Rappelle de notions de base

Programmes et Preuves

Master 2 -Programmation et Logiciels Sûrs

Stefano Guerrini

2009/10

1 Logique classique

Les formules sont définies par récurrence comme le plus petit ensemble qui contient

1. toutes les éléments d'une ensemble non vide de formules atomiques ;
2. les formules $A_1 \vee A_2$ et $A_1 \wedge A_2$ et $A_1 \to A_2$ obtenues à partir d'une pair de deux formules quelconques A_1 et A_1 en utilisant une des connecteurs binaires $\wedge$, $\vee$ ou $\to$
3. les formules $\neg A$ obtenu à partir d'une formule quelconque A
4. la constant logique $\perp$ est une formule (on utilisera cette formule pour dénoter le faux).

On utilisera

- les lettres $A, B, C, \ldots$ pour dénoter des formules quelconques et les lettres $X, Y, Z, \ldots$ pour dénoter des formules atomiques ;
- le lettres grecques $\Gamma, \Delta, \ldots$ pour dénoter des multi-ensembles finis de formules.

1.1 Validité logique

Une évaluation σ est une fonction qui assigne à toute les formules atomiques une valeur de vérité, soit une valeur sur un ensemble binaire $\{0, 1\}$ (ou $\{\texttt{faux}, \texttt{vrai}\}$) où 0 dénote le faux et 1 le vrai.

L'évaluation σ induit une fonction d'évaluation définie sur toutes les formules définie par :

1. $[X]_\sigma = \sigma(X)$ si X est une formule atomique ;
2. $[A \vee B]_\sigma = \begin{cases} 0 & \text{si } [A]_\sigma + [B]_\sigma = 0 \\ 1 & \text{autrefois} \end{cases}$
3. $[A \wedge B]_\sigma = \begin{cases} 1 & \text{si } [A]_\sigma \cdot [B]_\sigma = 1 \\ 0 & \text{autrefois} \end{cases}$
4. $[A \to B]_\sigma = \begin{cases} 1 & \text{si } [A]_\sigma = 1 \text{ ou } [B]_\sigma = 0 \\ 0 & \text{autrefois} \end{cases}$
5. $[\neg A]_\sigma = \begin{cases} 1 & \text{si } [A]_\sigma = 0 \\ 0 & \text{autrefois} \end{cases}$
6. $[\perp]_\sigma = 0$

Soit Γ et Δ deux multi-esenmbles de formules. On écriera

$$\Gamma \Vdash_\sigma \Delta$$

qu'on lit Γ implique logiquement Δ par rapport à l'évaluation σ quand

1. soit il y a $A \in \Gamma$ telle que $[A]_\sigma = 0$;
2. soit $[A]_\sigma = 1$ pour toutes $A \in \Gamma$ et $[B] + \sigma = 1$ pour au moins une formule $B \in \Delta$.

On écriera

$$\Gamma \Vdash \Delta$$

si $\Gamma \Vdash_\sigma \Delta$ pour toutes les évaluations σ.

En particulier :

1. une formule A est une tautologie si $\Vdash A$;
2. un multi-ensemble de formules n'est pas satisfaisable si $\Gamma \Vdash$;
3. dans $\Gamma \Vdash \Delta$ ce n'est pas possible que tous les deux Γ et Δ soient vides au même temps, c'est à dire que si on pense à $\Vdash$ comme à une relation entre multi-ensembles alors $\Gamma \Vdash \Delta$ est faux si $\Gamma = \Delta = \emptyset$.

Si $\Gamma = A_1, \ldots, A_k$ et $\Delta = B_1, \ldots, B_h$ on écriera

$$\Gamma \to \Delta = \begin{cases} A_1 \wedge \cdots \wedge A_k \to B_1 \vee \ldots \vee B_k & \text{si } h, k > 0 \\ B_1 \vee \ldots \vee B_k & \text{si } k = 0 \text{ et } h > 0 \\ A_1 \wedge \cdots \wedge A_k \to \perp & \text{si } k > 0 \text{ et } h = 0 \\ \perp & \text{si } k = 0 \text{ et } h = 0 \end{cases}$$

Sur la base de cette définition on a que

$$\Gamma \Vdash_\sigma \Delta \qquad \text{ssi} \qquad [\Gamma \to \Delta]_\sigma$$

1.2 Quelques propriétés

1. Coupure ou utilisation d'une lemme
   (a) $\Gamma_1 \Vdash A, \Delta_1$ et $\Gamma_2, A \Vdash \Delta_2$ implique $\Gamma_1, \Gamma_2 \Vdash \Delta_1, \Delta_2$
2. Propriétés des connecteurs logiques
   (a) $\Gamma_1 \Vdash A_1, \Delta_1$ et $\Gamma_2 \Vdash A_2, \Delta_2$ implique $\Gamma_1, \Gamma_2 \Vdash A_1 \wedge A_2, \Delta_1, \Delta_2$;
   (b) $\Gamma \Vdash A_1, \Delta$ implique $\Gamma \Vdash A_1 \vee A_2, \Delta$,
   $\Gamma \Vdash A_2, \Delta$ implique $\Gamma \Vdash A_1 \vee A_2, \Delta$;
   (c) $\Gamma, A_1 \Vdash A_2, \Gamma$ implique $\Gamma \Vdash A_1 \to A_2, \Delta$;
   (d) $\Gamma, A_1 \Vdash \Delta$ implique $\Gamma, A_1 \wedge A_2 \Vdash \Delta$,
   $\Gamma, A_2 \Vdash \Delta$ implique $\Gamma, A_1 \wedge A_2 \Vdash \Delta$
   (e) $\Gamma_1, A_1 \Vdash \Delta_1$ et $\Gamma_2, A_2 \Vdash \Delta_2$ implique $\Gamma_1, \Gamma_2, A_1 \vee A_2 \Vdash \Delta_1, \Delta_2$;
   (f) $\Gamma_1 \Vdash A_1, \Delta_1$ et $\Gamma_2, A_2 \Vdash \Delta_2$ implique $\Gamma_1, \Gamma_2, A_1 \to A_2 \Vdash \Delta_1, \Delta_2$;
3. Propriétés structurelles
   (a) $\Gamma \Vdash A, A, \Delta$ implique $\Gamma \Vdash A, \Delta$

   (b) $\Gamma \Vdash \Delta$ implique $\Gamma \Vdash A, \Delta$
   (c) $\Gamma, A, A \Vdash \Delta$ implique $\Gamma, A \Vdash \Delta$
   (d) $\Gamma \Vdash \Delta$ implique $\Gamma, A \Vdash \Delta$

4. Quelques variations sur les propriétés des connecteurs logiques
   (a) $\Gamma \Vdash A_1, \Delta$ et $\Gamma \Vdash A_2, \Delta$ implique $\Gamma \Vdash A_1 \wedge A_2, \Delta$;
   (b) $\Gamma \Vdash A_1, A_2, \Delta$ implique $\Gamma \Vdash A_1 \vee A_2, \Delta$;
   (c) $\Gamma, A_1, A_2 \Vdash \Delta$ implique $\Gamma, A_1 \wedge A_2 \Vdash \Delta$
   (d) $\Gamma, A_1 \Vdash \Delta$ et $\Gamma, A_2 \Vdash \Delta$ implique $\Gamma, A_1 \vee A_2 \Vdash \Delta$

1.3 Le calcul des séquents : le système LK

Un séquent c'est une pair de multi-ensembles Γ, Δ qu'on écriera

$$\Gamma \vdash \Delta$$

Comme cas particulier on a le séquent vide $\vdash$ qui correspond au cas $\Gamma = \Delta = \emptyset$.

1. Règles identités :

$$\frac{}{A \vdash A}\,\texttt{ax} \qquad\qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\,\texttt{cut}$$

2. Règles logiques :

$$\frac{\Gamma_1 \vdash A_1, \Delta_1 \qquad \Gamma_2 \vdash A_2, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A_1 \wedge A_2, \Delta_1, \Delta_2}\,\wedge_i\texttt{R} \qquad\qquad \frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta}\,\wedge\texttt{L}$$

$$\frac{\Gamma \vdash A_i, \Delta}{\Gamma \vdash, A_1 \vee A_2, \Delta}\,\vee\texttt{R} \qquad\qquad \frac{\Gamma_1, A_1 \vdash \Delta_1 \qquad \Gamma_2, A_2 \vdash \Delta_2}{\Gamma_1 . \Gamma_2, A_1 \vee A_2 \vdash \Delta_1, \Delta_2}\,\vee_i\texttt{R}$$

$$\frac{\Gamma, A_1 \vdash A_2, \Delta}{\Gamma \vdash A_1 \to A_2, \Delta}\,\to\texttt{R} \qquad\qquad \frac{\Gamma_1 \vdash A_1, \Delta_1 \qquad \Gamma_2, A_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2, A_1 \to A_2 \vdash \Delta_1, \Delta_2}\,\to\texttt{L}$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\,\neg\texttt{R} \qquad\qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\,\neg\texttt{L}$$

3. Règles structurelles :

$$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\,\texttt{CR} \qquad\qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,\texttt{CL}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\,\texttt{WR} \qquad\qquad \frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\,\texttt{WL}$$

Une démonstration de LK c'est une arbre qui a comme feuille des instances des règles `ax` et qui est obtenu par application des règles de dérivation de LK.

On écriera,

$$\Gamma \vdash_{\texttt{LK}} \Delta$$

s'il existes une démonstration du calcul des séquents de LK qui termine avec le séquent $\Gamma \vdash \Delta$.

En utilisant les propriétés de 1.2, on démontre la correction de LK, cet à dire que

$$\Gamma \vdash_{\mathtt{LK}} \Delta \quad \Longrightarrow \quad \Gamma \Vdash \Delta$$

La correction de LK assure que le séquent vide $\vdash$ n'est pas démontrable (cet à dire que le système n'est pas contradictoire). Pourquoi ?

Par contre, le théorème de complétude (on ne le démontrera pas) montre que

$$\Gamma \vdash_{\mathtt{LK}} \Delta \quad \Longleftarrow \quad \Gamma \Vdash \Delta$$