LC – Logique classique

Sylvain Brandel
2024 – 2025
sylvain.brandel@univ-lyon1.fr

Partie 3

LOGIQUE DU PREMIER ORDRE

Vocabulaire

- Symboles d'un langage (vocabulaire) du premier ordre :
  - $\mathcal{S}_{\mathcal{F}} = \{f, g, h, \dots\}$: symboles de fonctions avec fonction d'arité :
  $$ar : \mathcal{S}_{\mathcal{F}} \longrightarrow \mathbb{N} \setminus \{0\}$$
  - $\mathcal{S}_{\mathcal{C}} = \{a, b, c, \dots\}$: symboles de constantes (fonctions d'arité 0)
  - $\mathcal{S}_{\mathcal{R}} = \{P, Q, R, \dots\}$: symboles de relations (prédicats) avec fonction d'arité
  $$ar : \mathcal{S}_{\mathcal{R}} \longrightarrow \mathbb{N}$$

- Remarques
  - $\perp$ est un symbole de relation 0-aire
  - $=$ est un symbole de relation binaire

Termes

- On ajoute un ensemble infini de variables :
  - $\mathcal{V} = \{x, y, z \dots\}$: ensembles de variables

- Ensemble $\mathcal{T}$ des termes sur un langage $\mathcal{L}$:
  - Les variables et les constantes sont des termes
  - Si $t_1, \dots, t_n$ sont des termes et f un symbole de fonction tq $ar(f) = n$,
    alors $f(t_1, \dots, t_n)$ est un terme

- Un terme clos est un terme qui ne contient pas de variables

- $\mathcal{T}$ est le plus petit ensemble contenant les variables, les constantes,
  et stable par l'application des symboles de fonctions de $\mathcal{L}$ à des termes

Substitutions

- Substitution : fonction $\sigma : \mathcal{V} \longrightarrow \mathcal{T}$, domaine noté $dom(\sigma)$

- On note $[x_1 \coloneqq t_1, ..., x_n \coloneqq t_n]$ la substitution de domaine $\{x_1, \dots, x_n\}$ qui associe t_i à x_i pour $1 \leq i \leq n$

- Application d'une substitution σ sur un terme t, notée $t\sigma$:
  - Si $t = a$ (a : constante), $t\sigma = a$
  - Si $t = x,\ x \in dom(\sigma)$, $t\sigma = \sigma(x)$
  - Si $t = y,\ y \notin dom(\sigma)$, $t\sigma = y$
  - Si $t = f(t_1, \dots, t_n)$, $t\sigma = f(t_1\sigma, \dots, t_n\sigma)$

- Le terme u filtre le terme v s'il existe σ tq $u\sigma = v$

- Les termes u et v sont unifiables s'il existe σ tq $u\sigma = v\sigma$

Formules

- On ajoute les connecteurs et quantificateurs :
  - Connecteurs du calcul propositionnel : $\neg$, $\vee$, $\wedge$, $\Rightarrow$
  - Quantificateur universel : $\forall$
  - Quantificateur existentiel : $\exists$

- Ensemble $\mathcal{F}$ des formules :
  - Si $t_1, \dots, t_n$ sont des termes et R un symbole de relation tq $ar(R) = n$,
    alors $R(t_1, \dots, t_n)$ est une formule (atomique)
  - Si A est une formule, alors $\neg A$ est une formule
  - Si A et B sont des formules, alors $A \wedge B$, $A \vee B$, $A \Rightarrow B$ sont des formules
  - Si A est une formule et x une variable, alors $\forall x\ A$ et $\exists x\ A$ sont des formules

$\forall$ et $\exists$: priorité minimale

- Formule atomique :
  - Soit $\perp$
  - Soit $R(t_1, \dots, t_n)$ avec $t_1, \dots, t_n$: termes, R : symbole de relation n-aire

Formules

- Ensemble des sous-formules d'une formule A, noté $SF(A)$:
  - Si A est atomique, $SF(A) = \{A\}$
  - Si $A = \neg B \ ou \ \forall x \ B \ ou \ \exists x \ B$, $SF(A) = \{A\} \cup SF(B)$
  - Si $A = B \wedge C \ ou \ B \vee C \ ou \ B \Rightarrow C$, $SF(A) = \{A\} \cup SF(B) \cup SF(C)$

- Langage d'une formule A, noté $\mathcal{L}(A)$: l'ensemble (fini) des symboles de A

- Taille d'une formule A, notée $\tau(A)$:

  nombre de connecteurs et de quantificateurs apparaissant dans A :
  - Si A est atomique, $\tau(A) = 0$
  - Si $A = \neg B \ ou \ \forall x \ B \ ou \ \exists x \ B$, $\tau(A) = 1 + \tau(B)$
  - Si $A = B \wedge C \ ou \ B \vee C \ ou \ B \Rightarrow C$, $\tau(A) = 1 + \tau(B) + \tau(C)$

Variables libres et liées

- Ensemble des variables d'un terme t, noté $V(t)$:
  - Si t est une variable x, $V(t) = \{x\}$
  - Si t est une constante, $V(t) = \emptyset$
  - Si $t = f(t_1, \dots, t_n)$, $V(t) = V(t_1) \cup \dots \cup V(t_n)$

- Ensemble des variables libres d'une formule A, noté $FV(A)$:
  - Si $A = R(t_1, \dots, t_n)$ (R : symbole de relation), $FV(t) = V(t_1) \cup \dots \cup V(t_n)$
  - Si $A = \neg B$, $FV(A) = FV(B)$
  - Si $A = B \wedge C \ ou \ B \vee C \ ou \ B \Rightarrow C$, $FV(A) = FV(B) \cup FV(C)$
  - Si $A = \forall x \ B \ ou \ \exists x \ B$, $FV(A) = FV(B) \setminus \{x\}$

- Ensemble des variables liées (muettes) d'une formule A, noté $BV(A)$:
  - Si $A = R(t_1, \dots, t_n)$ (R : symbole de relation), $BV(t) = \emptyset$
  - Si $A = \neg B$, $BV(A) = BV(B)$
  - Si $A = B \wedge C \ ou \ B \vee C \ ou \ B \Rightarrow C$, $BV(A) = BV(B) \cup BV(C)$
  - Si $A = \forall x \ B \ ou \ \exists x \ B$, $BV(A) = BV(B) \cup \{x\}$

Variables libres et liées

- Deux formules sont α-équivalentes si elles sont syntaxiquement identiques à un renommage près des occurrences des variables liées

- Si pour une formule A, $FV(A) = \emptyset$, A est dite close

- Si pour une formule A, $FV(A) = \{x_1, \dots, x_n\}$, la fermeture (universelle) de A est la formule close $\forall x_1 \dots \forall x_n\ A$

Substitutions

- Application d'une substitution σ sur une formule A, notée $A\sigma$:
  - Si $A = R(t_1, \dots, t_n)$, $A\sigma = R(t_1\sigma, \dots, t_n\sigma)$
  - Si $A = \neg B$, $A\sigma = B\sigma$
  - Si $A = B\ \theta\ C$ avec $\theta \in \{\wedge, \vee, \Rightarrow\}$, $A\sigma = B\sigma\ \theta\ C\sigma$
  - Si $A = Qx\ B$ avec $Q \in \{\forall, \exists\}$, si $x \notin \bigcup_{y \in dom(\sigma \setminus \{x\})} V(\sigma(y))$, $A\sigma = Qx\ B\sigma$

(on remplace les variables non « protégées » par des quantificateurs)

Formules

- Si on se restreint aux symboles de relation d'arité 0
  - Une formule ne contient pas de variables
  - Une formule ne contient pas de termes
  - Une formule ne contient pas de quantificateurs

  On obtient … les formules du calcul propositionnel !

- Rappel, $\perp$ est un symbole de relation 0-aire

- Une « variable » propositionnelle est une relation 0-aire (une formule)

Sémantique

- Structure d'interprétation pour un langage $\mathcal{L}$: $\mathcal{SI} = (D, I)$
  - D : domaine, ensemble non vide
  - I : fonction d'interprétation
    - Pour chaque constante $c \in \mathcal{S}_{\mathcal{C}}$, $I(c) \in D$
    - Pour chaque symbole de fonction $f \in \mathcal{S}_{\mathcal{F}}$, $ar(f) = n$, $I(f) : D^n \longrightarrow D$
    - Pour chaque symbole de relation $R \in \mathcal{S}_{\mathcal{R}}$, $ar(R) = n$, $I(R) : D^n \longrightarrow \mathbb{B}$

- Affectation de valeurs aux variables :
  - Fonction $v : \mathcal{V} \longrightarrow D$
  - $v[x \coloneqq d]$ pour $d \in D$ est la fonction v' :
    - $v'(x) = d$
    - $v'(y) = v(y)$ pour $y \neq x$

Sémantique

- Valeur d'un terme t, notée $I_v(t)$:
  - Si $t = a$ (a : constante), $I_v(t) = I(a)$
  - Si $t = x$ (x : variable), $I_v(t) = v(x)$
  - Si $t = f(t_1, \dots, t_n)$, $I_v(t) = I(f)(I_v(t_1), \dots, I_v(t_n))$

- Valeur de vérité d'une formule A, notée $I_v(A)$:
  - Si $A = \perp$, $I_v(A) = 0$
  - Si $A = R(t_1, \dots, t_n)$, $I_v(A) = I(R)(I_v(t_1), \dots, I_v(t_n))$
  - Si $A = \neg B$, $I_v(A) = \overline{I_v(B)}$
  - Si $A = B \land C$, $I_v(A) = I_v(B) \cdot I_v(C)$
  - Si $A = B \lor C$, $I_v(A) = I_v(B) + I_v(C)$
  - Si $A = B \Rightarrow C$, $I_v(A) = I_v(B) \dot{\Rightarrow} I_v(C)$
  - Si $A = \forall x\, B$, $I_v(A) = 1$ si pour tout $d \in D$ on a $I_{v[x:=d]}(B) = 1$, 0 sinon
  - Si $A = \exists x\, B$, $I_v(A) = 1$ s'il existe un $d \in D$ tel que $I_{v[x:=d]}(B) = 1$, 0 sinon

Sémantique

A et B : formules, E : ensemble de formules, I : interprétation

- $I_v(A)$ ne dépend pas des variables liées
- Si $BV(A) = \emptyset$, alors $I_v(A) = I_{v'}(A)$ pour toutes valuations v et v'

- Si $I_v(A) = 1$, alors I_v satisfait A, noté $I_v \vDash A$
- Si $I_v \vDash A$ pour tout $A \in E$, alors I_v satisfait E, noté $I_v \vDash E$
- S'il n'existe aucune I_v telle que $I_v \vDash E$, alors E contradictoire
- Si $I_v \vDash A$ pour tout I et tout v, alors A valide noté $\vDash A$
- Si $I_v \vDash A$ pour tout I et tout v telles que $I_v \vDash E$,
  alors E déduit sémantiquement A noté $E \vDash A$
- Si $\{A\} \vDash B$ et $\{B\} \vDash A$, alors A et B sont sémantiquement équivalentes
  noté $A \equiv B$

Quelques résultats

- Proposition

  A et B formules, E ensemble de formules

  – $E \vDash A \Rightarrow B$ ssi $E \cup \{A\} \vDash B$

  – $E \vDash A$ ssi $E \cup \{\neg A\}$ contradictoire

Quelques équivalences remarquables

- Celles du calcul propositionnel

- $\forall x \neg A \equiv \neg \exists x A$ $\qquad \forall x A \equiv \neg \exists x \neg A$
- $\exists x \neg A \equiv \neg \forall x A$ $\qquad \exists x A \equiv \neg \forall x \neg A$

- Si $y \notin FV(A)$ alors
  - $\forall x A \equiv \forall y A[x \coloneqq y]$
  - $\exists x A \equiv \exists y A[x \coloneqq y]$

- Si $x \notin FV(B)$ alors
  - $(\forall x A) \wedge B \equiv \forall x (A \wedge B)$
  - $(\forall x A) \vee B \equiv \forall x (A \vee B)$
  - $(\exists x A) \wedge B \equiv \exists x (A \wedge B)$
  - $(\exists x A) \vee B \equiv \exists x (A \vee B)$

Quelques équivalences remarquables

- $\forall x \, \forall y \, A \equiv \forall y \, \forall x \, A$
- $\exists x \, \exists y \, A \equiv \exists y \, \exists x \, A$

- $\exists y \, \forall x \, A \vDash \forall x \, \exists y \, A$

- ATTENTION, on n’a pas $\forall x \, \exists y \, A \vDash \exists y \, \forall x \, A$

Déduction naturelle

$$\frac{}{\Gamma, A \vdash A}\,(ax) \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A}\,(aff)$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_i) \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow_e)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\vee_i^g) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\vee_i^d) \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\vee_e)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\wedge_i) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\wedge_e^g) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\wedge_e^d)$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,(\neg_i) \qquad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\neg_e) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\,(\bot_c)$$

$$\frac{\Gamma \vdash A \quad x\ n'est\ pas\ libre\ dans\ \Gamma}{\Gamma \vdash \forall x\ A}\,(\forall_i) \qquad \frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x := t]}\,(\forall_e)$$

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\ A}\,(\exists_i) \qquad \frac{\Gamma \vdash \exists x\ A \quad \Gamma, A \vdash C \quad x\ libre\ ni\ dans\ \Gamma, ni\ dans\ C}{\Gamma \vdash C}\,(\exists_e)$$

Déduction naturelle

- Proposition
  Les règles de déduction naturelle sont correctes

- Théorème

F : formule sans variable libre
$\vdash F$ prouvable par déduction naturelle ssi $\vDash F$

- Exemples
  - Tout homme est mortel ; Socrate est un homme donc Socrate est mortel
    - Symboles de constantes : S
    - Symboles de relation : $H : 1,\ M : 1$
  - $\vdash (\forall x\ A\ \vee\ \forall x\ B)\ \Rightarrow\ \forall x\ (A\ \vee B)$
  - $\vdash \neg\exists x\ A\ \Leftrightarrow\ \forall x\ \neg A$
  - $\vdash \forall x\ A\ \vee\ \exists x\ \neg A$

Déduction naturelle

Ajout de nouvelles règles

Exemple :

Les règles de la déduction naturelle de la logique propositionnelle

+

$$\frac{\Gamma \vdash A \quad x\ n'est\ pas\ libre\ dans\ \Gamma}{\Gamma \vdash \forall x\ A}(\forall_i) \qquad \frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x := t]}(\forall_e)$$

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\ A}(\exists_i) \qquad \frac{\Gamma \vdash \exists x\ A \quad \Gamma, A \vdash C \quad x\ libre\ ni\ dans\ \Gamma, ni\ dans\ C}{\Gamma \vdash C}(\exists_e)$$

+

$$\frac{}{\Gamma \vdash t = t}(=_i) \qquad \frac{\Gamma \vdash A[x := t] \quad \Gamma \vdash t = u}{\Gamma \vdash A[x := u]}(=_e)$$

- Pas de perte de cohérence

  F sans variable libre, $\vdash F$ séquent prouvable ssi $\vDash F$

Déduction naturelle

Ajout de nouvelles règles

Exemple :

Les règles de la déduction naturelle

+

$$\frac{}{\Gamma \vdash t = t}(=_i) \quad \text{reflexivity} \qquad \frac{\Gamma \vdash A[x := t] \quad \Gamma \vdash t = u}{\Gamma \vdash A[x := u]}(=_e)$$

$$\frac{\Gamma \vdash t = s}{\Gamma \vdash s = t}(=_{sym}) \quad \text{symmetry} \qquad \frac{\Gamma \vdash s = u \quad \Gamma \vdash u = t}{\Gamma \vdash s = t}(=_{trans}) \quad \text{transitivity}$$

- Pas de perte de cohérence

  F sans variable libre, $\vdash F$ séquent prouvable ssi $\vDash F$

- Exemple
  - L'égalité est symétrique et transitive

Déduction naturelle

Ajout de nouvelles règles

Propriété sur entiers :

- Ensemble N défini inductivement

$$\begin{cases} \longrightarrow Z & \text{c-à-d } Z \in N \\ n \longrightarrow S(n) & \text{c-à-d } S(n) \in N \text{ si } n \in N \end{cases}$$

- Prouver P sur N par induction
  - Stabilité de $F \subseteq N$ tel que si $n \in F$ alors $P(n)$
  - On montre
    - $P(Z)$ c-à-d $Z \in F$
    - Si $P(n)$ alors $P(S(n))$ c-à-d $S(n) \in F$ si $n \in F$

$$\boxed{\frac{P(Z) \quad \forall m\, P(m) \longrightarrow P(S(m))}{\forall n\, P(n)} (N_{ind})}$$

Déduction naturelle

Ajout de nouvelles règles

Propriété sur les listes d'entiers :

- Ensemble L défini inductivement

$$\begin{cases} \longrightarrow [\,] \\ l \longrightarrow n :: l,\, n \in \mathbb{N} \end{cases}$$

c-à-d $[\,] \in L$

c-à-d $e :: l \in L$ si $l \in L$ pour $n \in \mathbb{N}$

- Prouver P sur L par induction
  - Stabilité de $F \subseteq L$ tel que si $l \in F$ alors $P(l)$
  - On montre
    - $P([\,])$ — c-à-d $[\,] \in F$
    - Si $P(l)$ alors $pour\ tout\ n,\ P(n :: l)$ — c-à-d $e :: l \in F$ si $l \in F$ pour $n \in \mathbb{N}$

$$\boxed{\dfrac{P([\,]) \quad \forall n\, \forall l'\ P(l') \longrightarrow P(n :: l')}{\forall l\ P(l)}\,(L_{ind})}$$

Forme clausale

- Littéral : Formule atomique ou négation d'une formule atomique

- Clause : $\forall x_1 \dots \forall x_n \left(l_1 \vee \cdots \vee l_q\right)$ $n \geq 0$, chaque l_i : littéral

- La clause $\forall x_1 \dots \forall x_n \left(l_1 \vee \cdots \vee l_q\right)$ est notée $l_1 \vee \cdots \vee l_q$ (pas d'ambiguïté)

- Forme Normale Conjonctive (FNC)

  Conjonction de clauses $D_1 \wedge \cdots \wedge D_k,\ k > 0$, chaque D_i : clause

  $\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} l_i^j$, chaque l_i^j : littéral

- A : formule quelconque $\rightsquigarrow A'$: FNC tq A et A' équisatisfiables

  (laborieux)

Forme clausale

- Forme prénexe d'une formule A :

  Formule de la forme $Q_1x_1 \ldots Q_nx_n\ M$ où $n \geq 0$

  chaque Q_i : quantificateur

  M : sans quantificateur

  M : matrice de A

  $Q_1x_1 \ldots Q_nx_n$: préfixe de A

- Proposition

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq

  – A' est en forme prénexe

  – $A \ \equiv \ A'$

- Preuve

  Equivalences remarquables pour « faire sortir » les quantificateurs

Forme clausale

- Forme rectifiée d'une formule A :
  - $FV(A) \cap BV(A) = \emptyset$
  - Deux quantificateurs distincts de A lient deux variables différentes

- Proposition

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq
  - A' est en forme rectifiée
  - $A \equiv A'$

- Preuve

  Renommage des variables muettes

Forme clausale
Skolémisation

- Suppression d'un existentiel dans une formule A :

  A de la forme $\forall x_1 \dots \forall x_i \; \exists x_{i+1} \; Q_{i+2}x_{i+2} \dots Q_n x_n \; M$ $\quad i \geq 0, n \geq 1$

  chaque Q_i : quantificateur

  M : sans quantificateur

  A' de la forme $\forall x_1 \dots \forall x_i \; Q_{i+2}x_{i+2} \dots Q_n x_n \; M'$ où

  – $M' = M[x_{i+1} \coloneqq f(x_1, \dots, x_i)]$
  – f : symbole de fonction i-aire *frais* (fonction de Skolem)

- Proposition

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq

  – A' est obtenue à partir de A en supprimant un existentiel
  – A et A' sont équisatisfiables (pas équivalentes)

- Exemples

  – $\forall x \, \exists y \; R(x, y) \quad \leadsto \quad \forall x \; R(x, f(x))$ $\quad f$: fournit un y *qui va bien* pour chaque x
  – $\exists y \, \forall x \; R(x, y) \quad \leadsto \quad R(x, c)$ $\quad c$: symbole de constante (fonction 0-aire)

Forme clausale

Skolémisation

- Forme de Skolem d'une formule A

  Formule A' tq

  - A' ne contient pas d'existentiels
  - Si A comporte n existentiels, A' comporte n nouveaux symboles de fonctions

- Proposition

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq

  - A' est en forme de Skolem
  - A et A' sont équisatisfiables (pas équivalentes)

- Preuve

  On supprime les existentiels un par un

- Exemple

  - $\exists x_1 \, \forall y_1 \, \forall y_2 \, \exists x_2 \, \{ \, R(x_1, f(y_1)) \wedge R(f(y_2), x_1) \Rightarrow R(x_1, x_2) \, \}$

    $\rightsquigarrow \forall y_1 \, \forall y_2 \, \{ \, R(c, f(y_1)) \wedge R(f(y_2), c) \Rightarrow R(c, g(y_1, y_2)) \, \}$

Forme clausale

- Proposition

  Pour toute formule $A \in \mathcal{F}$, il existe $A' \in \mathcal{F}$ tq

  – A' est en FNC

  – A et A' sont équisatisfiables

- Preuve

  1) À partir de A, déterminer $A^{(1)}$ en forme rectifiée équivalente
  2) À partir de $A^{(1)}$, déterminer$A^{(2)}$ en forme prénexe équivalente
  3) Skolémiser $A^{(2)}$ pour obtenir $A^{(3)}$, $A^{(2)}$ et $A^{(3)}$ sont équisatisfiables
  4) Supprimer tous les universels de $A^{(3)}$ pour obtenir $A^{(4)}$ équivalente à $A^{(3)}$
  5) Mettre $A^{(4)}$ en FNC (pareil propositionnel) pour obtenir A' équivalente à $A^{(4)}$

  $\Rightarrow$ A et A' sont équisatisfiables

Unification

- Rappels substitution
  - substitution : fonction $\sigma : \mathcal{V} \longrightarrow \mathcal{T}$, domaine noté $dom(\sigma)$
  - On note $[x_1 \coloneqq t_1, \ldots, x_n \coloneqq t_n]$ la substitution de domaine $\{x_1, \ldots, x_n\}$ qui associe t_i à x_i pour $1 \leq i \leq n$ (les x_i distincts deux à deux)
  - L'application d'une substitution σ sur un terme t est notée $t\sigma$
  - Le terme u filtre le terme v s'il existe σ tq $u\sigma = v$
  - Les termes u et v sont unifiables s'il existe σ tq $u\sigma = v\sigma$
- Composition de $\sigma = [x_1 \coloneqq s_1, \ldots, x_n \coloneqq s_n]$ et $\theta = [y_1 \coloneqq t_1, \ldots, y_m \coloneqq t_m]$: substitution $[x_1 \coloneqq s_1\theta, \ldots, x_n \coloneqq s_n\theta, y_1 \coloneqq t_1, \ldots, y_m \coloneqq t_m]$ notée $\sigma\theta$ en ayant supprimé
  - Les éléments de la forme $x \coloneqq x$
  - Les éléments $y_j \coloneqq t_j$ tq $y_j \in dom(\theta)$

Unification

- Problème d'unification P : $s_1 = t_1 \wedge \cdots \wedge s_n = t_n$ ou $\top$ ou $\bot$

- σ solution de P (unificateur de P) si pour $1 \leq i \leq n$, $s_1\sigma \equiv t_1\sigma$
  Toute substitution solution de $\top$, aucune substitution solution de $\bot$

- Ensemble des solutions de P : $\mathcal{U}(P)$

- Exemple : $f(x, a) = f(f(b, y), y) \wedge y = a$

- P est unifiable si $\mathcal{U}(P) \neq \emptyset$

- Deux termes s et t sont unifiables
  si le problème d'unification $s = t$ a une solution

- Deux formules atomiques $r(s_1, \dots, s_n)$ et $r(t_1, \dots, t_n)$ sont unifiables
  si le problème d'unification $s_1 = t_1 \wedge \cdots \wedge s_n = t_n$ a une solution

Unification

- σ solution principale de P (unificateur le plus général de P) si
  pour tout unificateur de σ' de P il existe une substitution γ tq $\sigma' = \sigma\gamma$

- Proposition
  P problème d'unification
  Si $\mathcal{U}(P) \neq \emptyset$, il existe une solution principale unique σ notée $mgu(P)$
  ($most\ general\ unifier$)
  (À renommage près)

- P_1 et P_2 équivalents si $\mathcal{U}(P_1) = \mathcal{U}(P_2)$

- Forme résolue de P : $x_1 = t_1 \wedge \cdots \wedge x_n = t_n$ $\quad x_i$: distincts deux à deux
  hors des t_j

- Si P équivalent à forme résolue $x_1 = t_1 \wedge \cdots \wedge x_n = t_n$
  alors $mgu(P) = [x_1 \coloneqq t_1, \ldots, x_n \coloneqq t_n]$

- Exemple : $f(x,a) = f(f(b,y),y) \wedge y = a$ équivalent à $x = f(b,a) \wedge y = a$
  $mgu(P) = [x \coloneqq f(b,a),\ y \coloneqq a]$

Unification

Règles de transformation en forme résolue

Trivial $\dfrac{s = s}{\top}$

Décomposition $\dfrac{f(s_1, \dots, s_n) = f(t_1, \dots, t_n)}{s_1 = t_1 \ \wedge \cdots \wedge \ s_n = t_n}$

Incompatibilité $(clash)$ $\dfrac{f(s_1, \dots, s_n) = g(t_1, \dots, t_n)}{\bot}$ $\quad si\ f \neq g$

Union de deux variables $\dfrac{x = y \ \wedge \ P'}{x = y \ \wedge \ P'[x := y]}$ $\quad si\ x, y \in V(P')$

Remplacement de variables $\dfrac{x = s \ \wedge \ P'}{x = s \ \wedge \ P[x := s]}$ $\quad si\ x \in V(P') \setminus V(s)\ et\ s \notin \mathcal{V}$

Fusion $\dfrac{x = s \ \wedge \ x = t}{x = s \ \wedge \ s = t}$ $\quad si\ x \in \mathcal{V}\ et\ s, t \notin \mathcal{V}\ et\ |s| \leq |t|$

Test d'occurrence $(occur - check)$ $\dfrac{x_1 = t_1[x_2]_{p_1} \ \wedge \cdots \wedge \ x_n = t_n[x_1]_{p_n}}{\bot}$ $\quad si\ p_1 \cdot \ \dots \cdot p_n \neq \Lambda$

Unification

- U : ensemble de règles de transformation en forme résolue $\longrightarrow$ algo

- Proposition

  La transformation est correcte :

  Si $P_0 \rightarrow_U P_1$ alors P_0 et P_1 équivalents

- Proposition

  La transformation est complète :

  Si aucune règle de U applicable à P_i, alors P_i en forme résolue

- Proposition

  La transformation est bien fondée :

  Pas de chaine $P_0 \rightarrow_U P_1 \rightarrow_U P_2$ ... infinie

Unification

- Exemples
  - Symboles de constantes : a et b
  - Symboles de fonctions : $f : 2$
  - $\mathcal{V} = \{x, y, z\}$
  - $P \ : \ f(a, b) = f(a, a)$ $\qquad \mathcal{U}(P) = \emptyset \quad (clash)$
  - $P \ : \ f(x, y) = f(z, z)$ $\qquad \mathcal{U}(P) = [x \coloneqq z, y \coloneqq z]$
  - $P \ : \ f(x, f(a, y)) = f(f(b, z), x)$ $\qquad \mathcal{U}(P) = \emptyset \quad (clash)$
  - $P \ : \ f(f(a, y), f(y, z)) = f(x, x)$ $\qquad \mathcal{U}(P) = [x \coloneqq f(a, a), y \coloneqq a, z \coloneqq a]$
  - $P \ : \ f(x, f(x, z)) = f(f(y, z), y)$ $\qquad \mathcal{U}(P) = \emptyset \quad (occur - check)$

Résolution en logique du premier ordre

- Soient $L = R(s_1, \dots, s_n)$ et $L' = R(t_1, \dots, t_n)$ deux littéraux positifs ou nég.
  On note $mgu(L, L')$ le mgu du problème d'unification
  $$s_1 = t_1 \wedge \cdots \wedge s_n = t_n$$

- Système de preuve par résolution
  Soient C et C' deux clauses, L et L' deux littéraux
  Règles d'inférence

$$\frac{C \vee L \quad C' \vee \neg L' \quad \sigma = mgu(L, L')}{C\sigma \ \vee \ C'\sigma}(rés.) \qquad \frac{C \vee L \vee L' \quad \sigma = mgu(L, L')}{C\sigma \ \vee \ L\sigma}(fact.)$$

- Exemple

$$\frac{r\big(a, f(x)\big) \vee q(x) \quad \neg r\big(y, f(b)\big) \vee s(y, x)}{q(b) \vee s(a, b)}(rés. \quad \sigma = [x \coloneqq b, y \coloneqq a])$$

Résolution en logique du premier ordre

- Déduction, réfutation : pareil propositionnel

- Théorème (pareil propositionnel)

> Soit E un ensemble de clauses
> E est contradictoire ssi il existe une réfutation de E

- Exemple $E = \{C_1, C_2, C_3, C_4\}$
  - $C_1 \ : \ \neg R(z,z) \vee R(z,a)$
  - $C_2 \ : \ R(u, f(y)) \vee R(u,y)$
  - $C_3 \ : \ \neg R(x,a) \vee R(x,x)$
  - $C_4 \ : \ \neg R(v, f(y)) \vee \neg R(v,y)$

$$C_1, C_2 : \quad mgu(R(z,z), R(u, f(y))) = [u := f(y), z := f(y)]$$

$$C_3, C_4 : \quad mgu(R(x,x), R(v, f(y))) = [v := f(y), x := f(y)]$$

$$\dfrac{\dfrac{\dfrac{C_1 \qquad C_2}{R(f(y),a) \vee R(f(y),y)}\,\text{rés}}{R(f(a),f(a))}\,\mathit{fact}\,[y := a] \qquad \dfrac{\dfrac{C_3 \qquad C_4}{\neg R(f(y),a) \vee \neg R(f(y),y)}\,\text{rés}}{\neg R(f(a),f(a))}\,\mathit{fact}\,[\text{y:=a}]}{\emptyset}\,\text{rés}$$

Résolution en logique du premier ordre

- Application : calculer (syntaxiquement) la fonction $f(x_1, \dots, x_n)$

- On détermine la relation $R_f(x_1, \dots, x_n, y)$ tq

  $R_f(x_1, \dots, x_n, y)$ vraie ssi y $= f(x_1, \dots, x_n)$ $\qquad$ $R_f \rightsquigarrow$ ens. de clauses C

- Calcul de $f(t_1, \dots, t_n)$, avec $t_1, \dots t_n$: termes clos
  - On applique la résolution à $C,\ \neg R_f(t_1, \dots, t_n, y)$
  - On obtient $R_f(t_1, \dots, t_n, u)$ et donc $u = f(t_1, \dots, t_n)$

- Exemple
  - Symboles de constantes : Z
  - Symboles de fonctions : $S : 1$
  - Symboles de relation : $Plus : 3$ et $Mult : 3$
  - Addition : $C = \{Plus(Z, x_2, x_2),\ \neg Plus(x_1, x_2, y) \vee Plus(S(x_1), x_2, S(y))\}$
    - Dériver C, $\neg Plus(Z, S(Z), y)$ $\qquad$ on obtient $Plus(Z, S(Z), S(Z))$
    - Dériver C, $\neg plus(S(Z), S(Z), y)$ $\qquad$ on obtient $Plus(S(Z), S(Z), S(S(Z)))$