Cours 2-5
Démonstration automatique
(48 heures, 6 ECTS)

Évelyne Contejean

21 septembre 2012

Intervenants

Pierre Courtieu — CEDRIC, CNAM & LRI, Paris 11

Pierre.Courtieu@cnam.fr

Sylvain Conchon — LRI, Paris 11

Sylvain.Conchon@lri.fr

Évelyne Contejean — LRI, Paris 11

Evelyne.Contejean@lri.fr

Xavier Urbain — CEDRIC & LRI, ENSIIE

Xavier.Urbain@ensiie.fr

Ralf Treinen — PPS, Paris 7

treinen@pps.univ-paris-diderot.fr

Motivation

Mécaniser la recherche d'un raisonnement simple possible à partir de faits et de règles de déduction.

Applications :

- Preuve de théorèmes mathématiques du 1er ordre
- Automatisation partielle des preuves dans un démonstrateur interactif (*cfr* cours 2-7-2)
- Terminaison et propriétés de fonctions
- Preuves de programmes C, java, . . . (*cfr* cours 2-36-1)

Communauté

Outils :
Otter, CiME, E-prover, H1, Vampire, Waldmeister,
Aprove, Matchbox, Muterm, VMTL, TALP, TTT,
Simplify, Alt-Ergo, Barcelogic, CVC3, Yices, Z3

Équipes (académiques et R&D) :
France, Allemagne, Autriche, Espagne, Grande-Bretagne,
Pays-Bas, Suède, USA, Japon

Objectifs du cours

Fournir les bases nécessaires pour

- comprendre le fonctionnement et les fondements théoriques des outils de démonstration automatique
- coder de tels outils.

Thèmes abordés

- Traitement de l'égalité par récriture
- Contraintes du premier ordre
- Résolution
- Solveurs modulo théories (SMT)

Calendrier prévisionnel

- 21/09 EC
- 28/09 EC
- 05/10 EC
- 12/10 XU
- 19/10 XU
- 26/10 XU
- 02/11
- 09/11 XU + PC
- 16/11 PC
- 23/11 PC 1h30
- 30/11 PARTIEL/EXAM
- 07/12 PARTIEL/EXAM
- 14/12 RT
- 21/12 EC 1h30
- 28/12 VACANCES
- 04/01 VACANCES
- 11/01 RT
- 18/01 RT
- 25/01 RT
- 01/02 SC
- 08/02 SC
- 15/02 SC
- 22/02
- 01/03
- 08/03 EXAM
- 15/03 EXAM

Modalités de contrôle

- 1 projet en récriture : P_1
- 1 projet SMT : P_2
- 1 examen final : E

$$note = max(E, (P_1 + P_2 + 2 * E)/4)$$

Traitement de l'égalité par la récriture

Comment savoir si des égalités sont conséquences d'autres égalités ?

$$\left\{ \begin{array}{l} \forall x, y, z, \quad (x \bullet y) \bullet z = x \bullet (y \bullet z) \bigwedge \\ \forall x, \quad x \bullet e = x \bigwedge \\ \forall x, \quad x \bullet I(x) = e \end{array} \right\} \quad \Longrightarrow \quad (\forall x, \quad e \bullet x = x)$$

$$\left\{ \begin{array}{l} \forall l, nil \# l = l \bigwedge \\ \forall x, l_1, l_2, \quad (cons \ x \ l_1) \# l_2 = cons \ x \ (l_1 \# l_2) \end{array} \right\}$$
$$\Longrightarrow$$
$$(\forall l_1, l_2, l_3, \quad (l_1 \# l_2) \# l_3 = l_1 \# (l_2 \# l_3))$$

Algèbres universelles

ou

Algèbres de termes

Intuition

Une vision uniforme et abstraite des objets (1er ordre) dans différents domaines :

- mathématiques, éléments de groupes, d'anneaux, d'espaces vectoriels et autres structures
- programmation, structures de données
- logique

Exemple

```
type penao : Zero | Succ of peano;;
let rec add(x,y) =
  match y with
  Zero -> x
| Succ(y) -> Succ(add(x,y));;
let rec mul(x,y) =
  match y with
  Zero -> Zero
| Succ(y) -> add(x,(mul(x,y)));;
let rec plus_petit (x,y) =
  match x with
  Zero -> true
| Succ x' -> ...
```

exemples de termes : `Zero`, `Succ (Succ (Succ Zero))`

`add (Zero, (mul ((Succ Zero), (Succ (Succ Zero)))))`

`Succ`, `add Zero`, `mul` ne sont pas des termes

Définition formelle

Définition (Signature)

Une signature est un triplet $(\mathscr{S}, \mathscr{F}, \tau)$,

- $\mathscr{S}$ *est un ensemble non vide de sortes,*
- $\mathscr{F}$ *est un ensemble de symboles de fonctions.*
- $\tau : \mathscr{F} \to \mathscr{S}^+$. *Si* $\tau(f) = (s_1, \ldots, s_n, s)$, *on note*

$$f : s_1 \times s_2 \times \ldots \times s_n \to s$$

domaine de $f = s_1 \times \ldots \times s_n$
codomaine de $f = s$
arité de $f = n$.
symboles de fonction d'arité 0 : symboles de constante

Signature de l'exemple peano

$$\mathscr{S} = \{peano, bool\}$$

$$\mathscr{F} = \{Zero, Succ, add, mul, plus\_petit\}$$

$Zero : peano$
$Succ : peano \rightarrow peano$
$add, mul : peano \times peano \rightarrow peano$
$plus\_petit : peano \times peano \rightarrow bool$

Définition des termes, v1

$(\mathscr{S}, \mathscr{F}, \tau)$ une signature,
$\mathscr{X} = \biguplus_{s \in \mathscr{S}} \mathscr{X}_s$ un ensemble de symboles de variables
$\mathscr{F} \cap \mathscr{X} = \emptyset$

Définition (Termes)

- $x \in \mathscr{X}_s$ *est un terme de sorte* s
- *si* $f \in \mathscr{F}$ *et* $f : s_1 \times \ldots \times s_n \to s$,
  t_i *un terme de sorte* s_i, $1 \leqslant i \leqslant n$,
  alors $f(t_1, \ldots, t_n)$ *est un terme de sorte* s.

$\mathcal{T}(\mathscr{F}, \mathscr{X})$: termes bâtis sur $(\mathscr{S}, \mathscr{F}, \tau)$ et $\mathscr{X}$
termes clos : $\mathcal{T}(\mathscr{F}) = \mathcal{T}(\mathscr{F}, \emptyset)$
$\mathcal{T}(\mathscr{F})$ est non vide ssi il existe $f \in \mathscr{F}$, f symbole de constante

Digression sur la terminologie « symbole » de fonctions/variables

On ne veut surtout PAS CALCULER

cfr Modélisation en CAML

Variables d'un terme

Définition (Ensemble de variables d'un terme)

$Var(t)$ est défini inductivement par :

- *si x appartient à $\mathscr{X}_s$, $Var(x) = \{x\}$.*
- $Var(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} Var(t_i)$.

$$\mathrm{Var}(add(Zero, Zero)) = \{\}$$
$$\mathrm{Var}(mul(Succ(x), add(Zero, y))) = \{x, y\}$$

Terme linéaire

Définition (Terme linéaire)

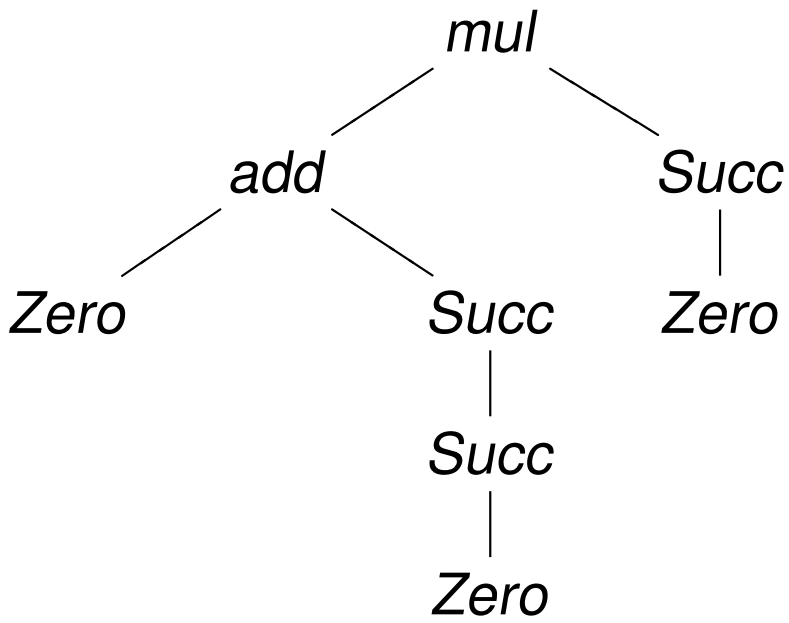
- $x \in \mathcal{X}_s$ *est un terme linéaire*
- $f(t_1, \ldots, t_n)$ *est linéaire si* t_i *est linéaire,* $1 \leqslant i \leqslant n$ *et les* $Var(t_i)$ *sont deux à deux disjoints.*

$mul(x, add(y, z))$ est linéaire
$plus\_petit(x, x)$ n'est pas linéaire

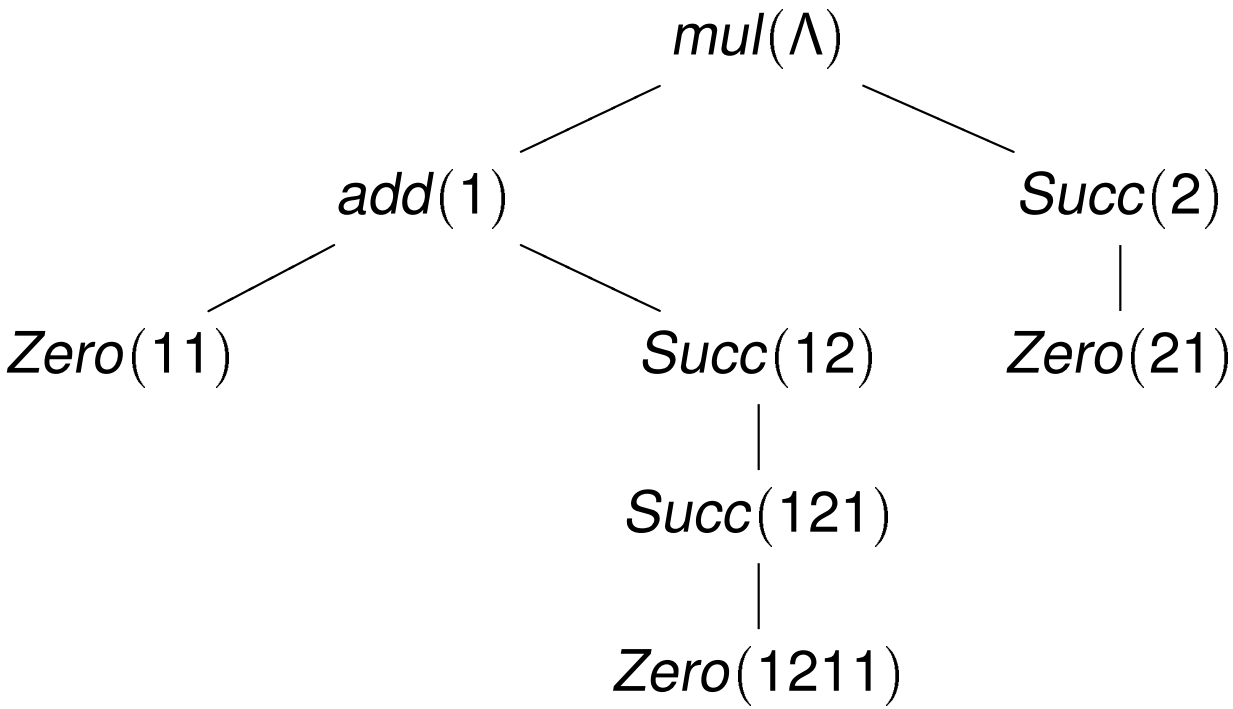
Les termes vus comme arbres

terme : arbre fini étiqueté par $\mathscr{X}$ et $\mathscr{F}$

$$mul(add(Zero, Succ(Succ(Zero))), Succ(Zero))$$



Les termes vus comme arbres (suite)



Positions

$\mathbb{N}_+^*$ ensemble des séquences sur $\mathbb{N}_+$
Λ séquence vide, $p \cdot q$ concaténation de p et q

Définition (Ordre préfixe $\leqslant_{\text{pref}}$ sur $\mathbb{N}_+^*$)

$$p \leqslant_{pref} q \text{ si et seulement si } \exists r \in \mathbb{N}_+^* \quad p \cdot r = q$$

Définition (Ensemble clos par préfixe)

$$\forall p, q \in \mathbb{N}_+^* \quad (p \leqslant_{pref} q) \wedge q \in \mathscr{P} \Rightarrow p \in \mathscr{P}$$

Définition (Feuille)

$p \in \mathscr{P}$, p est une feuille de $\mathscr{P}$ si p est maximal dans $\mathscr{P}$ pour $\leqslant_{pref}$.

Arbre de positions

Définition (Arbre de positions)

$\mathscr{P}$ *clos par préfixe et*

$$\forall p \in N_+^* \quad \forall n, i \in \mathbb{N}_+ \quad (p \cdot n \in \mathscr{P}) \wedge (i \leqslant n) \Rightarrow p \cdot i \in \mathscr{P}$$

arbre de positions = ensemble des positions d'un terme

Définition des termes, v2

Définition (Terme)

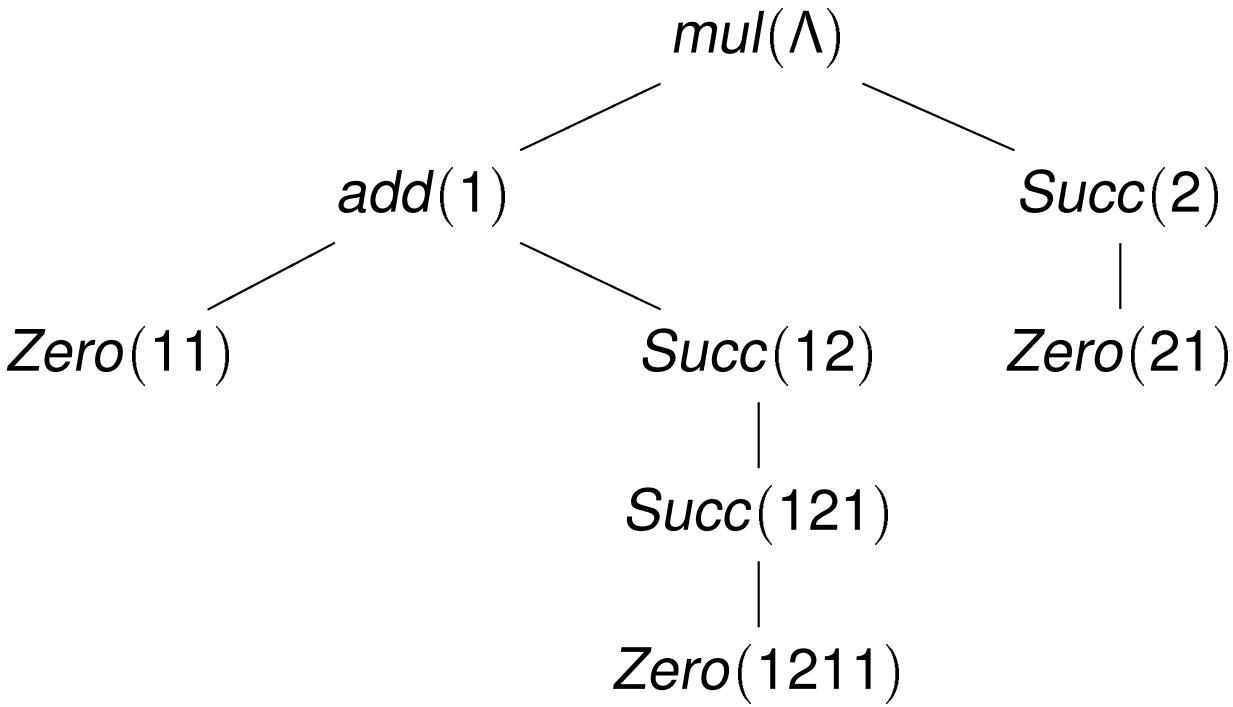
$(\mathscr{S}, \mathscr{F}, \tau)$ une signature, $\mathscr{X}$ un ensemble de symboles de variable, $\mathscr{P}$ un arbre de positions.
Une fonction de $t : \mathscr{P} \to \mathscr{F} \cup \mathscr{X}$ défini un terme quand

- *Si $t(p)$ est variable ou constante, alors p est une feuille de $\mathscr{P}$.*
- *Si $t(p) = f$, $f : s_1 \times \ldots \times s_n \to s$, alors $p \cdot i \in \mathscr{P}$, pour $i = 1, \ldots n$, $f_i = t(p \cdot i)$ a pour codomaine s_i, et*

$$\forall j \in \mathbb{N}_+ \quad p \cdot j \in \mathscr{P} \Rightarrow j \leqslant n$$

$\mathscr{P}$ ensemble des positions de t, noté $\mathrm{Pos}(t)$.

Les termes vus comme arbres (fin)



$$\mathrm{Pos}(t) = \{\Lambda, 1, 2, 11, 12, 21, 121, 1211\}$$

$$t(\Lambda) = mul \qquad t(12) = Succ$$
$$t(1) = add \qquad t(21) = Zero$$
$$t(2) = Succ \qquad t(121) = Succ$$
$$t(11) = Zero \qquad t(1211) = Zero$$

Lien entre les définitions

v1 : seulement des arbres finis
v2 : aussi des arbres infinis

Exemple

$\mathscr{P} = \{1^n \mid n \in \mathbb{N}\}$ *est un arbre de positions infini*
$t(p) = Succ$
$Succ(Succ(Succ(\ldots(Succ(\ldots$

v1 = v2 + $\mathscr{P}$ fini

Remarque : si t de sorte s au sens v1,
alors $t(\Lambda)$ au sens v2 a pour codomaine s.
profondeur de t : longueur max. des positions de $\mathrm{Pos}(t)$
taille de t : cardinal de $\mathrm{Pos}(t)$

Sous-termes

sous-terme = sous-expression

Définition

t terme de $\mathcal{T}(\mathcal{F}, \mathcal{X})$, p une position de $Pos(t)$.
$t|_p$ sous-terme de t à la position p est défini par

$$Pos(t|_p) = \{q \in \mathbb{N}_+^* \mid p \cdot q \in Pos(t)\}$$
$$t|_p(q) = t(p \cdot q)$$

Alternative

Définition

- $t|_\Lambda = t$
- $x|_{i \cdot p}$ *n'est pas défini pour* $x \in \mathcal{X}$
- $f(t_1, \ldots, t_i, \ldots, t_n)|_{i \cdot p} = t_i|_p$

Sous-termes

Notation (Relation sous-terme)

$t \triangleright s$ (ou $s \triangleleft t$) s'il existe une position $p \neq \Lambda$, telle que $t|_p = s$.

Exemple

$$t = mul(add(Zero, Succ(Succ(Zero))), Succ(Zero))$$
$$t|_{12} = Succ(Succ(Zero))$$

Exercice

Vérifier que la première définition est correcte, i.e.

- $Pos(t|_p)$ *est un arbre de positions,*
- *les conditions de la définition v2 sur l'arité et les sortes sont satisfaites.*

Vérifier que les deux définitions sont équivalentes.

Remplacement de sous-termes

Définition

t et u deux termes de $\mathcal{T}(\mathcal{F}, \mathcal{X})$, p une position de t telle que $t|_p$ et u de même sorte. Le terme $t[u]_p$ est le terme défini par

- $t[u]_\Lambda = u$
- $f(t_1, \ldots, t_i, \ldots, t_n)[u]_{i \cdot p} = f(t_1, \ldots, t_i[u]_p, \ldots, t_n)$

$t[u]_p = t$, avec u à la position p

Exemple

$$t = mul(add(Zero, Succ(Succ(Zero))), Succ(Zero))$$
$$u = mul(Zero, Zero)$$
$$t[u]_{12} = mul(add(Zero, mul(Zero, Zero)), Succ(Zero))$$

Sous-termes : identités remarquables

Exercice

t et u deux termes de $\mathcal{T}(\mathcal{F}, \mathcal{X})$, $p \in Pos(t)$ *avec* $t|_p$ *et u ont la même sorte. Vérifier que*

- $t = t[t|_p]_p$,
- $u = (t[u]_p)|_p$.

Substitutions

Définition

- *une application des variables dans les termes qui conserve les sortes*
- *égale à l'identité sauf sur un nombre fini de symboles de variables* $\{x_1, \ldots, x_n\}$

$\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ si $t_i = \sigma(x_i)$

Domaine $\mathrm{Dom}(\sigma) = \{x_1, \ldots, x_n\}$.

Si tous les $t_1, \ldots, t_n$ sont clos, σ est close.

Notation postfixée : $x\sigma$.

Extension naturelle aux termes

Fonction unique $\mathscr{H}_\sigma$ des termes dans les termes

- $\mathscr{H}_\sigma(x) = x$ si $x \notin \mathrm{Dom}(\sigma)$,
- $\mathscr{H}_\sigma(x_i) = x_i\sigma$ si $x_i \in \mathrm{Dom}(\sigma)$,
- $\mathscr{H}_\sigma(f(s_1, \ldots, s_n)) = f(\mathscr{H}_\sigma(s_1), \ldots, \mathscr{H}_\sigma(s_n))$

On identifie σ et $\mathscr{H}_\sigma$

Renommage

Renommage : analogue de l'α-conversion,

Définition (Renommage)

$\sigma = \{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}$ *avec* y_i *variables deux à deux distinctes.*

t un terme de $\mathcal{T}(\mathscr{F}, \mathscr{X})$, ρ un renommage avec $\mathrm{Var}(t) \subset \mathrm{Dom}(\rho)$

$t' = t\rho$ est appelé un renommage de t par ρ,

$t \stackrel{\bullet}{=} t'$.

Exercice

Montrer que $\stackrel{\bullet}{=}$ *est une relation d'équivalence.*

Points délicats

Bien distinguer renommage sur les substitutions et les termes :

- $\rho = \{x \mapsto x', y \mapsto y'\}$ et $t = add(add(x, y), z)$
  on ne peut pas parler du renommage $add(add(x', y'), z)$ de t par ρ
  car $z \notin \mathrm{Dom}(\rho)$,
- Solution : étendre ρ en $\rho' = \{x \mapsto x', y \mapsto y', z \mapsto z\}$,
  parler du renommage de t en $add(add(x', y'), z)$ par ρ'.
- $add(x', x')$ n'est pas un renommage de $t' = add(x, y)$,
  on ne peut pas trouver un renommage ρ'' tq $t'\rho'' = add(x', x')$
  instance stricte.

Composition

composition des substitutions = composition des fonctions

Proposition

La composée de deux substitutions est une substitution :

- *conserve les sortes*
- *domaine fini*

Attention notation postfixe : $\sigma \circ \theta$ s'écrit $\theta\sigma$

Définition

σ est idempotente si $\sigma\sigma = \sigma$.

Toute substitution close est idempotente.

Subsumption

Lien substitution-instance-subsumption :

Définition (Subsumption)

s et t deux termes, s est plus général que t,
s'il existe une substitution θ telle que $s\theta = t$.

Notation $s \preccurlyeq t$, *s* subsume *t*, *t* est une instance (par θ) de *s*

Extension naturelle aux substitutions.

Interprétation des termes non clos

$[\![t]\!]$ = ensemble de des instances closes de t

Proposition

s et t deux termes.

- $s \leqslant\!\!\bullet\, t$ *si et seulement si* $[\![t]\!] \subseteq [\![s]\!]$.
- $s \doteq t$ *si et seulement si* $[\![t]\!] = [\![s]\!]$.

Justification de terminologie : s est dit plus général que t si $s \leqslant\!\!\bullet\, t$ car s représente un ensemble d'instances qui contient celui de t.

Des termes syntaxiques aux véritables objets

Les termes sont interprétés en les objets d'intérêt *cfr* CAML

$\mathscr{F}$-algèbres

Définition

$(\mathscr{S}, \mathscr{F}, \tau)$ une signature. Une $\mathscr{F}$-algèbre est constituée

- *d'un support non vide $\mathscr{A}_s$ associé à chaque sorte s de $\mathscr{S}$,*
- *d'une interprétation $f_{\mathscr{A}}$ pour chaque f de $\mathscr{F}$ telle que si*

$$f : s_1 \times \ldots s_n \rightarrow s,$$

alors $f_{\mathscr{A}}$ est une application de

$$\mathscr{A}_{s_1} \times \ldots \times \mathscr{A}_{s_n} \rightarrow \mathscr{A}_s.$$

Interprétation des termes clos

Définition

$$[\![f(t_1, \ldots, t_n)]\!] = f_{\mathscr{A}}([\![t_1]\!], \ldots, [\![t_n]\!])$$

Cas de base : les symboles de constantes, interprétés en constantes.

Il n'y a pas de symboles de variables.

$\mathscr{F}$-algèbres : exemple des entiers de Peano

Exemple

- - *Le support de la sorte peano est l'ensemble* $\mathbb{N}$,
  - *le support de la sorte bool est l'ensemble des booléens* $\{vrai, faux\}$.
- - *L'interprétation de la constante Zero est égale à 0,*
  - *celle de Succ est la fonction* $n \mapsto n + 1$,
  - *celle de plus_petit est* $\leqslant$,
  - *celle de add est +,*
  - *et celle de mul est* $\times$.
- $[\![mul(add(Zero, Succ(Succ(Zero))), Succ(Zero))]\!] = 2.$

$\mathscr{F}$-algèbres « naturelles »

$(\mathscr{S}, \mathscr{F}, \tau)$ une signature, si $\mathcal{T}(\mathscr{F})$ contient au moins un terme de chaque sorte, $\mathcal{T}(\mathscr{F})$ est une $\mathscr{F}$-algèbre :

- le support de $s \in \mathscr{S}$ est l'ensemble (non-vide) des termes de sorte s de $\mathcal{T}(\mathscr{F})$,
- l'interprétation d'un symbole de fonction $f : s_1 \times \ldots s_n \to s$, est définie par

$$f_{\mathcal{T}(\mathscr{F})}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$$

$\mathcal{T}(\mathscr{F}, \mathscr{X})$ est aussi une $\mathscr{F}$-algèbre (attention à la non-vacuité).

Interprétation des termes (non clos)

Problème : comment interpréter les symboles de variables ?

terme = ensemble de ses instances closes

interprétation d'un terme $\sim$ ensemble des interprétations de ses instances closes

$\mathscr{A}$-assignation : un ensembles de fonctions $\mathscr{I}_s$ de $\mathscr{X}_s$ dans $\mathscr{A}_s$

$$[\![x]\!]_{\mathscr{I}} = \mathscr{I}(x)$$
$$[\![f(t_1, \ldots, t_n)]\!]_{\mathscr{I}} = f_{\mathscr{A}}([\![t_1]\!]_{\mathscr{I}}, \ldots, [\![t_n]\!]_{\mathscr{I}})$$

Remarque : pour la $\mathscr{F}$-algèbre $\mathscr{T}(\mathscr{F}, \mathscr{X})$, une assignation est une substitution infinie

Homomorphismes de $\mathscr{F}$-algèbres

Définition

$\mathscr{A}$ et $\mathscr{B}$ deux $\mathscr{F}$-algèbres. Un homomorphisme de $\mathscr{A}$ dans $\mathscr{B}$ est un ensemble d'applications $\{h_s \mid s \in \mathscr{S}\}$ tel que

- *pour toute sorte s de $\mathscr{S}$, h_s est une application de $\mathscr{A}_s$ dans $\mathscr{B}_s$,*
- *pour tout symbole de fonction $f : s_1 \times \ldots \times s_n \to s$*

$$\forall a_1, \ldots, a_n \in \mathscr{A} \quad h_s(f_{\mathscr{A}}(a_1, \ldots, a_n)) = f_{\mathscr{B}}(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$$

$\mathscr{A}$-assignation : homomorphisme de $\mathscr{T}(\mathscr{F}, \mathscr{X})$ dans la $\mathscr{F}$-algèbre $\mathscr{A}$ (définie de façon unique à partir des valeurs prises sur $\mathscr{X}$)

Représenter les objets par des termes ?

avec les termes, on ne calcule pas : $add(Zero, x) \neq x$.

identifier tous les termes qui « représentent » la même chose.

préciser la notion de compatibilité nécessaire (sur les $\mathscr{F}$-algèbres)

Algèbres quotients I

Définition (Précongruence, congruence)

$\mathscr{A}$ *une* $\mathscr{F}$*-algèbre.* *précongruence* $\sim$ *:*

- *relation sur* $\mathscr{A}$
- *compatible avec la structure de* $\mathscr{F}$*-algèbre*

$$t_1 \sim u_1 \wedge \ldots t_n \sim u_n \Rightarrow f_{\mathscr{A}}(t_1, \ldots, t_n) \sim f_{\mathscr{A}}(u_1, \ldots, u_n)$$

congruence = précongruence + relation d'équivalence

Algèbres quotients II

Définition

$\mathscr{A}$ une $\mathscr{F}$-algèbre, $\sim$ congruence sur $\mathscr{A}$. $\mathscr{A}/\sim$ $\mathscr{F}$-algèbre définie par :

- *support pour s de $\mathscr{S}$: $\{\bar{t} \mid t \in \mathscr{A}_s\}$, $\bar{t}$ = classe d'équivalence de t modulo $\sim$.*
- *interprétation de $f : s_1 \times \ldots \times s_n \to s$:*

$$f_{\mathscr{A}/\sim}(\overline{t_1}, \ldots, \overline{t_n}) = \overline{f_{\mathscr{A}}(t_1, \ldots, t_n)}$$

définition correcte :la classe de $f_{\mathscr{A}}(t_1, \ldots, t_n)$ ne dépend que des classes de $t_1, \ldots, t_n$, et pas des représentants choisis, car $\sim$ est une précongruence.

Exemple

$$\mathscr{S}'_{peano} = \{peano\}$$
$$\mathscr{F}'_{peano} = \{Zero, Succ, add, mul\}$$

$(\mathbb{N}, 0, n \mapsto n+1, +, \times)$ est une $\mathscr{F}'_{peano}$-algèbre.

$\equiv_p$ (égal modulo p) est une congruence

$(\mathbb{N}, 0, n \mapsto n+1, +, \times)/\equiv_p$ est l'algèbre quotient

$$(\mathbb{Z}/p\mathbb{Z}, 0, n \mapsto n+1, +, \times)$$

Logique équationnelle

ou

encore une vision duale syntaxique/sémantique des objets à identifier

Équations

paire de termes de même sorte $\{s, t\}$

notation usuelle $s = t$

Définition (Modèle)

E un ensemble d'équations sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$. $\mathcal{A}$, $\mathcal{F}$-algèbre est un modèle de E si pour toute $\mathcal{A}$-assignation $\mathcal{I}$

$$\forall s, t.\ \ s = t \in E \implies [\![s]\!]_{\mathcal{I}} = [\![t]\!]_{\mathcal{I}}$$

notation $\mathcal{A} \models E$.

les variables de E sont quantifiées universellement (de façon implicite)

notation $E \models s = t$ si tout modèle de E est aussi un modèle de $\{s = t\}$

théorie équationnelle associée à E : $\{s = t \mid E \models s = t\}$

Exemple

$(\mathbb{N}, 0, n \mapsto n+1, \leqslant, +, \times)$ est un modèle de

$$\left\{ \begin{array}{rcl} add(x,y) & = & add(y,x) \\ mul(add(x,y),z) & = & add(mul(x,z),mul(y,z)) \end{array} \right\}$$

et

$$\left\{ \begin{array}{rcl} add(x,Zero) & = & x \\ add(x,Succ(y)) & = & Succ(add(x,y)) \end{array} \right\} \models$$

$$add(x,Succ(Succ(y)) = Succ(Succ(add(x,y))$$

La congruence $=_E$

$\mathcal{T}(\mathcal{F}, \mathcal{X})$ une algèbre et E un ensemble d'équations

$=_E$ est la plus petite congruence sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$ telle que, pour toute substitution σ,

$$\forall s = t \in E \;\; s\sigma =_E t\sigma$$

$=_E$ existe et est unique

$\mathcal{T}(\mathcal{F}, \mathcal{X})/ =_E$ est une $\mathcal{F}$-algèbre de façon canonique et par définition

$$\mathcal{T}(\mathcal{F}, \mathcal{X})/ =_E \models E$$

$\mathcal{T}(\mathcal{F})/ =_E$ a un status spécial parmi les modèles de E :

Proposition

$\mathcal{A}$ une $\mathcal{F}$-algèbre, $\mathcal{A} \models E$. Si $\mathcal{F}$ contient au moins un symbole de chaque sorte, il existe un unique homomorphisme de $\mathcal{T}(\mathcal{F})/ =_E$ dans $\mathcal{A}$.

Questions liées à l'égalité

$\mathcal{T}(\mathcal{F}, \mathcal{X})$ une algèbre, E un ensemble fini et $s = t$ une équation

Définition

problème du mot (associé à) $s = t$: décider si $E \models s = t$

Définition

problème d'unification (modulo E) (associé à) $s = t$:
trouver toutes les substitutions σ telles que $E \models s\sigma = t\sigma$

Définition

problème inductif modulo E (associé à) $s = t$:
décider si $\mathcal{T}(\mathcal{F})/=_E \models s = t$

Exemple

$$E = \{add(x, Zero) = x;\ \ add(x, Succ(y)) = Succ(add(x, y))\}$$

Une solution au problème d'unification modulo E

$$add(x, Succ(y)) = Succ(Succ(z))$$

est

$$\sigma = \{y \mapsto Succ(u); z \mapsto add(x, u)\}$$

car

$$\begin{aligned} add(x, Succ(y))\sigma &= add(x, Succ(Succ(u))) \\ Succ(Succ(z))\sigma &= Succ(Succ(add(x, u))) \end{aligned}$$

Première mécanisation : raisonnement équationnel

$$\frac{}{s = s}$$ Réflexivité

$$\frac{s = t}{t = s}$$ Symétrie

$$\frac{s = t \qquad t = u}{s = u}$$ Transitivité

$$\frac{s = t}{u[s\sigma]_p = u[t\sigma]_p}$$ Remplacement

Logique équationnelle

faits ou axiomes : un ensemble d'équations fixées E

règles de déduction : les règles du raisonnement équationnel

arbre de dérivation

$s = t$ obtenu à partir de E et des règles du raisonnement équationnel

$$E \vdash s = t$$

Exemple

$$\left\{\begin{array}{rcl} x \cdot e & = & x \\ x \cdot I(x) & = & e \\ (x \cdot y) \cdot z & = & x \cdot (y \cdot z) \end{array}\right\} \vdash e \cdot x$$

$$\dfrac{\dfrac{\dfrac{(x \cdot I(x)) = e}{e = (x \cdot I(x))}}{e \cdot I(I(x)) = (x \cdot I(x)) \cdot I(I(x))} \qquad \dfrac{(x \cdot y) \cdot z = x \cdot (y \cdot z)}{(x \cdot I(x)) \cdot I(I(x)) = x \cdot (I(x) \cdot I(I(x)))}\, x \cdot I(x) = e}{e \cdot I(I(x)) = x \cdot (I(x) \cdot I(I(x)))} \qquad x \cdot (I(x) \cdot I(I(x))) = x \cdot e}{e \cdot I(I(x)) = x \cdot e} \qquad x \cdot e = x}{e \cdot I(I(x)) = x}$$

$$\dfrac{\dfrac{\dfrac{(x \cdot e) = x}{x = (x \cdot e)}}{x \cdot I(I(y)) = (x \cdot e) \cdot I(I(y))} \qquad \dfrac{(x \cdot y) \cdot z = x \cdot (y \cdot z)}{(x \cdot e) \cdot I(I(y)) = x \cdot (e \cdot I(I(y)))} \qquad \dfrac{\vdots}{e \cdot I(I(x)) = x}}{x \cdot I(I(y)) = x \cdot y} \qquad x \cdot (e \cdot I(I(y))) = x \cdot y}{(x \cdot e) \cdot I(I(y)) = x \cdot y}$$

$$\dfrac{\dfrac{e \cdot I(I(x)) = e \cdot x}{e \cdot x = e \cdot I(I(x))} \qquad \dfrac{\vdots}{e \cdot I(I(x)) = x}}{e \cdot x = x}$$

Équivalence syntaxe-sémantique

Théorème (Birkhoff)

Si chaque sorte contient au moins un terme clos, alors

$$E \vdash s = t \Leftrightarrow E \models s = t \Leftrightarrow s =_E t$$

Étape équationnelle

$=_E$: plus petite congruence sur $\mathcal{T}(\mathcal{F}, \mathcal{X})$ qui contient E.

$\leftrightarrow_E$: la plus petite précongruence contenant E

$$s \longleftrightarrow_E t \quad \text{si} \quad s = s[u\sigma]_p \quad t = s[v\sigma]_p \quad \text{où} \quad u = v \in E$$

on peut préciser

$$s \longleftrightarrow^p_{u=v,\sigma} t$$

$$=_E \quad \text{est la relation} \quad \longleftrightarrow^*_E$$

Exemple

$$
\begin{aligned}
e \cdot x \quad & \longleftrightarrow^{2}_{N} e \cdot (x \cdot e) \longleftrightarrow^{22}_{I} e \cdot (x \cdot (I(x) \cdot I(I(x)))) \\
& \longleftrightarrow^{2}_{A} e \cdot ((x \cdot I(x)) \cdot I(I(x))) \longleftrightarrow^{21}_{I} e \cdot (e \cdot I(I(x))) \\
& \longleftrightarrow^{\Lambda}_{A} (e \cdot e) \cdot I(I(x)) \longleftrightarrow^{1}_{N} e \cdot I(I(x)) \longleftrightarrow^{1}_{I} (x \cdot I(x)) \cdot I(I(x)) \\
& \longleftrightarrow^{\Lambda}_{A} x \cdot (I(x) \cdot I(I(x))) \longleftrightarrow^{2}_{I} x \cdot e \longleftrightarrow^{\Lambda}_{N} x
\end{aligned}
$$

Exercice

En général le problème du mot et le problème inductif associé à une même équation ont des comportements différents.
Considérons la signature $(\mathscr{S}''_{peano}, \mathscr{F}''_{peano}, \tau''_{peano})$ qui comporte une seule sorte et un symbole de fonction constante *Zero*, un symbole unaire *Succ* et un symbole binaire *add*. Soit E l'ensemble d'équations

$$\{add(x, Zero) = x;\ \ add(x, Succ(y)) = Succ(add(x, y))\}$$

Montrer que la propriété $\mathcal{T}(\mathscr{F}''_{peano})/=_E \models add(Zero, x) = x$ est vraie, mais que $E \models add(Zero, x) = x$ est faux.

Récriture

ou

les équations dirigées

Étape de récriture

règle : couple de termes (l, r) noté $l \to r$

$$s \longrightarrow_R t \quad \text{si} \quad s = s[l\sigma]_p \quad t = s[r\sigma]_p \quad \text{où} \quad l \to r \in R$$

on peut préciser

$$s \longrightarrow^p_{l \to r, \sigma} t$$

$$E_R = \{l = r \mid l \to r \in R\}$$

Notations

$\rightarrow$ relation sur un ensemble $\mathscr{A}$

$\rightarrow^*$ clôture réflexive transitive

$\rightarrow^+$ clôture transitive

$\leftarrow$ relation inverse

$\leftrightarrow$ clôture symmétrique

Forme normale

Définition (Forme normale)

$\rightarrow$ une relation sur $\mathscr{A}$. x est en forme normale pour $\rightarrow$ s'il n'existe pas d'élément y tel que $x \rightarrow y$.
y est une forme normale de x s'il est en forme normale et $x \rightarrow^* y$.

Confluence sur les relations abstraites

Définition (Church-Rosser, confluence, confluence locale)

Soit $\mathscr{A}$ un ensemble. Une relation $\rightarrow_R$ sur $\mathscr{A}$

- *possède la propriété de Church-Rosser si et seulement si*

$$\forall x, y \in \mathscr{A},\ \ x \overset{*}{\underset{R}{\longleftrightarrow}} y \ \ \Rightarrow \ \ (\exists z \in \mathscr{A},\ \ x \overset{*}{\underset{R}{\rightarrow}} z \overset{*}{\underset{R}{\leftarrow}} y).$$

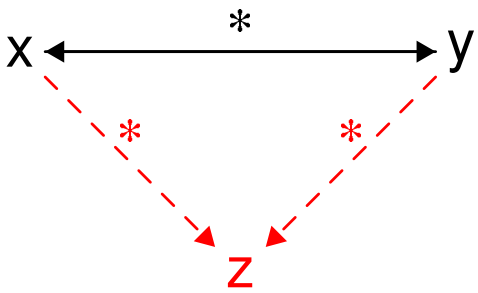
- *est confluente si et seulement si*

$$\forall x, y, z \in \mathscr{A},\ \ y \overset{*}{\underset{R}{\leftarrow}} x \overset{*}{\underset{R}{\rightarrow}} z \ \ \Rightarrow \ \ (\exists v \in \mathscr{A},\ \ y \overset{*}{\underset{R}{\rightarrow}} v \overset{*}{\underset{R}{\leftarrow}} z).$$

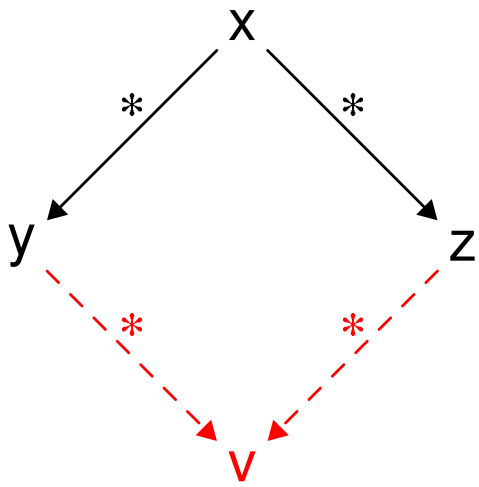
- *est localement confluente si et seulement si*

$$\forall x, y, z \in \mathscr{A},\ \ y \underset{R}{\leftarrow} x \underset{R}{\rightarrow} z \ \ \Rightarrow \ \ (\exists v \in \mathscr{A},\ \ y \overset{*}{\underset{R}{\rightarrow}} v \overset{*}{\underset{R}{\leftarrow}} z).$$

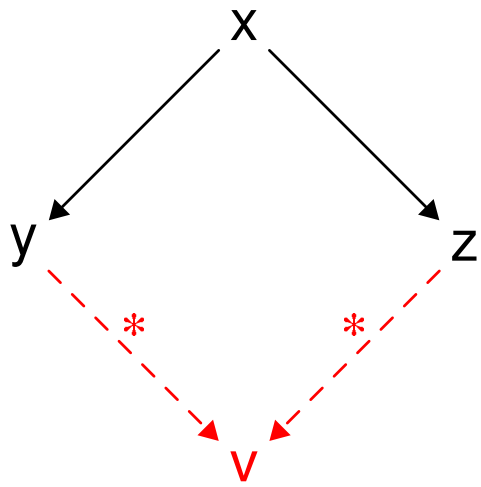
Définitions graphiques



Church-Rosser



Confluence



Confluence locale

Church-Rosser = confluence

Proposition

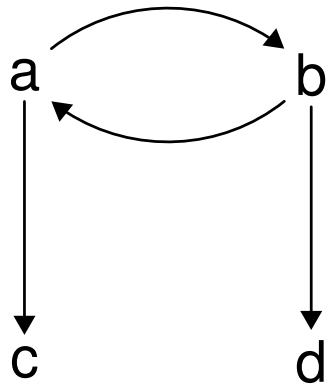
Une relation $\rightarrow$ possède la propriété de Church-Rosser si et seulement si elle est confluente.

confluence ≠ confluence locale

contre-exemple

$$\mathscr{A} = \{a, b, c, d\}$$

$$\{a \to b; a \to c; b \to a; b \to d\}$$



$\to$ est localement confluente, mais pas confluente

Lemme de Newman (1942)

Théorème

$\rightarrow$ une relation sur $\mathscr{A}$, telle que $\leftarrow$ est bien fondée.
$\rightarrow$ est localement confluente si et seulement si $\rightarrow$ est confluente.

Convergence

Définition

$\rightarrow$ une relation sur $\mathscr{A}$, $\rightarrow$ est convergente si elle est confluente et $\leftarrow_R$ bien fondée.

Lemme

$\rightarrow$ une relation convergente sur $\mathscr{A}$. Alors tout élément x de $\mathscr{A}$ a une forme normale unique qui est notée $x\downarrow$.