Algebraic and Coalgebraic methods in software development

Manuel A. Martins [1]

MAP-i
2017/18

[1] Mathematics Department, Aveiro University, Portugal

Outline

1. Equational specification
   - Term algebra, free algebra, initial and final objects.
   - Equational calculus. Initial models.
   - Term rewriting
   - Generalizations

Outline

1. Equational specification
   - Term algebra, free algebra, initial and final objects.
   - Equational calculus. Initial models.
   - Term rewriting
   - Generalizations

Term Algebra

Definition (term)

Let Σ *be a signature and* $X = \langle X_s \rangle_{s \in S}$ *a* S*-sorted set of variables for* Σ. *The* S*-set* Σ*-terms over* X *is the smallest* S*-set* $\mathrm{T}(\Sigma, \mathrm{X})$ *s.t.:*

- $X_s \subseteq \mathrm{T}(\Sigma, \mathrm{X})_s$;
- $\Omega_{\epsilon,s} \subseteq \mathrm{T}(\Sigma, \mathrm{X})_s$;
- *For any* $f : s_1, \ldots, s_n \to s \in \Sigma$ *and* $t_1 \in \mathrm{T}(\Sigma, \mathrm{X})_{s_1}, \ldots, t_n \in \mathrm{T}(\Sigma, \mathrm{X})_{s_n}$, $f(t_1, \ldots, t_n) \in \mathrm{T}(\Sigma, \mathrm{X})_s$;

Term Algebra

Definition (term)

Let Σ be a signature and $X = \langle X_s \rangle_{s \in S}$ a S-sorted set of variables for Σ. The S-set Σ-terms over X is the smallest S-set $\mathrm{T}(\Sigma, \mathrm{X})$ s.t.:

- $X_s \subseteq \mathrm{T}(\Sigma, \mathrm{X})_s$;
- $\Omega_{\epsilon, s} \subseteq \mathrm{T}(\Sigma, \mathrm{X})_s$;
- *For any* $f : s_1, \ldots, s_n \to s \in \Sigma$ *and* $t_1 \in \mathrm{T}(\Sigma, \mathrm{X})_{s_1}, \ldots, t_n \in \mathrm{T}(\Sigma, \mathrm{X})_{s_n}$, $f(t_1, \ldots, t_n) \in \mathrm{T}(\Sigma, \mathrm{X})_s$;

Definition (Term Algebra)

If $\mathrm{T}(\Sigma, \mathrm{X})$ is non empty, the term algebra over X is the algebra $\mathcal{T}(\Sigma, X)$ with carrier set $\mathrm{T}(\Sigma, \mathrm{X})$, and for any $f : s_1, \ldots, s_n \to s \in \Sigma$ and every $t_1 \in \mathrm{T}(\Sigma, \mathrm{X})_{s_1}, \ldots, t_n \in \mathrm{T}(\Sigma, \mathrm{X})_{s_n}$,

$$f^{\mathcal{T}(\Sigma, X)}(t_1, \ldots, t_n) := f(t_1, \ldots, t_n)$$

Fact

$\mathcal{T}(\Sigma, X)$ is the Σ-algebra generated by X

Fact

$\mathcal{T}(\Sigma, X)$ is the Σ-algebra generated by X

Definition

Σ is non empty iff for every $s \in S$ there is a $t \in T(\Sigma, \emptyset)$.

$T(\Sigma, \emptyset)$ is called ground term algebra.

Fact

$\mathcal{T}(\Sigma, X)$ is the Σ-algebra generated by X

Definition

Σ is non empty iff for every $s \in S$ there is a $t \in T(\Sigma, \emptyset)$.

$T(\Sigma, \emptyset)$ is called ground term algebra.

Example (naturals revisited)

Since Σ_N is non empty, the term algebra exists. The carrier set is

$$0, s(0), s(s(0)), s(s(s(0))), \ldots$$

Example (A simple programming language)

```
Gen
    E
    bool
    P
Op
            0, x1, ..., xn :       → E
                     s, p : E → E
                 +, −, ∗ : E, E → E
                   _ = _ : E, E → bool
                  _ := _ : E, E → P
                    _;_ : P, P → P
if _ then _ else - fi : bool, P, P → P
     repeat _ do _ od : E, P → P
```

E correct expressions (for simplicity integers)
bool for booleans
P for programmes

Example (A simple programming language)

Gen
- E
- bool
- P

Op

$$0, x_1, \ldots, x_n : \ \to \mathrm{E}$$
$$\mathrm{s}, \mathrm{p} : \mathrm{E} \to \mathrm{E}$$
$$+, -, * : \mathrm{E}, \mathrm{E} \to \mathrm{E}$$
$$\_ = \_ : \mathrm{E}, \mathrm{E} \to \mathtt{bool}$$
$$\_ := \_ : \mathrm{E}, \mathrm{E} \to \mathrm{P}$$
$$\_ ; \_ : \mathrm{P}, \mathrm{P} \to \mathrm{P}$$
$$\mathtt{if}\ \_\ \mathtt{then}\ \_\ \mathtt{else}\ -\ \mathtt{fi} : \mathtt{bool}, \mathrm{P}, \mathrm{P} \to \mathrm{P}$$
$$\mathtt{repeat}\ \_\ \mathtt{do}\ \_\ \mathtt{od} : \mathrm{E}, \mathrm{P} \to \mathrm{P}$$

E correct expressions (for simplicity integers)
bool for booleans
P for programmes

What means the following term?

$y_1 := 1; y_2 := 1;$
repeat 5 do
$\quad y_1 := y_1 * y_2;$
$\quad y_2 := y_2 + 1$
od

Definition

Let K be a class of algebras over Σ. An object $\mathbf{A} \in K$ is called initial in K iff for any $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{A} \to \mathbf{B}$.

Definition

Let K be a class of algebras over Σ. An object $\mathbf{A} \in K$ is called initial in K iff for any $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{A} \to \mathbf{B}$.
An object $\mathbf{A} \in K$ is called final in K iff for any object $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{B} \to \mathbf{A}$.

Definition

Let K be a class of algebras over Σ. An object $\mathbf{A} \in K$ is called initial in K iff for any $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{A} \to \mathbf{B}$.
An object $\mathbf{A} \in K$ is called final in K iff for any object $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{B} \to \mathbf{A}$.

Fact

Initial (final) algebras are unique up to isomorphism.

Definition

Let K be a class of algebras over Σ. An object $\mathbf{A} \in K$ is called initial in K iff for any $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{A} \to \mathbf{B}$.
An object $\mathbf{A} \in K$ is called final in K iff for any object $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{B} \to \mathbf{A}$.

Fact

Initial (final) algebras are unique up to isomorphism.

Fact

Let Σ a non empty signature. Then $\mathcal{T}(\Sigma)$ is initial in $Alg(\Sigma)$.

Definition

Let K be a class of algebras over Σ. An object $\mathbf{A} \in K$ is called initial in K iff for any $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{A} \to \mathbf{B}$.
An object $\mathbf{A} \in K$ is called final in K iff for any object $\mathbf{B} \in K$ there exists a unique homomorphism $h : \mathbf{B} \to \mathbf{A}$.

Fact

Initial (final) algebras are unique up to isomorphism.

Fact

Let Σ a non empty signature. Then $\mathcal{T}(\Sigma)$ is initial in $Alg(\Sigma)$.

Fact

For any signature Σ the trivial algebra is final in $Alg(\Sigma)$.

Example

I- The class of algebras over the signature of natural numbers $\Sigma = \{0, suc, +\}$, with just one sort *nat*, satisfying the axioms $suc(0 + n) = n$ and $suc(n) + m = suc(n + m)$ has both initial and final algebras.

Example

I- The class of algebras over the signature of natural numbers $\Sigma = \{0, suc, +\}$, with just one sort *nat*, satisfying the axioms $suc(0 + n) = n$ and $suc(n) + m = suc(n + m)$ has both initial and final algebras.

II- Moore Automata. Let IN and OUT be fixed. There is final algebra but not initial.

Gen

in
out
stat

Op

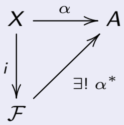
$c :\to inc \in In$
$k :\to outk \in Out$
$next : in, stat \to stat$
$print : stat \to out$

Show that there is no initial algebra but there is an interesting final algebra.

Algebra livre

Definition

Let K be a class of Σ-algebra. An algebra $\mathcal{F}$ (not necessarily in K) s.t. $X \subseteq F$ is called free for K over X iff for any $\mathcal{A} \in K$ and every $\alpha : X \to A$ there is a unique homomorphism $\alpha^* : \mathcal{F} \to \mathcal{A}$ that extends α, i.e., $\alpha^*(x) = \alpha(x)$ for all $x \in X$.



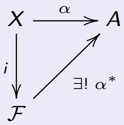
If $\mathcal{F} \in K$ we say that $\mathcal{F}$ is free in K over X.

(we will just write α instead of α^*)

Algebra livre

Definition

Let K be a class of Σ-algebra. An algebra $\mathcal{F}$ (not necessarily in K) s.t. $X \subseteq F$ is called free for K over X iff for any $\mathcal{A} \in K$ and every $\alpha : X \to A$ there is a unique homomorphism $\alpha^* : \mathcal{F} \to \mathcal{A}$ that extends α, i.e., $\alpha^*(x) = \alpha(x)$ for all $x \in X$.



If $\mathcal{F} \in K$ we say that $\mathcal{F}$ is free in K over X.

(we will just write α instead of α^*)

Fact

If $\mathrm{T}(\Sigma, \mathrm{X})$ is non empty, $\mathcal{T}(\Sigma, X)$ is free in $Alg(\Sigma)$ over X.

Models and equations

- A Σ-equation is a pair $\langle t_1, t_2 \rangle$ with $t_1, t_2 \in \mathrm{T}(\Sigma, \mathrm{X})_s$. We will write $t_1 \approx t_2$.

Models and equations

- A Σ-equation is a pair $\langle t_1, t_2 \rangle$ with $t_1, t_2 \in \mathrm{T}(\Sigma, \mathrm{X})_s$. We will write $t_1 \approx t_2$.

$\models$ - equational satisfaction

- $\mathcal{A} \models t_1 \approx t_2$ if, for every $h : X \to A$ $h^*(t_1) = h^*(t_2)$.

Models and equations

- A Σ-equation is a pair $\langle t_1, t_2 \rangle$ with $t_1, t_2 \in \mathrm{T}(\Sigma, \mathrm{X})_s$. We will write $t_1 \approx t_2$.

$\models$ - equational satisfaction

- $\mathcal{A} \models t_1 \approx t_2$ if, for every $h : X \to A$ $h^*(t_1) = h^*(t_2)$.
- $\mathcal{A} \models \Phi$ if, for every $t_1 \approx t_2 \in \Phi$ $\mathcal{A} \models t_1 \approx t_2$.

Models and equations

- A Σ-equation is a pair $\langle t_1, t_2 \rangle$ with $t_1, t_2 \in \mathrm{T}(\Sigma, \mathrm{X})_s$. We will write $t_1 \approx t_2$.

$\models$ - equational satisfaction

- $\mathcal{A} \models t_1 \approx t_2$ if, for every $h : X \to A$ $h^*(t_1) = h^*(t_2)$.
- $\mathcal{A} \models \Phi$ if, for every $t_1 \approx t_2 \in \Phi$ $\mathcal{A} \models t_1 \approx t_2$.
- $K \models t_1 \approx t_2$ if, for every $\mathcal{A} \in K$ $\mathcal{A} \models t_1 \approx t_2$.

Models and equations

- A Σ-equation is a pair $\langle t_1, t_2 \rangle$ with $t_1, t_2 \in \mathrm{T}(\Sigma, \mathrm{X})_s$. We will write $t_1 \approx t_2$.

$\models$ - equational satisfaction

- $\mathcal{A} \models t_1 \approx t_2$ if, for every $h : X \to A$ $h^*(t_1) = h^*(t_2)$.
- $\mathcal{A} \models \Phi$ if, for every $t_1 \approx t_2 \in \Phi$ $\mathcal{A} \models t_1 \approx t_2$.
- $K \models t_1 \approx t_2$ if, for every $\mathcal{A} \in K$ $\mathcal{A} \models t_1 \approx t_2$.
- A pair $\langle \Sigma, \Phi \rangle$ is called a *flat specification*.

Galois connection

- A model of a specification flat $\langle \Sigma, \Phi \rangle$ is an Σ-algebra such that $\mathcal{A} \models \Phi$. The class of all models of Φ, $\mathrm{Mod}(\Phi)$.

Galois connection

- A model of a specification flat $\langle \Sigma, \Phi \rangle$ is an Σ-algebra such that $\mathcal{A} \models \Phi$. The class of all models of Φ, $\mathrm{Mod}(\Phi)$.
- [Semantic consequence] $\Phi \models_{\Sigma} t_1 \approx t_2$ iff $\mathrm{Mod}[\Phi] \models_{\Sigma} t_1 \approx t_2$.

Galois connection

- A model of a specification flat $\langle \Sigma, \Phi \rangle$ is an Σ-algebra such that $\mathcal{A} \models \Phi$. The class of all models of Φ, $\mathrm{Mod}(\Phi)$.
- [Semantic consequence] $\Phi \models_\Sigma t_1 \approx t_2$ iff $\mathrm{Mod}[\Phi] \models_\Sigma t_1 \approx t_2$.
- The theory of K - $\mathrm{Th}_\Sigma(K)_s := \{t_1 \approx t_2 \in \mathrm{Eq}(\Sigma, X) : K \models t_1 \approx t_2\}$

Galois connection

- A model of a specification flat $\langle \Sigma, \Phi \rangle$ is an Σ-algebra such that $\mathcal{A} \models \Phi$. The class of all models of Φ, $\mathrm{Mod}(\Phi)$.
- [Semantic consequence] $\Phi \models_{\Sigma} t_1 \approx t_2$ iff $\mathrm{Mod}[\Phi] \models_{\Sigma} t_1 \approx t_2$.
- The theory of K - $\mathrm{Th}_{\Sigma}(K)_s := \{t_1 \approx t_2 \in \mathrm{Eq}(\Sigma, X) : K \models t_1 \approx t_2\}$

Galois connection.

1. $\Phi \subseteq \Psi$ implies $\mathrm{Mod}(\Phi) \supseteq \mathrm{Mod}(\Psi)$;
2. $K \subseteq K'$ implies $\mathrm{Th}_{\Sigma}(K) \supseteq \mathrm{Th}_{\Sigma}(K')$;
3. $\Phi \subseteq \mathrm{Th}_{\Sigma}(\mathrm{Mod}(\Phi))$ and $K \subseteq \mathrm{Mod}(\mathrm{Th}_{\Sigma}(K))$.

Equational calculus

Assume that Σ are non empty.

(i) $$\frac{}{\Phi \vdash_{\Sigma} t_1 \approx t_2} \text{ for every } t_1 \approx t_2 \in \Phi$$

Equational calculus

Assume that Σ are non empty.

(i) $\dfrac{}{\Phi \vdash_\Sigma t_1 \approx t_2}$ for every $t_1 \approx t_2 \in \Phi$

(ii) $\dfrac{}{\emptyset \vdash_\Sigma t \approx t}$ (reflexivity)

Equational calculus

Assume that Σ are non empty.

(i) $\dfrac{}{\Phi \vdash_\Sigma t_1 \approx t_2}$ for every $t_1 \approx t_2 \in \Phi$

(ii) $\dfrac{}{\emptyset \vdash_\Sigma t \approx t}$ (reflexivity)

(iii) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma t_2 \approx t_1}$ (symmetry)

Equational calculus

Assume that Σ are non empty.

(i) $$\frac{}{\Phi \vdash_\Sigma t_1 \approx t_2} \text{ for every } t_1 \approx t_2 \in \Phi$$

(ii) $$\frac{}{\emptyset \vdash_\Sigma t \approx t} \qquad \text{(reflexivity)}$$

(iii) $$\frac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma t_2 \approx t_1} \qquad \text{(symmetry)}$$

(iv) $$\frac{\Phi \vdash_\Sigma t_1 \approx t_2;\ \Phi' \vdash_\Sigma t_2 \approx t_3}{\Phi \cup \Phi' \vdash_\Sigma t_1 \approx t_3} \qquad \text{(transitivity)}$$

Equational calculus

Assume that Σ are non empty.

(i) $$\frac{}{\Phi \vdash_\Sigma t_1 \approx t_2} \text{ for every } t_1 \approx t_2 \in \Phi$$

(ii) $$\frac{}{\emptyset \vdash_\Sigma t \approx t} \qquad \text{(reflexivity)}$$

(iii) $$\frac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma t_2 \approx t_1} \qquad \text{(symmetry)}$$

(iv) $$\frac{\Phi \vdash_\Sigma t_1 \approx t_2; \Phi' \vdash_\Sigma t_2 \approx t_3}{\Phi \cup \Phi' \vdash_\Sigma t_1 \approx t_3} \qquad \text{(transitivity)}$$

(v) $$\frac{\Phi_1 \vdash_\Sigma t_1 \approx t_1', \ldots, \Phi_n \vdash_\Sigma t_n \approx t_n'}{\Phi_1 \cup \cdots \cup \Phi_n \vdash_\Sigma f(t_1, \ldots t_n) \approx f(t_1', \ldots t_n')}, \text{ for any } f \in \Sigma \qquad \text{(congruence)}$$

Equational calculus

Assume that Σ are non empty.

(i) $\dfrac{}{\Phi \vdash_\Sigma t_1 \approx t_2}$ for every $t_1 \approx t_2 \in \Phi$

(ii) $\dfrac{}{\emptyset \vdash_\Sigma t \approx t}$ (reflexivity)

(iii) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma t_2 \approx t_1}$ (symmetry)

(iv) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2; \Phi' \vdash_\Sigma t_2 \approx t_3}{\Phi \cup \Phi' \vdash_\Sigma t_1 \approx t_3}$ (transitivity)

(v) $\dfrac{\Phi_1 \vdash_\Sigma t_1 \approx t_1', \ldots, \Phi_n \vdash_\Sigma t_n \approx t_n'}{\Phi_1 \cup \cdots \cup \Phi_n \vdash_\Sigma f(t_1, \ldots t_n) \approx f(t_1', \ldots t_n')}$, for any $f \in \Sigma$ (congruence)

(vi) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma \sigma(t_1) \approx \sigma(t_2)}$,for any substitution $\sigma : \mathrm{T}(\Sigma, \mathrm{X}) \to \mathrm{T}(\Sigma, \mathrm{X})$ (replacement)

Equational calculus

Assume that Σ are non empty.

(i) $\dfrac{}{\Phi \vdash_\Sigma t_1 \approx t_2}$ for every $t_1 \approx t_2 \in \Phi$

(ii) $\dfrac{}{\emptyset \vdash_\Sigma t \approx t}$ (reflexivity)

(iii) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma t_2 \approx t_1}$ (symmetry)

(iv) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2; \Phi' \vdash_\Sigma t_2 \approx t_3}{\Phi \cup \Phi' \vdash_\Sigma t_1 \approx t_3}$ (transitivity)

(v) $\dfrac{\Phi_1 \vdash_\Sigma t_1 \approx t_1', \ldots, \Phi_n \vdash_\Sigma t_n \approx t_n'}{\Phi_1 \cup \cdots \cup \Phi_n \vdash_\Sigma f(t_1, \ldots t_n) \approx f(t_1', \ldots t_n')}$, for any $f \in \Sigma$ (congruence)

(vi) $\dfrac{\Phi \vdash_\Sigma t_1 \approx t_2}{\Phi \vdash_\Sigma \sigma(t_1) \approx \sigma(t_2)}$,for any substitution $\sigma : \mathrm{T}(\Sigma, \mathrm{X}) \to \mathrm{T}(\Sigma, \mathrm{X})$ (replacement)

Examples

- Let $\Sigma = \langle S, \Omega \rangle$ with $S = \{S_0, S_1, S_2\}$, and Ω with $\Omega_{\epsilon, S_1} = \{a, b\}$, $\Omega_{\epsilon, S_2} = \{c, d\}$ and $\Omega_{S_1 S_2, S_0} = \{f\}$. Let $\Phi = \{a \approx b, c \approx d\}$. We have

$$\Phi \vdash f(a, c) \approx f(b, d)$$

Examples

- Let $\Sigma = \langle S, \Omega \rangle$ with $S = \{S_0, S_1, S_2\}$, and Ω with $\Omega_{\epsilon, S_1} = \{a, b\}$, $\Omega_{\epsilon, S_2} = \{c, d\}$ and $\Omega_{S_1 S_2, S_0} = \{f\}$. Let $\Phi = \{a \approx b, c \approx d\}$. We have

$$\Phi \vdash f(a, c) \approx f(b, d)$$

- [Flags] Let
$\Phi =$ Axioms of booleans $+ \{up?(dn(F)) \approx false, up?(up(F)) \approx true, up?(rev(F)) \approx \neg up?(F)\}$.
$\Phi \vdash rev(rev(F)) \approx F$?

Examples

- Let $\Sigma = \langle S, \Omega \rangle$ with $S = \{S_0, S_1, S_2\}$, and Ω with $\Omega_{\epsilon, S_1} = \{a, b\}$, $\Omega_{\epsilon, S_2} = \{c, d\}$ and $\Omega_{S_1 S_2, S_0} = \{f\}$. Let $\Phi = \{a \approx b, c \approx d\}$. We have

$$\Phi \vdash f(a, c) \approx f(b, d)$$

- [Flags] Let $\Phi =$ Axioms of booleans $+ \{up?(dn(F)) \approx false, up?(up(F)) \approx true, up?(rev(F)) \approx \neg up?(F)\}$. $\Phi \vdash rev(rev(F)) \approx F$?

- [Nat]:

$$\mathtt{nat}$$

$$0 : \ \to \mathtt{nat}$$
$$s : \mathtt{nat} \to \mathtt{nat}$$
$$+ : \mathtt{nat}, \mathtt{nat} \to \mathtt{nat}$$

$$0 + n \approx n$$
$$s(m) + n \approx s(m + n)$$

Examples

- Let $\Sigma = \langle S, \Omega \rangle$ with $S = \{S_0, S_1, S_2\}$, and Ω with $\Omega_{\epsilon, S_1} = \{a, b\}$, $\Omega_{\epsilon, S_2} = \{c, d\}$ and $\Omega_{S_1 S_2, S_0} = \{f\}$. Let $\Phi = \{a \approx b, c \approx d\}$. We have

$$\Phi \vdash f(a, c) \approx f(b, d)$$

- [Flags] Let $\Phi = \text{Axioms of booleans} + \{up?(dn(F)) \approx false, up?(up(F)) \approx true, up?(rev(F)) \approx \neg up?(F)\}$. $\Phi \vdash rev(rev(F)) \approx F$?

- [Nat]:

$\mathbf{nat}$

$0 : \ \rightarrow \mathbf{nat}$
$s : \mathbf{nat} \rightarrow \mathbf{nat}$
$+ : \mathbf{nat}, \mathbf{nat} \rightarrow \mathbf{nat}$

$0 + n \approx n$
$s(m) + n \approx s(m + n)$

Show that $\Phi \vdash s(0) + n \approx s(n)$

Completeness

- Let we define $t_1 \equiv_\Phi t_2$ iff $\Phi \vdash t_1 \approx t_2$.

Completeness

- Let we define $t_1 \equiv_\Phi t_2$ iff $\Phi \vdash t_1 \approx t_2$.

Fact

$\equiv_\Phi$ is a congruence on $\mathcal{T}(\Sigma, X)$.

Completeness

- Let we define $t_1 \equiv_\Phi t_2$ iff $\Phi \vdash t_1 \approx t_2$.

Fact

$\equiv_\Phi$ is a congruence on $\mathcal{T}(\Sigma, X)$.

Lemma

$\Phi \vdash t_1 \approx t_2$ *iff* $\mathcal{T}(\Sigma, X)/\equiv_\Phi \models t_1 \approx t_2$

Completeness

- Let we define $t_1 \equiv_\Phi t_2$ iff $\Phi \vdash t_1 \approx t_2$.

Fact

$\equiv_\Phi$ is a congruence on $\mathcal{T}(\Sigma, X)$.

Lemma

$\Phi \vdash t_1 \approx t_2$ *iff* $\mathcal{T}(\Sigma, X)/\equiv_\Phi \models t_1 \approx t_2$

Theorem (Soundness and completeness of Birkhoff)

$\Phi \vdash t_1 \approx t_2$ *iff* $\Phi \models t_1 \approx t_2$

Completeness

- Let we define $t_1 \equiv_\Phi t_2$ iff $\Phi \vdash t_1 \approx t_2$.

Fact

$\equiv_\Phi$ is a congruence on $\mathcal{T}(\Sigma, X)$.

Lemma

$\Phi \vdash t_1 \approx t_2$ *iff* $\mathcal{T}(\Sigma, X)/ \equiv_\Phi \models t_1 \approx t_2$

Theorem (Soundness and completeness of Birkhoff)

$\Phi \vdash t_1 \approx t_2$ *iff* $\Phi \models t_1 \approx t_2$

Proof.

($\Rightarrow$) Induction.
($\Leftarrow$) It is enough to show that $\Phi \models t_1 \approx t_2$ implies $\mathcal{T}(\Sigma, X)/ \equiv_\Phi \models t_1 \approx t_2$. □

Initial models

What should be a “good model” of a specification?

Initial models

What should be a "good model" of a specification?

Recall:
An algebra $\mathcal{A}$ is *reachable* if for each element a there is a ground term t st $t^{\mathcal{A}} = a$.

Initial models

What should be a "good model" of a specification?

Recall:
An algebra $\mathcal{A}$ is *reachable* if for each element a there is a ground term t st $t^{\mathcal{A}} = a$.

- Let $\mathcal{A} \in \mathrm{Mod}(\Phi)$. We say that $\mathcal{A}$ *contains junk* if it is not reachable and we say that $\mathcal{A}$ *contains confusion* if it satisfies a ground equation $t_1 \approx t_2 \in \mathrm{Eq}(\Sigma)$ s.t. $\Phi \not\models t_1 \approx t_2$.

Initial models

What should be a "good model" of a specification?

Recall:
An algebra $\mathcal{A}$ is *reachable* if for each element a there is a ground term t st $t^{\mathcal{A}} = a$.

- Let $\mathcal{A} \in \mathrm{Mod}(\Phi)$. We say that $\mathcal{A}$ *contains junk* if it is not reachable and we say that $\mathcal{A}$ *contains confusion* if it satisfies a ground equation $t_1 \approx t_2 \in \mathrm{Eq}(\Sigma)$ s.t. $\Phi \not\models t_1 \approx t_2$.

Theorem

$\mathcal{T}(\Sigma)/\equiv_{\Phi}$ *is a model in* $\mathrm{Mod}(\Phi)$ *containing no junk and no confusion.*

Initial models

What should be a "good model" of a specification?

Recall:
An algebra $\mathcal{A}$ is *reachable* if for each element a there is a ground term t st $t^{\mathcal{A}} = a$.

- Let $\mathcal{A} \in \mathrm{Mod}(\Phi)$. We say that $\mathcal{A}$ *contains junk* if it is not reachable and we say that $\mathcal{A}$ *contains confusion* if it satisfies a ground equation $t_1 \approx t_2 \in \mathrm{Eq}(\Sigma)$ s.t. $\Phi \not\models t_1 \approx t_2$.

Theorem

$\mathcal{T}(\Sigma)/\equiv_{\Phi}$ *is a model in* $\mathrm{Mod}(\Phi)$ *containing no junk and no confusion.*

Theorem

$\mathcal{T}(\Sigma)/\equiv_{\Phi}$ *is initial in* $\mathrm{Mod}(\Phi)$.

Initial models

What should be a "good model" of a specification?

Recall:
An algebra $\mathcal{A}$ is *reachable* if for each element a there is a ground term t st $t^{\mathcal{A}} = a$.

- Let $\mathcal{A} \in \mathrm{Mod}(\Phi)$. We say that $\mathcal{A}$ *contains junk* if it is not reachable and we say that $\mathcal{A}$ *contains confusion* if it satisfies a ground equation $t_1 \approx t_2 \in \mathrm{Eq}(\Sigma)$ s.t. $\Phi \not\models t_1 \approx t_2$.

Theorem

$\mathcal{T}(\Sigma)/\equiv_\Phi$ *is a model in* $\mathrm{Mod}(\Phi)$ *containing no junk and no confusion.*

Theorem

$\mathcal{T}(\Sigma)/\equiv_\Phi$ *is initial in* $\mathrm{Mod}(\Phi)$.

Corollary

Let $t_1 \approx t_2 \in \mathrm{Eq}(\Sigma)$, *i.e. ground equation. Then*

$$\mathcal{T}(\Sigma)/\equiv_\Phi \models t_1 \approx t_2 \Leftrightarrow \Phi \models t_1 \approx t_2.$$

[Bool]:

$\mathtt{bool}$

$true: \ \to \mathtt{bool}$
$false: \ \to \mathtt{bool}$
$\neg : \mathtt{bool} \to \mathtt{bool}$
$\wedge : \mathtt{bool},\mathtt{bool} \to \mathtt{bool}$
$\Rightarrow: \mathtt{bool},\mathtt{bool} \to \mathtt{bool}$

$\neg true \approx false$
$\neg false \approx true$
$p \wedge true \approx p$
$p \wedge false \approx false$
$p \wedge \neg p \approx false$
$p \Rightarrow q \approx \neg(p \wedge \neg q)$

(i) Present 3 finite models with 1, 2 and 3 elements.
(ii) Classify the models with respect to "junk" and "confusion".
(iii) Build the algebra $\mathcal{T}(\Sigma_{Bool})/\equiv_\Phi$, where Φ is the set of equations of the specification.

Term rewriting I

- Term rewriting is a technic used in standard mathematics to show that an equation can be shown as consequence of a given set of equations (see for instance Group theory.). It is the **support of CafeOBJ!**

Term rewriting I

- Term rewriting is a technic used in standard mathematics to show that an equation can be shown as consequence of a given set of equations (see for instance Group theory.). It is the **support of CafeOBJ!**

Definition (Rewriting)

Let $t_1, t_2 \in T(\Sigma, X)_s$ and $r = u_1 \rhd u_2$ a rewriting rule over Σ. We say that t_1 directly reduces into t_2 by r, we write $t_1 \rhd_r t_2$, if there is a substitution $\alpha : X \to \mathrm{T}(\Sigma, \mathrm{X})$ s.t.:

- *$\alpha(u_1)$ is a subterm of t_1 and*
- *t_2 can be obtained from t_1 by replacing the subterm $\alpha(u_1)$ by $\alpha(u_2)$.*

- $\rhd_r$ is a binary relation over $T(\Sigma, X)$.

Term rewriting I

- Term rewriting is a technic used in standard mathematics to show that an equation can be shown as consequence of a given set of equations (see for instance Group theory.). It is the **support of CafeOBJ!**

Definition (Rewriting)

Let $t_1, t_2 \in T(\Sigma, X)_s$ and $r = u_1 \rhd u_2$ a rewriting rule over Σ. We say that t_1 directly reduces into t_2 by r, we write $t_1 \rhd_r t_2$, if there is a substitution $\alpha : X \to \mathrm{T}(\Sigma, \mathrm{X})$ s.t.:

- *$\alpha(u_1)$ is a subterm of t_1 and*
- *t_2 can be obtained from t_1 by replacing the subterm $\alpha(u_1)$ by $\alpha(u_2)$.*

- $\rhd_r$ is a binary relation over $T(\Sigma, X)$.
- $\rhd_R = \bigcup_{r \in R} \rhd_r$.

Term rewriting I

- Term rewriting is a technic used in standard mathematics to show that an equation can be shown as consequence of a given set of equations (see for instance Group theory.). It is the **support of CafeOBJ!**

Definition (Rewriting)

Let $t_1, t_2 \in T(\Sigma, X)_s$ and $r = u_1 \rhd u_2$ a rewriting rule over Σ. We say that t_1 directly reduces into t_2 by r, we write $t_1 \rhd_r t_2$, if there is a substitution $\alpha : X \to \mathrm{T}(\Sigma, \mathrm{X})$ s.t.:

- *$\alpha(u_1)$ is a subterm of t_1 and*
- *t_2 can be obtained from t_1 by replacing the subterm $\alpha(u_1)$ by $\alpha(u_2)$.*

- $\rhd_r$ is a binary relation over $T(\Sigma, X)$.
- $\rhd_R = \bigcup_{r \in R} \rhd_r$.
- A computation is a sequence $t_1, \ldots, t_n \in \mathrm{T}(\Sigma, \mathrm{X})$ s.t. $t = t_1 \rhd_R \cdots \rhd_R t_n = t'$ and we write $t \rhd_R^* t'$ (it is the transitive closure of $\rhd_R$.).

Term rewriting II

Definition (Normal form)

Let $t, t' \in T(\Sigma, X)_s$ and R a rewriting system over Σ. t' is a normal form of t, we write $t \blacktriangleright_R t'$, if there is a terminating computation $t_1, \ldots, t_n$ s.t. $t = t_1$ and $t' = t_n$.

Term rewriting II

Definition (Normal form)

Let $t, t' \in T(\Sigma, X)_s$ and R a rewriting system over Σ. t' is a normal form of t, we write $t \blacktriangleright_R t'$, if there is a terminating computation $t_1, \ldots, t_n$ s.t. $t = t_1$ and $t' = t_n$.

In such case, we say that $t_1 \approx t_2$ can be deduced by rewriting in R, in symbols $\Vdash_R t_1 \approx t_2$, if there is a term t_3 s.t. $t_1 \blacktriangleright_R t_3$ and $t_2 \blacktriangleright_R t_3$.

Term rewriting II

Definition (Normal form)

Let $t, t' \in T(\Sigma, X)_s$ *and* R *a rewriting system over* Σ. t' *is a normal form of* t, *we write* $t \blacktriangleright_R t'$, *if there is a terminating computation* $t_1, \ldots, t_n$ *s.t.* $t = t_1$ *and* $t' = t_n$.

In such case, we say that $t_1 \approx t_2$ *can be deduced by rewriting in* R, *in symbols* $\Vdash_R t_1 \approx t_2$, *if there is a term* t_3 *s.t.* $t_1 \blacktriangleright_R t_3$ *and* $t_2 \blacktriangleright_R t_3$.

Theorem

$\Vdash_R t_1 \approx t_2 \Rightarrow \mathrm{Eq}(R) \vdash t_1 \approx t_2$.

Term rewriting II

Definition (Normal form)

Let $t, t' \in T(\Sigma, X)_s$ and R a rewriting system over Σ. t' is a normal form of t, we write $t \blacktriangleright_R t'$, if there is a terminating computation $t_1, \ldots, t_n$ s.t. $t = t_1$ and $t' = t_n$.

In such case, we say that $t_1 \approx t_2$ can be deduced by rewriting in R, in symbols $\Vdash_R t_1 \approx t_2$, if there is a term t_3 s.t. $t_1 \blacktriangleright_R t_3$ and $t_2 \blacktriangleright_R t_3$.

Theorem

$\Vdash_R t_1 \approx t_2 \Rightarrow \mathrm{Eq}(R) \vdash t_1 \approx t_2$.

Theorem

If R is terminating and confluent then

$$\mathrm{Eq}(R) \vdash t_1 \approx t_2 \Rightarrow \Vdash_R t_1 \approx t_2.$$

Birkhof's Theorem

- A class K is a *variety* iff it is closed under subalgebras, homomorphic images and direct products.

Birkhof's Theorem

- A class K is a *variety* iff it is closed under subalgebras, homomorphic images and direct products.

Theorem (Birkhoff's theorem)

A class K is a variety iff $K = \mathrm{Mod}(\Phi)$ for some set of equations Φ.

Birkhof's Theorem

- A class K is a *variety* iff it is closed under subalgebras, homomorphic images and direct products.

Theorem (Birkhoff's theorem)

A class K is a variety iff $K = \mathrm{Mod}(\Phi)$ for some set of equations Φ.

Example

Let $\Sigma = \langle \{S\}, \Omega \rangle$ where $\Omega_{\epsilon,S} = \{a, b\}$. Suppose that we would like to specify, using equations, the class of all Σ-algebras with exactly two elements. Birkhoff's theorem states that it can not be done.

Birkhof's Theorem

- A class K is a *variety* iff it is closed under subalgebras, homomorphic images and direct products.

Theorem (Birkhoff's theorem)

A class K is a variety iff $K = \mathrm{Mod}(\Phi)$ for some set of equations Φ.

Example

Let $\Sigma = \langle \{S\}, \Omega \rangle$ where $\Omega_{\epsilon,S} = \{a, b\}$. Suppose that we would like to specify, using equations, the class of all Σ-algebras with exactly two elements. Birkhoff's theorem states that it can not be done.

Example

Let $\Sigma = \langle \{S\}, \Omega \rangle$ where $\Omega_{\epsilon,S} = \{0\}$ and $\Omega_{S,S} = \{\times\}$.
The class K of Σ-algebras satisfying the familiar cancellation law: if $a \neq 0$ and $a \times b = a \times c$ then $b = c$, is not a variety.

Other specification languages

- First order logic (FOL)

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations

(This is the language used in cafeOBJ)

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations
(This is the language used in cafeOBJ)
- Partial Algebra - partial functions

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations

(This is the language used in cafeOBJ)

- Partial Algebra - partial functions
- Error Algebras

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations
(This is the language used in cafeOBJ)
- Partial Algebra - partial functions
- Error Algebras
- Ordered sorted algebras (order on sorts)

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations
(This is the language used in cafeOBJ)
- Partial Algebra - partial functions
- Error Algebras
- Ordered sorted algebras (order on sorts)
- Multialgebra - nondeterministic functions

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations (This is the language used in cafeOBJ)
- Partial Algebra - partial functions
- Error Algebras
- Ordered sorted algebras (order on sorts)
- Multialgebra - nondeterministic functions
- Hidden and Observational logic

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations
(This is the language used in cafeOBJ)
- Partial Algebra - partial functions
- Error Algebras
- Ordered sorted algebras (order on sorts)
- Multialgebra - nondeterministic functions
- Hidden and Observational logic
- K-logics

Other specification languages

- First order logic (FOL)
- Fragments of FOL: Algebraic signatures; Horn logic; conditional equations
(This is the language used in cafeOBJ)
- Partial Algebra - partial functions
- Error Algebras
- Ordered sorted algebras (order on sorts)
- Multialgebra - nondeterministic functions
- Hidden and Observational logic
- K-logics
- More abstract - INSTITUTIONS.

Where is the Category Theory in this Module?

- Classes of algebras with respective morphisms defines a category.
  - Exercise – prove the validity of the category axioms
- A category of specifications can be naturally defined.
  - Exercise – define a suitable notion of specifications morphism
- The quotient construction is functorial
  - Exercise – show it
- ...

Where is the Category Theory in this Module?

Algebra categorically – to be revisited in the next module

- notion of algebra
- derivation of a polinomial functor F_Σ from an one-sorted algebraic signature Σ

An example

Any model of the signature

Sorts $account$

Ops $new :\to account$

$undo : account \to account$

$deposit : account \times \mathbb{Z} \to account$

$debit : account \times \mathbb{Z} \to account$

is an algebra

$$1 + X + X \times \mathbb{Z} + X \times \mathbb{Z} \xrightarrow{[undo, deposit, debit]} X$$