TD2 - Conception et vérification de programmes

Bastien Maubert

1 Une preuve fastidieuse

Prouver que $\vdash \Box p \wedge \Diamond q \rightarrow \Diamond(p \wedge q)$

2 Au tableau

3 K est correct et complet

But : montrer que $\vdash \phi$ ssi $\models \phi$.

$Q1)$: Montrer la correction de K.

Pour la complétude on a besoin de quelques définitions.

Definition 1 ($\Gamma \vdash \phi$)
On écrit $\Gamma \vdash \phi$ si il existe un nombre fini de formules $\psi_1, \ldots, \psi_n \in \Gamma$ telles que $\vdash (\psi_1 \wedge \cdots \wedge \psi_n) \rightarrow \phi$.

Definition 2 (consistant)
Un ensemble de formules Γ est consistant si $\Gamma \nvdash \perp$.

Exemples : $\emptyset$ est consistant. $\{p\}$ est consistant. $\{p, \neg p\}$ n'est pas consistant : $\vdash p \wedge \neg p \rightarrow \perp$

Definition 3 (Ensemble maximal consistant)
Un emc est un ensemble de formules Γ tel que :
- Γ est consistant ;
- Γ est maximal : pour tout ensemble de formules Γ' tel que $\Gamma \subsetneq \Gamma'$, Γ' n'est pas consistant.

Maintenant quelques lemmes.

Lemma 1 (Lemme de Lindenbaum) *Si Γ est consistant, il existe un emc Γ' tel que $\Gamma \subseteq \Gamma'$.*

La preuve est constructive. Soit Γ un ensemble consistant. On essaye d'ajouter toutes les formules qui ne rendent pas l'ensemble inconsistant.

Soit $\psi_1, \psi_2, \ldots$ une enumeration des formules du language $\mathcal{L}_K$. On définit une suite d'ensembles de formules :

$$\Gamma_0 = \Gamma$$

Pour tout $n \geq 1$,

$$\Gamma_n = \begin{cases} \Gamma_{n-1} \cup \{\psi_n\}, & \text{si } \Gamma_{n-1} \cup \{\psi_n\} \text{ est consistant ;} \\ \Gamma_{n-1} \cup \{\neg\psi_n\}, & \text{sinon.} \end{cases}$$

On définit :

$$\Gamma' = \bigcup_{n \geq 0} \Gamma_n$$

Il ne reste que deux choses à montrer pour avoir le lemme de Lindenbaum :
$Q2$) : Prouver que Γ' est consistant.
$Q3$) : Prouver que Γ' est maximal.
Maintenant, définissons le modèle canonique.

Definition 4 (Modèle canonique)
Le modèle canonique est un tuple $\mathcal{M} = \{W,\ R,\ V\}$ avec :
- W est l'ensemble de tous les emc ;
- R est la relation binaire sur W définie par :
  wRu si pour toute formule $\psi \in u$, on a $\Diamond\psi \in w$;
- $V : \quad p \quad \mapsto \quad \{w \in W \mid p \in w\}$

Définition alternative de R, avec les $\Box$:
$Q4$) : Démontrer que wRu ssi pour toute formule χ telle que $\Box\chi \in w$, $\chi \in u$.
Encore un lemme :

Lemma 2 (Truth lemma) *Pour toute formule ψ, on a $\mathcal{M}, w \models \psi$ ssi $\psi \in w$.*

$Q5$) : Prouver ce lemme.
$Q6$) : Conclure en prouvant la complétude de K.

4 Model checking de $\mathcal{L}_K$

Problème : étant donnés un modèle pointé $\mathcal{M}, w$ et une formule ϕ de $\mathcal{L}_K$, décider si $\mathcal{M}, w \models \phi$. Montrer que le model checking de $\mathcal{L}_K$ est dans P.

5 Model checking de FO

Problème : étant donnés une formule ϕ de la logique du premier ordre, un modèle $\mathcal{M}$ et une interprétation des variables I, décider si $\mathcal{M}, I \models \phi$. Montrer que le model checking de FO est PSPACE-complet.