

Logique

L3 Informatique

Peter Habermehl



Université Paris Diderot, Sorbonne Paris Cité
UFR Informatique
Laboratoire LIAFA
Peter.Habermehl@liafa.jussieu.fr

Retour sur la notion de substitution

Définition :

- Une **substitution** est une fonction $\sigma : \mathcal{X} \rightarrow \mathcal{T}_{\Sigma, \mathcal{X}}$.
- Le **domaine** d'une substitution σ est l'ensemble $Dom(\sigma) = \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$.
- Le **codomaine** d'une substitution σ est l'ensemble $Codom(\sigma) = \{VI(\sigma(x)) \mid x \in Dom(\sigma)\}$.
- Un **renommage** est une substitution **injective** σ t.q. $\sigma(x) = y \forall x \in Dom(\sigma)$.
- Si le domaine d'une substitution σ est **fini** on note $\sigma = \{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$ si $\sigma(x_i) = t_i$ et $x_i \in Dom(\sigma)$.
- L'application d'une **substitution** à un terme est l'**extension** de σ aux termes donnée par $\sigma(f(t_1, \dots, t_n)) = f(\sigma(t_1), \dots, \sigma(t_n))$.

La théorie de l'unification

Composition de deux substitutions

Soient σ et τ deux substitution. La **composition** de σ avec τ est donnée par $\sigma \circ \tau(x) = \sigma(\tau(x))$.

Exemple : Soit $\sigma = \{x \leftarrow f(y), w \leftarrow g(z, z)\}$ et $\tau = \{y \leftarrow f(a), z \leftarrow g(x, b)\}$. La substitution $\tau \circ \sigma$ est donnée par $\{x \leftarrow f(f(a)), y \leftarrow f(a), w \leftarrow g(g(x, b), g(x, b)), z \leftarrow g(x, b)\}$ et la substitution $\sigma \circ \tau$ est donnée par $\{y \leftarrow f(a), z \leftarrow g(f(y), b), x \leftarrow f(y), w \leftarrow g(z, z)\}$.

Comparer deux substitutions

La substitution σ est une **instance** de la substitution τ (ou τ est **plus générale** que σ), ce que l'on écrit $\sigma \leq \tau$, ss'il existe une substitution ρ t.q. pour toute variable $x \in \mathcal{X}$, $\sigma(x) = (\rho \circ \tau)(x)$.

Exemple : $\{x \leftarrow f(y), y \leftarrow z\}$ est plus générale que $\{x \leftarrow f(b), y \leftarrow h(c), z \leftarrow h(c)\}$

Identifier deux substitutions

Remarque : La relation \leq n'est pas antisymétrique.

Exemple : Soient $\sigma_1 = \{x \leftarrow y\}$ et $\sigma_2 = \{y \leftarrow x\}$. On a $\sigma_1 \leq \sigma_2$ et $\sigma_2 \leq \sigma_1$ et $\sigma_1 \neq \sigma_2$.

Lemme : La relation d'équivalence engendrée par \leq est donnée par: $\sigma \sim \sigma'$ ssi \exists un renommage ρ t.q. $\sigma = \rho \circ \sigma'$.

Alors, $\sigma_1 \sim \sigma_2$ dans l'exemple précédent car: $\sigma_1 = \sigma_1 \circ \sigma_2$ et $\sigma_2 = \sigma_2 \circ \sigma_1$.

Substitution(s) principale(s)

Soit \mathcal{S} en ensemble de substitutions et $\tau \in \mathcal{S}$. On dit que τ est **principale** ssi toute substitution $\sigma \in \mathcal{S}$ est une instance de τ .

Exemple : Soit $\mathcal{S} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, où $\sigma_1 = \{x \leftarrow y\}$, $\sigma_2 = \{y \leftarrow x\}$, $\sigma_3 = \{x \leftarrow y, z \leftarrow x\}$, $\sigma_4 = \{x \leftarrow z, y \leftarrow z\}$ et $\sigma_5 = \{x \leftarrow a, y \leftarrow a\}$.

Alors σ_1 , σ_2 et σ_3 sont principales pour \mathcal{S} . En effet, $\sigma_2, \sigma_3, \sigma_4, \sigma_5 \leq \sigma_1$ et $\sigma_1, \sigma_3, \sigma_4, \sigma_5 \leq \sigma_2$ et $\sigma_1, \sigma_2, \sigma_4, \sigma_5 \leq \sigma_3$.
Mais $\sigma_1 \not\leq \sigma_4$ car $\sigma_1 \neq \{x \leftarrow y, z \leftarrow y\} = \{z \leftarrow y\} \circ \sigma_4$. De même, $\sigma_1 \not\leq \sigma_5$ (entre autres).

Unification comme solution d'un système d'équations

Une **équation** est une paire de termes de la forme $s \doteq t$, elle est **unifiable** ssi il existe une substitution σ t.q. $\sigma(s) = \sigma(t)$. Cette substitution est un **unificateur** ou une **solution** de l'équation $s \doteq t$.

Un **système fini** ou **problème fini d'équations** \mathcal{P} est un ensemble $\{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$ d'équations, il est **unifiable** ssi il existe une substitution qui est unificateur de toutes les équations de \mathcal{P} . Cette substitution est un **unificateur** ou une **solution** de l'ensemble \mathcal{P} .

Définition :

- L'ensemble de variables de \mathcal{P} est notée $Var(\mathcal{P})$.
- L'application d'une substitution σ à $\mathcal{P} = \{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$ donne le système $\sigma(\mathcal{P}) = \{\sigma(s_1) \doteq \sigma(t_1), \dots, \sigma(s_n) \doteq \sigma(t_n)\}$.

Module ces considérations, l'unificateur principal d'un problème \mathcal{P} est unique modulo renommage, c'est à dire :

Si σ et σ' sont deux unificateurs principaux de \mathcal{P} , alors $\sigma \sim \sigma'$.

- 1 On identifie deux unificateurs σ et σ' d'un problème \mathcal{P} s'ils ne diffèrent que par des renommage de variables, c'est à dire, si $\sigma \sim \sigma'$.
- 2 On considère uniquement comme unificateurs de \mathcal{P} les substitutions σ t.q. $Dom(\sigma) \subseteq Var(\mathcal{P})$.

Exemple : Soit $\mathcal{S} = \{x \doteq y\}$. Prenons trois unificateurs principaux de \mathcal{S} : $\sigma_1 = \{x \leftarrow y\}$, $\sigma_2 = \{y \leftarrow x\}$ et $\sigma_3 = \{x \leftarrow y, z \leftarrow w\}$. Alors $\sigma_1 = \sigma_2$ (car $[\sigma_1]_{\sim} = [\sigma_2]_{\sim}$) et σ_3 n'est plus considéré comme un unificateur de \mathcal{S} .

Définition : Un problème d'unification \mathcal{P} est en forme résolue ssi il est de la forme $\{x_1 \doteq t_1, \dots, x_n \doteq t_n\}$, où

- 1 toutes les variables x_i sont distinctes ($i \neq j$ implique $x_i \neq x_j$)
- 2 aucune x_i n'apparaît dans un t_j ($\forall i \forall j x_i \notin VI(t_j)$)

Notation : Si \mathcal{P} est un système en forme résolue $\{x_1 \doteq t_1, \dots, x_n \doteq t_n\}$ on note \vec{P} la substitution $\{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$.

$$\frac{\mathcal{P} \cup \{s \doteq s\}}{\mathcal{P}} \quad (\text{effacer}) \quad \frac{\mathcal{P} \cup \{t \doteq x\} \quad t \notin \mathcal{X}}{\mathcal{P} \cup \{x \doteq t\}} \quad (\text{orienter})$$

$$\frac{\mathcal{P} \cup \{f(s_1, \dots, s_n) \doteq f(t_1, \dots, t_n)\}}{\mathcal{P} \cup \{s_1 \doteq t_1, \dots, s_n \doteq t_n\}} \quad (\text{décomposer})$$

$$\frac{\mathcal{P} \cup \{x \doteq s\} \quad x \in \text{Var}(\mathcal{P}) \quad x \notin \text{VI}(s)}{\{x \leftarrow s\}(\mathcal{P}) \cup \{x \doteq s\}} \quad (\text{remplacer})$$

Exemple

Soit $\mathcal{P} = \{f(x, h(b), c) \doteq f(g(y), y, c)\}$.

$$\frac{\frac{\frac{f(x, h(b), c) \doteq f(g(y), y, c)}{x \doteq g(y), h(b) \doteq y, c \doteq c} \text{d}}{x \doteq g(y), h(b) \doteq y} \text{e}}{x \doteq g(y), y \doteq h(b)} \text{o}}{x \doteq g(h(b)), y \doteq h(b)} \text{r}$$

L'unificateur principal de P est $\sigma = \{x \leftarrow g(h(b)), y \leftarrow h(b)\}$.

Ainsi, $\sigma f(x, h(b), c) = f(g(h(b)), h(b), c) = \sigma f(g(y), y, c)$.

- 1 On démarre avec un problème \mathcal{P}
- 2 On applique les règles de transformation tant qu'on peut, on obtient un problème \mathcal{S}
- 3 Si le problème \mathcal{S} est en forme résolue
 - ▶ alors renvoyer $\vec{\sigma}$
 - ▶ sinon échec

Vers la correction et la complétude de l'algorithme

Lemme :

- 1 L'algorithme termine.
- 2 Si σ est un unificateur d'un problème $\mathcal{P} = \{x_1 \doteq t_1, \dots, x_n \doteq t_n\}$, alors $\sigma = \sigma \circ \vec{\mathcal{P}}$.
- 3 Si une règle transforme un problème \mathcal{P} dans un problème \mathcal{S} , alors les unificateur de \mathcal{P} et \mathcal{S} sont les mêmes.
- 4 Si \mathcal{P} est en forme résolue, alors $\vec{\mathcal{P}}$ est solution du problème \mathcal{P} .

Théorème : (Correction) Si l'algorithme trouve une substitution \vec{S} pour le problème P , alors P est unifiable et \vec{S} est un unificateur principal de P .
Autrement dit,
Si P n'est pas unifiable, l'algorithme échoue.

Théorème : (Complétude) Si le système P est unifiable, alors l'algorithme calcule l'unificateur principal de P .
Autrement dit,
Si l'algorithme échoue, alors le système P n'est pas unifiable.

Résolution

Méthode par réfutation :

On suppose que A est close (pas de variables libres).
Dans ce cas, avoir un modèle et être satisfaisable est la même notion.
 A est valide ssi $\neg A$ est insatisfaisable (n'a pas de modèle) ssi en appliquant la méthode de résolution à $\neg A$ on obtient une contradiction (réfutation).

La résolution pour le calcul des prédicats

Résolution

- Forme prénexe
- Skolemisation
- Forme clausale
- Règles de résolution
- Correction et complétude

Quelques équivalences logiques (rappel)

$$\begin{aligned}
 \forall x. A &\equiv \neg \exists x. \neg A \\
 \neg \forall x. A &\equiv \exists x. \neg A \\
 \exists x. A &\equiv \neg \forall x. \neg A \\
 \neg \exists x. A &\equiv \forall x. \neg A \\
 \forall x. (A \wedge B) &\equiv \forall x. A \wedge \forall x. B \\
 \exists x. (A \vee B) &\equiv \exists x. A \vee \exists x. B \\
 \exists x. (A \rightarrow B) &\equiv \forall x. A \rightarrow \exists x. B \\
 \forall x. \forall y. A &\equiv \forall y. \forall x. A \\
 \exists x. \exists y. A &\equiv \exists y. \exists x. A
 \end{aligned}$$

D'autres exemples d'équivalence lorsque $x \notin VI(A)$

$$\begin{aligned}
 \forall x. A &\equiv \exists x. A && \equiv A \\
 \forall x. (A \wedge B) &\equiv A \wedge \forall x. B \\
 \exists x. (A \wedge B) &\equiv A \wedge \exists x. B \\
 \forall x. (A \vee B) &\equiv A \vee \forall x. B \\
 \exists x. (A \vee B) &\equiv A \vee \exists x. B \\
 \exists x. (A \rightarrow B) &\equiv A \rightarrow \exists x. B \\
 \forall x. (A \rightarrow B) &\equiv A \rightarrow \forall x. B \\
 \exists x. (B \rightarrow A) &\equiv \forall x. B \rightarrow A \\
 \forall x. (B \rightarrow A) &\equiv \exists x. B \rightarrow A
 \end{aligned}$$

Forme préfixe

Définition : Une formule G est dite en **forme préfixe** ssi elle est de la forme $Q_1 x_1 \dots Q_n x_n A$, où chaque Q_i est un quantificateur \forall ou \exists et A ne contient pas de quantificateur.

Théorème : Pour toute formule G il existe une formule G' en forme préfixe t.q $G \equiv G'$.

Exemples

$$\begin{aligned}
 (\forall x p(x)) \wedge r(x) &\equiv \forall y (p(y) \wedge r(x)) \\
 (\forall x p(x)) \wedge (\forall x r(x)) &\equiv \forall x (p(x) \wedge r(x)) \\
 (\forall x p(x)) \wedge (\forall x r(x)) &\equiv \forall x \forall y (p(x) \wedge r(y)) \\
 (\forall x p(x)) \vee (\forall x r(x)) &\equiv \forall x \forall y (p(x) \vee r(y)) \\
 (\forall x p(x)) \rightarrow (\exists y r(y)) &\equiv \exists x \exists y (p(x) \rightarrow r(y)) \\
 \neg[(\forall x p(x)) \rightarrow (\exists y r(y))] &\equiv \forall x \forall y \neg(p(x) \rightarrow r(y))
 \end{aligned}$$

Skolemisation partielle

Définition : Soit G une formule prénex de la forme $\forall x_1 \dots \forall x_n \exists x_{n+1} Q_{n+2} x_{n+2} Q_{n+i} x_{n+i} A$. Soit f un **nouveau** symbole de fonction n -aire. La formule $\forall x_1 \dots \forall x_n Q_{n+2} x_{n+2} Q_{n+i} x_{n+i} \{x_{n+1} \leftarrow f(x_1, \dots, x_n)\}(A)$ est la **skolemisation partielle** de G .

Lemme : Soit G une formule prénex et soit G' sa skolemisation partielle. Alors G a un modèle ssi G' a un modèle.

Skolemisation

Définition : Soit G une formule prénex ayant n quantificateurs \exists . La **Skolemisation** de G est la formule obtenue par n applications successives de la skolemisation partielle.

Théorème : Soit G' la Skolemisation de la formule G . Alors

- Si G contient n quantificateurs \exists , G' contient **au plus** n nouveaux symboles de fonction.
- G' ne contient pas de quantificateurs \exists .
- G a un modèle ssi G' a un modèle.

Exemples

G' est la skolemisation partielle de G .

$$\begin{array}{cc}
 G & G' \\
 \forall x \forall y \exists z r(x, z) & \forall x \forall y r(x, f(x, y)) \\
 \forall x \exists z \forall y \exists w \exists w' s(w', x, h(z)) & \forall x \forall y \exists w \exists w' s(w', x, h(g(x))) \\
 \exists x \exists z \forall y s(x, x, z) & \exists z \forall y s(a, a, z)
 \end{array}$$

Exemples

G' est la Skolemisation de G .

$$\begin{array}{cc}
 G & G' \\
 \forall x \forall y \exists z r(x, z) & \forall x \forall y r(x, f(x, y)) \\
 \forall x \exists z \forall y \exists w \exists w' s(w', x, h(z)) & \forall x \forall y s(i(x, y), x, h(g(x))) \\
 \exists x \exists z \forall y s(x, x, z) & \forall y s(a, a, b)
 \end{array}$$

Définition :

- Un **littéral** est une formule de la forme $r(t_1, \dots, t_n)$ ou $\neg r(t_1, \dots, t_n)$.
- Une **clause** est une formule de la forme $L_1 \vee \dots \vee L_q$, $q \geq 0$, où chaque L_i est un littéral. La **clause vide** s'écrit \perp .
- Une formule est en **forme normal conjonctive (FNC)** ssi elle est de la forme $C_1 \wedge \dots \wedge C_n$, $n \geq 0$, où chaque C_i est une clause. La **FNC vide** s'écrit \top .

\top est une FNC. \perp est une FNC.

$\neg p(h(x))$ est une FNC.

$\neg p(h(x)) \vee p(y)$ est une FNC.

$(\neg p(h(x)) \vee p(y)) \wedge p(z)$ est une FNC.

$(\neg p(h(x)) \vee p(y)) \wedge (p(z) \vee \neg p(h(x)))$ est une FNC.

$\neg(p(x) \vee \neg p(z))$ n'est pas une FNC.

$p(x) \wedge (\neg p(z) \rightarrow p(h(z)))$ n'est pas une FNC.

$p(x) \vee (\neg p(z) \wedge p(h(z)))$ n'est pas une FNC.

Existence de la FNC

Théorème : Pour toute formule A **sans quantificateurs**, il existe une formule A' en FNC telle que $A' \equiv A$.

Preuve : Comme dans le cas propositionnel : utiliser les équivalences suivantes:

$A \rightarrow B$	\equiv	$\neg A \vee B$
$\neg\neg A$	\equiv	A
$\neg(A \wedge B)$	\equiv	$\neg A \vee \neg B$
$\neg(A \vee B)$	\equiv	$\neg A \wedge \neg B$
$A \vee (B \wedge C)$	\equiv	$(A \vee B) \wedge (A \vee C)$

Unicité

La FNC d'une formule **n'est pas unique**.

Exemple:

$$p \vee \neg p \equiv p \vee p \vee \neg p \equiv \top.$$

Donc,

$p \vee \neg p$, $p \vee p \vee \neg p$ et \top sont trois FNC de la formule $p \vee \neg p$.

Vers la mise sous forme clausale

Lemme : Soit $\Delta = \{A_1, \dots, A_n\}$ un ensemble de formules sans quantificateurs. Soit $FNC_\Delta = \{E_1, \dots, E_n\}$ un ensemble de formules où chaque E_i est une FNC de A_i . Soit C_Δ l'ensemble de clauses de FNC_Δ construit comme

$$\bigcup_{1 \leq i \leq n} \{D_{i_1}, \dots, D_{i_k} \mid E_i \in FNC_\Delta \text{ et } E_i = D_{i_1} \wedge \dots \wedge D_{i_k}\}.$$

Alors l'ensemble de formules Δ a un modèle ssi l'ensemble de clauses C_Δ a un modèle.

Exemple

$$G = \neg[[Q(a) \wedge (\forall x Q(x) \rightarrow Q(f(x)))] \rightarrow \exists z Q(f(f(z)))]$$

- 1 $G_1 = \neg[\neg[Q(a) \wedge (\forall x (\neg Q(x) \vee Q(f(x))))] \vee \exists z Q(f(f(z)))]$.
- 2 $G_2 = \forall z \forall x \neg[\neg[Q(a) \wedge (\neg Q(x) \vee Q(f(x)))] \vee Q(f(f(z)))]$.
- 3 $G_3 = G_2$.
- 4 $G_4 = \forall z \forall x [[Q(a) \wedge (\neg Q(x) \vee Q(f(x)))] \wedge \neg Q(f(f(z)))]$.
- 5 $C_G = \{Q(a), \neg Q(x) \vee Q(f(x)), \neg Q(f(f(z)))\}$.

Mise sous forme clausale

Théorème : Pour toute formule G il existe un ensemble de clauses C_G t.q

- $VI(C_1) \cap VI(C_2) = \emptyset$ si $C_1, C_2 \in C_G$ et $C_1 \neq C_2$
- G a un modèle ssi C_G a un modèle.

Preuve :

- 1 Utiliser l'équivalence $A \rightarrow B \equiv \neg A \vee B$ pour éliminer les implications de G . On obtient une formule $G_1 \equiv G$.
- 2 Calculer G_2 , la forme prénex de G_1 . On a $G_2 \equiv G_1$.
- 3 Calculer $G_3 = \forall x_1 \dots \forall x_m A$ ($m \geq 0$), la Skolemisation de G_2 . On a que G_3 a un modèle ssi G_2 a un modèle
- 4 Calculer la forme normal conjonctive de A . On obtient $G_4 = \forall x_1 \dots \forall x_m (C_1 \wedge \dots \wedge C_n)$ ($m \geq 0, n \geq 0$). On a $G_4 \equiv G_3$.
- 5 Donner comme résultat $C_G = \{C'_1, \dots, C'_n\}$ qui est un renommage de $\{C_1, \dots, C_n\}$ afin d'éviter les variables communes. On a que G a un modèle ssi C_G a un modèle.

Exemple

$$G = (\exists y r(x, y) \vee \forall z q(z, z)) \wedge (\neg \forall x p(x)).$$

- 1 $G_1 = G$.
- 2 $G_2 = \exists x' \exists y \forall z (r(x, y) \vee q(z, z)) \wedge (\neg p(x'))$.
- 3 $G_3 = \forall z (r(x, b) \vee q(z, z)) \wedge (\neg p(a))$.
- 4 $G_4 = G_3$.
- 5 $C_G = \{r(x, b) \vee q(z, z), \neg p(a)\}$.

Résolution pour le calcul des prédicats

Axiomes : aucun

Règles d'inférence :

$$\frac{D \vee r(s_1, \dots, s_n) \quad C \vee \neg r(t_1, \dots, t_n)}{\sigma(D \vee C)} \text{ (coupure)}$$

où σ est l'unificateur principal du problème $\{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$

$$\frac{D \vee L \vee L'}{\sigma(D \vee L)} \text{ (factorisation)}$$

où

- $L = r(s_1, \dots, s_n)$ (resp. $L = \neg r(s_1, \dots, s_n)$) et $L' = r(t_1, \dots, t_n)$ (resp. $L' = \neg r(t_1, \dots, t_n)$)
- σ est l'unificateur principal du problème $\{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$

Rappel : Le cas particulier de la règle coupure lorsque $r(s_1, \dots, s_n)$ et $r(t_1, \dots, t_n)$ sont unifiables :

$$\frac{r(s_1, \dots, s_n) \quad \neg r(t_1, \dots, t_n)}{\perp}$$

Notation : Comme dans le cas propositionnel, on écrit $\Delta \vdash_R A$ si A est dérivée à partir de l'ensemble Δ par résolution et $\Delta \vdash_R \perp$ si \perp est dérivée à partir de l'ensemble Δ par résolution.

Notion de réfutation

Un ensemble de formules est **réfutable** ssi en lui appliquant la méthode de résolution on obtient \perp .

Exemple I

Montrer que l'ensemble suivant est contradictoire.

$$H_1: \exists x_0 t(x_0)$$

$$H_2: \forall x_2 (d(x_2) \rightarrow \forall x_1 r(x_1, x_2))$$

$$H_3: \forall x_3 \forall x_4 (\neg(t(x_3) \rightarrow \neg q(x_4)) \rightarrow \neg r(x_3, x_4))$$

$$H_4: \neg \forall x_5 (\neg d(x_5) \vee \neg q(x_5))$$

D'abord, on donne un ensemble de **clauses** C équivalent à $\{H_1, H_2, H_3, H_4\}$.

$$C = \{t(a), \neg d(x_2) \vee r(x_1, x_2), \neg t(x_3) \vee \neg q(x_4) \vee \neg r(x_3, x_4), d(b), q(b)\}$$

Puis on donne une **réfutation** de l'ensemble C par la méthode de résolution.

$$\frac{\frac{\frac{\neg t(x_3) \vee \neg q(x_4) \vee \neg r(x_3, x_4) \quad t(a)}{\neg q(x_4) \vee \neg r(a, x_4)} \quad q(b)}{\neg d(x_2) \vee r(x_1, x_2) \quad \neg r(a, b)} \quad d(b)}{\neg d(b)}$$

⊥

Exemple II

Montrer que la formule J_4 est conséquence logique de la formule

$$J_1 \wedge J_2 \wedge J_3.$$

$$J_1: \exists x_0 t(x_0)$$

$$J_2: \forall x_2 (d(x_2) \rightarrow \forall x_1 r(x_1, x_2))$$

$$J_3: \forall x_3 \forall x_4 (\neg(t(x_3) \rightarrow \neg q(x_4)) \rightarrow \neg r(x_3, x_4))$$

$$J_4: \forall x_5 (\neg d(x_5) \vee \neg q(x_5))$$

D'abord on utilise le fait que $J_1 \wedge J_2 \wedge J_3 \models J_4$ ssi $J_1 \wedge J_2 \wedge J_3, \neg J_4$ est réfutable. Ceci car les formules n'ont pas de variables libres.

On donne donc un ensemble de **clauses** C équivalent à $\{J_1 \wedge J_2 \wedge J_3, \neg J_4\}$.

$$C = \{t(a), \neg d(x_2) \vee r(x_1, x_2), \neg t(x_3) \vee \neg q(x_4) \vee \neg r(x_3, x_4), d(b), q(b)\}$$

On donne une **réfutation** de l'ensemble C par la méthode de résolution.

Exemple III

Exemple III

Montrer que la formule $J : \forall x p(x) \vee \exists y \neg p(y)$ est valide.

D'abord on utilise le fait que J est valide ssi $\neg J$ est réfutable.

On donne donc un ensemble de **clauses** C équivalent à $\{\neg J\}$.

$$C = \{\neg p(a), p(y)\}$$

On donne une **réfutation** de l'ensemble C par la méthode de résolution.

$$\frac{\neg p(a) \quad p(y)}{\perp}$$

$$\frac{\frac{\frac{\neg t(x_3) \vee \neg q(x_4) \vee \neg r(x_3, x_4) \quad t(a)}{\neg q(x_4) \vee \neg r(a, x_4)} \quad q(b)}{\neg d(x_2) \vee r(x_1, x_2) \quad \neg r(a, b)} \quad d(b)}{\neg d(b)}$$

⊥

avec formalisation : au tableau

Vers la complétude de la résolution

Soit Σ une signature contenant au moins une constante.

Définition :

- L'**univers d'Herbrand** de Σ est l'ensemble des termes clos sur Σ .
- La **base d'Herbrand** est l'ensemble d'atomes clos sur Σ .
- Une **interprétation de Herbrand** de Σ est une interprétation t.q.
 - ▶ Son domaine est l'univers d'Herbrand
 - ▶ Pour chaque $f \in \Sigma_F$ d'arité n , $\mathcal{I}(f)(t_1, \dots, t_n) = f(t_1, \dots, t_n)$
 - ▶ Pour chaque $p \in \Sigma_P$ d'arité n , on se donne un sous-ensemble \mathcal{S}_p de la base de Herbrand t.q. $\mathcal{I}(p)(t_1, \dots, t_n) = \mathbf{V}$ ssi $p(t_1, \dots, t_n) \in \mathcal{S}_p$.

Théorème : La résolution est **correcte**, i.e., si $\Delta \vdash_R A$, alors le séquent $\Delta \vdash A$ est valide et si $\Delta \vdash_R \perp$, alors Δ n'a pas de modèle.

Théorème : La résolution est **complète** pour la réfutation, i.e., si Δ n'a pas de modèle, alors $\Delta \vdash_R \perp$.

Lemmes pour le Théorème de Herbrand

Lemme : Soit t un terme dont les variables libres appartiennent à $\{x_1, \dots, x_n\}$. Soit \mathcal{I} une interprétation ayant \mathcal{D} comme domaine et σ une valuation dans le domaine \mathcal{D} . Soit la substitution $\tau = \{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$ et soient $d_1 \dots d_n$ t.q. $[t_i]_{\mathcal{I}, \sigma} = d_i$. Alors $[t]_{\mathcal{I}, \sigma[x_1:=d_1] \dots [x_n:=d_n]} = [\tau(t)]_{\mathcal{I}, \sigma}$.

Lemme : Soit G une formule dont les variables libres appartiennent à $\{x_1, \dots, x_n\}$. Soit \mathcal{I} une interprétation ayant \mathcal{D} comme domaine et σ une valuation dans le domaine \mathcal{D} . Soit la substitution $\tau = \{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$ et soient $d_1 \dots d_n$ t.q. $[t_i]_{\mathcal{I}, \sigma} = d_i$. Alors $[G]_{\mathcal{I}, \sigma[x_1:=d_1] \dots [x_n:=d_n]} = [\tau(G)]_{\mathcal{I}, \sigma}$.

Exercice : Soit $G = r(x_1, x_2)$ et $\tau = \{x_1 \leftarrow a, x_2 \leftarrow s(a)\}$. Soit $\mathcal{I}(r)(n, m) = \mathbf{V}$ ssi $n < m$, $\mathcal{I}(a) = 0$ et $\mathcal{I}(s)(n) = n + 1$. Vérifier le résultat précédent.

Théorème de Herbrand

Théorème : Un ensemble de clauses \mathcal{C} admet un modèle ssi il existe une interprétation \mathcal{I}_H de Herbrand t.q. \mathcal{I}_H est un modèle de \mathcal{C} .

Preuve : Si il existe une interprétation de Herbrand qui est un modèle de \mathcal{C} , alors \mathcal{C} admet un modèle.

Soit \mathcal{C} un ensemble de clauses qui admet un modèle. Alors il existe une interprétation \mathcal{I} qui est un modèle de \mathcal{C} . On va montrer qu'il existe une interprétation \mathcal{I}_H de Herbrand qui est un modèle de \mathcal{C} .

En effet, pour chaque symbole de prédicat p , on construit $\mathcal{I}_H(p)$ comme suit :

$$\mathcal{I}_H(p)(t_1, \dots, t_n) = \mathbf{V} \text{ ssi } \mathcal{I} \text{ est un modèle de la formule } p(t_1, \dots, t_n)$$

Preuve du théorème de Herbrand

$$(3) [\tau(A_i)]_{\mathcal{I}, \sigma} = \mathbf{V} \text{ pour tout } \sigma$$

ssi

\mathcal{I} est un modèle de $\tau(A_i)$

ssi (def. Herbrand)

\mathcal{I}_H est un modèle de $\tau(A_i)$

ssi

$$[\tau(A_i)]_{\mathcal{I}_H, \sigma_H} = \mathbf{V} \text{ pour tout } \sigma_H$$

implique

$$[\tau(A_1 \vee \dots \vee A_k)]_{\mathcal{I}_H, \sigma_H} = \mathbf{V} \text{ pour tout } \sigma_H$$

ssi (lemme, où $[t_i]_{\mathcal{I}_H, \sigma_H} = t_i$)

$$[A_1 \vee \dots \vee A_k]_{\mathcal{I}_H, \sigma_H} [x_1 := t_1] \dots [x_n := t_n] = \mathbf{V} \text{ pour tout } \sigma_H$$

ssi (les t_i sont arbitraires)

$$[\forall x_1 \dots \forall x_n (A_1 \vee \dots \vee A_k)]_{\mathcal{I}_H, \sigma_H} = \mathbf{V} \text{ pour tout } \sigma_H$$

ssi

$$[E]_{\mathcal{I}_H, \sigma_H} = \mathbf{V} \text{ pour tout } \sigma_H$$

ssi \mathcal{I}_H est un modèle de E

Preuve du théorème de Herbrand

$$\mathcal{I}_H(p)(t_1, \dots, t_n) = \mathbf{V} \text{ ssi } \mathcal{I} \text{ est un modèle de la formule } p(t_1, \dots, t_n)$$

Soit une clause quelconque $E = \forall x_1 \dots \forall x_n (A_1 \vee \dots \vee A_k)$ où chaque A_i est un littéral. On veut montrer que \mathcal{I}_H est un modèle de E .

Par hypothèse $[E]_{\mathcal{I}, \sigma} = \mathbf{V}$ pour tout σ

ssi

$$(1) [(A_1 \vee \dots \vee A_k)]_{\mathcal{I}, \sigma} [x_1 := a_1] \dots [x_n := a_n] = \mathbf{V} \text{ pour tout } \sigma, a_1, \dots, a_n$$

Soient t_1, \dots, t_n une suite de termes clos. (cette suite existe car l'univers de Herbrand n'est pas vide). Soient $d_i = [t_i]_{\mathcal{I}, \sigma}$

(1) implique

$$(2) [(A_1 \vee \dots \vee A_k)]_{\mathcal{I}, \sigma} [x_1 := d_1] \dots [x_n := d_n] = \mathbf{V} \text{ pour tout } \sigma$$

implique

$$[A_i]_{\mathcal{I}, \sigma} [x_1 := d_1] \dots [x_n := d_n] = \mathbf{V} \text{ pour tout } \sigma$$

ssi (lemme avec $\tau = \{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$)

$$(3) [\tau(A_i)]_{\mathcal{I}, \sigma} = \mathbf{V} \text{ pour tout } \sigma$$

Arbres sémantiques complets

Définition : Soit B_0, B_1, B_2, \dots une énumération de tous les atomes clos d'une signature Σ . L'**arbre sémantique complet** associé à cette énumération est un arbre (binaire et équilibré) t.q.

- la racine est B_0
- chaque nœud B_i possède un arc gauche \mathbf{V} et un arc droit \mathbf{F}
- tous les successeurs de B_i sont étiquetés par B_{i+1}

Exercice :

- 1 Construire un arbre sémantique complet A_1 pour l'énumération finie $q(a), q(b), r(a), r(b)$.
- 2 Construire un arbre sémantique complet A_2 pour l'énumération infinie $q(a), q(b), q(s(a)), q(s(b)), q(s(s(a))), q(s(s(b))), \dots$

Nœud d'échec pour un ensemble de clauses

Définition : Soit A un arbre sémantique complet et soit \mathcal{C} un ensemble de clauses. Un nœud n de A est dit **nœud d'échec pour \mathcal{C}** ssi le segment de la branche qui va de la racine de A jusqu'à n suffit à falsifier au moins une instance close d'une clause de \mathcal{C} et si aucun prédécesseur de n n'est un nœud d'échec de A .

Exercice : Identifier dans les arbres A_1 et A_2 au moins un nœud d'échec pour l'ensemble de clauses $\{\neg r(x) \vee q(x), q(a), r(a)\}$.

Exercice : Si $\perp \in \mathcal{C}$, qu'est-ce qu'on peut dire par rapport aux nœuds d'échec pour \mathcal{C} ?

Arbres sémantiques partiels

Définition : Soit A un arbre sémantique complet et soit \mathcal{C} un ensemble de clauses. Un **arbre sémantique partiel** associé à \mathcal{C} est un arbre obtenu à partir de A en éliminant les sous-arbres issus des nœuds d'échec.

Définition : Un arbre sémantique partiel A est **clos** s'il est fini et si toute feuille de A est un nœud d'échec.

Exercice : Construire un arbre sémantique partiel clos associé à $\mathcal{C} = \{\neg r(x) \vee q(s(x)), r(a), \neg q(s(a))\}$.

Corollaire du théorème de Herbrand

Théorème : Soit \mathcal{C} un ensemble de clauses. Aucune interprétation de Herbrand ne satisfait \mathcal{C} ssi il existe un arbre sémantique partiel associé à \mathcal{C} qui est clos.

Corollaire : Un ensemble de clauses \mathcal{C} n'a pas de modèle ssi il existe un arbre sémantique partiel associé à \mathcal{C} qui est clos.

Complétude de la résolution

Lemme : Soient C_1 et C_2 deux clauses. Soient C'_1 et C'_2 deux instances de C_1 et C_2 respectivement. Soit C'_{res} la clause obtenue par application d'un pas de résolution (coupure ou factorisation) à C'_1 et C'_2 . Alors il existe une clause C_{res} t.q.

- C'_{res} est une instance de C_{res}
- C_{res} est obtenue par résolution à partir de C_1 et C_2 .

Théorème : La résolution est **complète** pour la réfutation, i.e., si Δ n'a pas de modèle, alors $\Delta \vdash_R \perp$.