms

The equational system $E = \{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$ is in **solved form** iff

- All the s_i are **distinct variables**.
- No s_i appears in t_j .

Example : $E_0 = \{x \doteq y, z \doteq f(a)\}$ is in solved form but

$$E_1 = \{x \doteq y, x \doteq f(a)\},$$

$$E_2 = \{x \doteq y, y \doteq f(a)\},$$

$$E_3 = \{x \doteq z, y \doteq f(y)\} \text{ do not.}$$

Notation : For the solved system $E = \{\alpha_1 \doteq t_1, \dots, \alpha_n \doteq t_n\}$ we note \vec{E} the substitution $\{\alpha_1/t_1, \dots, \alpha_n/t_n\}$.

The transformation rules

$$\frac{E \cup \{s \doteq s\}}{E} \quad (\text{erase}) \quad \frac{E \cup \{t \doteq \alpha\} \quad t \notin \mathcal{X}}{E \cup \{\alpha \doteq t\}} \quad (\text{orient})$$

$$\frac{E \cup \{f(s_1, \dots, s_n) \doteq f(t_1, \dots, t_n)\}}{E \cup \{s_1 \doteq t_1, \dots, s_n \doteq t_n\}} \quad (\text{decompose})$$

$$\frac{E \cup \{\alpha \doteq s\} \quad \alpha \in \text{Var}(E) \quad \alpha \notin \text{Var}(s)}{E\{\alpha/s\} \cup \{\alpha \doteq s\}} \quad (\text{substitute})$$

The unification algorithm

1. Take an equational system E
2. Compute a new system P by applying the transformation rules as far as possible.
3. If the system P is in solved form
 - then send the answer \vec{P}
 - else fail

Example : Unification of the system

$$\{p(a, x, f(g(y))) \doteq p(z, f(z), f(u))\}$$

$$\frac{p(a, x, f(g(y))) \doteq p(z, f(z), f(u))}{a \doteq z, x \doteq f(z), f(g(y)) \doteq f(u)} \quad d$$

$$\frac{a \doteq z, x \doteq f(z), f(g(y)) \doteq f(u)}{z \doteq a, x \doteq f(z), f(g(y)) \doteq f(u)} \quad o$$

$$\frac{z \doteq a, x \doteq f(z), f(g(y)) \doteq f(u)}{z \doteq a, x \doteq f(a), f(g(y)) \doteq f(a)} \quad s$$

$$\frac{z \doteq a, x \doteq f(a), f(g(y)) \doteq f(a)}{z \doteq a, x \doteq f(a), u \doteq g(y)} \quad d$$

$$\frac{z \doteq a, x \doteq f(a), u \doteq g(y)}{z \doteq a, x \doteq f(a), u \doteq g(y)} \quad o$$

solved form

yields the (idempotent) substitution $\{z/a, x/f(a), u/g(y)\}$.

Soundness and completeness of the algorithm

Theorem : The algorithm terminates.

Theorem : (Soundness) If the algorithm finds a substitution \vec{S} for the problem P , then P is unifiable and \vec{S} is a m.g.u. of P .

That is,

If P is not unifiable, then the algorithm fails.

Theorem : (Completeness) If the system P is unifiable, then the algorithm computes the m.g.u. of P .

That is,

If the algorithm fails, then the system P is not unifiable.