Preuves en calcul des prédicats

Méthode de résolution de Robinson, extension de la méthode de résolution vue précédemment en calcul propositionnel

Dans ce chapitre toutes les formules sont closes

La méthode de résolution de Robinson pour prouver $\tau \models \varphi$

Calcul propositionnel

- Mettre $\tau \wedge \neg\varphi$ sous FNC
- On obtient un ensemble de clauses
- Tant qu'on peut obtenir une nouvelle clause en appliquant la méthode de résolution et qu'on n' a pas obtenu la clause vide, appliquer résolution

Calcul des prédicats

- Mettre $\tau \wedge \neg\varphi$ sous **forme prénexe**, puis sous **forme de Skolem**, puis sous FNC
- On obtient un ensemble de clauses
- Tant qu'on peut obtenir une nouvelle clause en appliquant la règle de résolution ou **la règle de diminution** et qu'on n' a pas obtenu la clause vide, appliquer résolution ou diminution

$\tau \models \varphi$ si et seulement si par méthode de résolution de Robinson on a obtenu la clause vide

Formes prénexes

Une formule φ est sous **forme prénexe** si elle est de la forme *:*

$$Q_1 x_1 \, Q_2 x_2 \, \ldots \, Q_n x_n \, \psi(x_1, x_2, \ldots, x_n)$$

où chaque Q_i est $\forall$ ou $\exists$ et où $\psi(x_1, x_2, \ldots, x_n)$ est une formule qui ne contient aucun quantificateur

Exemples

$\forall x \; \exists y \; p(x, y)$ est sous forme prénexe

$\forall x \; q(x) \; \exists y \; p(x, y)$ n'est pas sous forme prénexe

Théorème : toute formule peut être remplacée par une formule équivalente qui est sous forme prénexe

Comment trouver une forme prénexe équivalente ?

- Eliminer les $\Longrightarrow$ et les $\Leftrightarrow$ et n'utiliser que des $\wedge$ et des $\vee$
- Renommer les variables liées plusieurs fois afin de ne pas avoir de variable liée plusieurs fois
- Faire remonter les quantificateur en utilisant les équivalences :
  - $\neg \exists x A(x) \equiv \forall x \neg A(x)$
  - $\neg \forall x A(x) \equiv \exists x \neg A(x)$
  - $(C \vee \forall x A(x)) \equiv \forall x(C \vee A(x))$
  - $(C \vee \exists x A(x)) \equiv \exists x(C \vee A(x))$
  - $(\forall x A(x) \vee C) \equiv \forall x(A(x) \vee C)$
  - $(\exists x A(x) \vee C) \equiv \exists x(A(x) \vee C)$

  Et idem avec $\wedge$:
  - $(C \wedge \forall x A(x)) \equiv \forall x(C \wedge A(x))$
  - $(C \wedge \exists x A(x)) \equiv \exists x(C \wedge A(x))$
  - $(\forall x A(x) \wedge C) \equiv \forall x(A(x) \wedge C)$
  - $(\exists x A(x) \wedge C) \equiv \exists x(A(x) \wedge C)$

Exemple: trouver une forme de prénexe équivalente à

$$(\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})) \Longrightarrow (\exists \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x}))$$

$$(\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})) \Longrightarrow (\exists \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x}))$$

Élimination du $\Longrightarrow$:

$$\neg\big(\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})\big) \vee \big(\exists \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})\big)$$

Renommage de x, qui est liée 2 fois, en y :

$$\neg(\forall \boldsymbol{x}\ \boldsymbol{P}(\boldsymbol{x})) \vee (\exists \boldsymbol{y}\ \boldsymbol{P}(\boldsymbol{y}))$$

Remontée des quantificateurs à gauche :

$$(\exists \boldsymbol{x} \neg \boldsymbol{P}(\boldsymbol{x})) \vee (\exists \boldsymbol{y}\ \boldsymbol{P}(\boldsymbol{y}))$$

$$\exists \boldsymbol{x}(\neg \boldsymbol{P}(\boldsymbol{x})) \vee (\exists \boldsymbol{y}\ \boldsymbol{P}(\boldsymbol{y}))$$

$$\exists \boldsymbol{x} \exists \boldsymbol{y}(\neg \boldsymbol{P}(\boldsymbol{x}) \vee \boldsymbol{P}(\boldsymbol{y}))$$

Forme de Skolem

Soit $\varphi \equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n \, \boldsymbol{\psi(x_1, x_2, \dots, x_n)}$ une formule mise sous forme prénexe.

On appelle **forme de Skolem** de φ la formule φ^S obtenue en enlevant tous les quantificateurs $\exists$ et en remplaçant chacune des variables x_i quantifiée avec $\exists$ par $f_i(x_{j1}, x_{j2}, \dots x_{jn})$ où $x_{j1}, x_{j2}, \dots x_{jn}$ sont (toutes) les variables quantifiées par des $\forall$ placés avant le $\exists x_i$.

Les symboles fonctionnels f_i. introduits doivent être **tous différents** et être **différents de ceux déjà utilisés dans** φ

Lorsqu'il n'y a pas de quantificateur $\forall$ devant un $\exists x_i$ on introduit **un symbole de constante** (fonction 0-aire) qui remplace x_i

Exemple

$\exists x\ \forall y\ \exists z\ \forall u\ \exists v\ P(x,y,z,u,v)$

est skolémisée en :

$\forall y\ \forall u\ \ P(c,y,f(y),u,g(y,u))$ où c est une constante, f un fonction d'arité 1, et g une fonction d'arité 2

Remarque

La forme de skolem n'est pas nécessairement « équivalente » à la formule *initiale*

Exemple :

$$\forall x\, P(x)\ \vee \exists y\, Q(y)$$

peut être skolémisée en

$\forall x\ (Q(a)\ \vee P(x))$ ou en
$\forall x\ (P(x)\ \ \vee Q(f(x)))$

Pourquoi on peut quand même utiliser les formes de Skolem :

Théorème : toute formule sous forme prénexe ψ peut être remplacée par une formule skolémisée ψ^S telle que :

- ψ est satisfiable si et seulement si et ψ^S est satisfiable
- ψ est contradictoire si et seulement si et ψ^S est contradictoire.

Résolution en calcul des prédicats

Rappel : résolution en calcul propositionnel

On peut appliquer la méthode de résolution sur deux clauses C_1 et C_2 s'il existe un proposition P telle que P apparaît sous forme positive dans C_1 et sous forme négative dans C_2 :

De :

$C_1 : p \vee F_1$ $\qquad$ $C_2 : \neg p \vee F_2$

on déduit :

$F_1 \vee F_2$

En calcul des prédicats, ça se complique ….

$C_1 : p(x) \vee F_1$ $\qquad$ $C_2 : \neg p(y) \vee F_2$

$C_1 : p(a) \vee F_1$ $\qquad$ $C_2 : \neg p(y) \vee F_2$

$C_1 : p(a) \vee F_1$ $\qquad$ $C_2 : \neg p(b) \vee F_2$

Unification

l'**unification** est un processus algorithmique qui, étant donnés deux atomes, trouve si elle existe une **substitution** qui appliquée aux deux atomes les rend identiques.

Substitution : liste (finie) de couples (x|t) où x est une variable et t un terme qui ne contient pas x.
On remplace x par t

Exemple :
p(x, f(x,y), z) et
p(a, z, u) peuvent être unifiés par la substitution
(u|f(a,y)) (z|f(a,y)) (x|a), en
p(a,f(a,y),f(a,y)) :
On a d'abord remplacé :
x par a
puis z par f(a,y)
enfin u par f(a,y)

En revanche, p(a) et p(b) ne peuvent pas être unifiés

Deux atomes (= prédicat appliqué à des termes) sont ils unifiables ?

Non, s'il ne s'agit pas du même prédicat

Exemple : p(x,y) et q(x,y) ne sont pas unifiables

Si c'est le même

Oui ssi chacun des couples de termes est unifiable

Exemple : p(t1,t2) et p(t'1,t'2) sont unifiables ssi :

1. ***t1 et t'1 sont unifiables***
2. ***t2 et t'2 sont unifiables***

Deux termes (fonction appliquée à des termes) sont ils unifiables ?

Si l'un des termes est une variable x :

NON si l'autre est une fonction contenant x comme variable

Exemple : x et f(x,y) ne sont pas unifiables

OUI sinon

Exemple : x et f(y,y) sont unifiables par (x| f(y,y))

Exemple : x et y sont unifiables par (x| y) ou par (y| x)

Sinon // les 2 termes sont des fonctions

NON s'il ne s'agit pas de la même fonction.

Exemple : f(x) et g(y) ne sont pas unifiables

Si il s'agit de la même fonction :OUI ssi chacun des couples de termes (premier paramètre avec premier paramètre, etc) est unifiable.

Plus grand unificateur

Un unificateur le plus général possible, tout autre unificateur peut être obtenu en ajoutant des substitutions.

Exemple

Les termes f(x, x, y) et f(f(y, y, z), f(y, y, z), a) sont-ils unifiables ?

Oui si et seulement si

- x et f(y,y,z) sont unifiables
- x et f(y,y,z) sont unifiables
- y et a sont unifiables

- Donc oui avec comme plus grand unificateur (y|a)(x|f(y,y,z))

- Terme unifié : f(f(a,a,z),f(a,a,z),a)

Exemple

Les termes f(x, x, y) et f(f(y, y, z), f(y, x, z), a) sont-ils unifiables ?

Oui si et seulement si

- x et f(y,y,z) sont unifiable, ok
- x et f(y,x,z) sont unifiables nok
- y et a sont unifiables

- Donc non

Règle de résolution en calcul des prédicats

A partir des deux clauses $\boldsymbol{A \vee F_1}$ **et** $\boldsymbol{\neg B \vee F_2}$ où

- A et B sont deux atomes unifiables
- Φ est un renommage des variables tel que $\boldsymbol{\Phi(A \vee F_1)}$ et $\boldsymbol{\neg B \vee F_2}$ n'ont aucune variable commune
- σ est un plus grand unificateur de $\boldsymbol{\Phi(A)}$ et $\boldsymbol{B}$

On peut dériver la clause $\boldsymbol{\sigma(\Phi(F_1) \vee F_2)}$

Règle de diminution en calcul des prédicats

Rappel **: en calcul propositionnel, la clause P $\vee$ P $\vee$ F1 est « naturellement » réduite en P $\vee$ F1**

En calcul des prédicats, ça se complique ….

A partir de la clause $\boldsymbol{A \vee B \vee F_1}$ **où**

- A et B sont **deux atomes unifiables**
- $\boldsymbol{\sigma}$ est un plus grand unificateur de A et B

On peut dériver la clause $\boldsymbol{\sigma(A) \vee \sigma(F_1)}$

Exemple **: p(x,g(y))** $\vee$ **p(f(c),z)** $\vee$ **r(x,y,z)**
peut être réduit en p(f(c),g(y)) $\vee$ **r(f(c),y,g(y)) via l'unificateur (z|g(y)) (x|f(c))**

Exemple

Hypothèses :

- $\forall x((S(x) \lor T(x)) \Longrightarrow P(x))$
- $\forall x(S(x) \lor R(x))$
- $\neg R(a)$

Peut on en déduire P(a) ?

Pour cela, on essaye de déduire la clause vide des hypothèses et de la négation du résultat (soit ici : $\neg P(a)$)

Exemple (suite et fin)

∀x((S(x) v T(x)) $\Longrightarrow P(x)$)
Donne les 2 clauses C1 et C2 ci-dessous.

Et on obtient les clauses

- **C1: (¬ S(x) v P(x))**
- **C2: (¬ T(x) v P(x))**
- **C3: (S(x) v R(x))**
- **C4 : ¬ R(a)**
- **C5 : ¬ P(a)**

- Par résolution entre C3 et C4 avec la substitution (x|a) on obtient

C6: S(a)

- Par résolution entre C6 et C1 avec la substitution (x|a) on obtient

C7: P(a)

Par résolution entre C7 et C5 on obtient la clause vide.

On a construit un contre-exemple syntaxique montrant qu'on ne peut pas avoir les 5 clauses C1, C2, C3, C4 et C5.