Système F_ω

Documents autorisés (en particulier le poly).

Nous allons étudier le système F_ω, déjà vu rapidement en cours. Alors que le système F est une forme simplifiée de logique d'ordre 2, F_ω est essentiellement la même chose que la logique d'ordre supérieur (d'ordre ω).

On rappelle que F_ω est un système à trois niveaux:

1. les termes de preuve $s, t, u, v, \ldots$, qui ont pour types les formules $F, G, \ldots$;
2. les expressions logiques S, T, $\ldots$, ont pour types les sortes K, L, $\ldots$; parmi les expressions logiques, les formules sont celles qui sont de sorte $Prop$;
3. les sortes, parmi lesquelles la sorte $Prop$ des formules, et la sorte ι des individus (termes du premier ordre).

De façon formelle, les *sortes* sont définies par la grammaire:

$$K \quad ::= \quad Prop \mid \iota \mid K \to K$$

Les *pré-expressions logiques* sont définies par la grammaire:

$$S, T, \ldots \quad ::= \quad X_K \mid \lambda X_K \cdot T \mid S\,T \mid \mathrm{Imp} \mid \mathrm{All}_K$$

où la notation X_K dénote une variable de sorte K, et l'on suppose qu'il existe une infinité dénombrable de variables de sorte K, pour chaque sorte K. Il y a d'autre part une constante All_K pour chaque sorte K. On notera en abrégé:

$$\begin{aligned} F \Rightarrow G &= \mathrm{Imp}\ F\ G \\ \forall X : K \cdot F &= \mathrm{All}_K(\lambda X_K \cdot F) \end{aligned}$$

Une *expression logique* S de sorte K est une pré-expression logique telle que l'on puisse déduire $\triangleright S : K$ dans le système suivant:

$$\frac{}{\triangleright X_K : K}\,(KVar) \qquad \frac{}{\triangleright \mathrm{Imp} : Prop \to Prop \to Prop}\,(\mathrm{Imp}) \qquad \frac{}{\triangleright \mathrm{All}_K : (K \to Prop) \to Prop}\,(\mathrm{All}_K)$$

$$\frac{\triangleright S : K \to K' \quad \triangleright T : K}{\triangleright S\,T : K'}\,(KApp) \qquad \frac{\triangleright T : K'}{\triangleright \lambda X_K \cdot T : K \to K'}\,(KAbs)$$

Il s'agit donc d'un typage simple du λ-calcul formé des pré-expressions logiques, en style de Church, c'est-à-dire où toutes les variables sont annotées par le type (la sorte) qu'elle doivent avoir. On n'a donc pas besoin de contexte de typage pour définir le type des variables. Ce calcul, muni de la règle de réduction $(\lambda X_K \cdot S)T \to S[X_K := T]$, est confluent et fortement normalisant.

On observera, ce que l'on n'a pas besoin de démontrer, que pour toute pré-expression logique T, il existe au plus une sorte K telle que $\triangleright T : K$ soit dérivable. K sera *la sorte* de T, et l'on notera parfois $T : K$ pour le rappeler.

Les *termes de preuve* sont juste les λ-termes usuels:

$$s, t, u, v, \ldots \quad ::= \quad x \mid \lambda x \cdot s \mid st$$

Nous utiliserons les règles de réduction suivantes, collectivement nommées *β-réduction*:

$$\begin{array}{rcl}(\lambda x \cdot u)v & \to & u[x := v] \\ (\lambda X_K \cdot S)T & \to & S[X_K := T]\end{array}$$

Nous noterons encore $\to$ la relation de réécriture par β-réduction, $\to^*$ sa clôture réflexive-transitive, $=_\beta$ sa clôture réflexive-symétrique-transitive (β-conversion).

Les règles de typage de F_ω sont formées à l'aide de jugements $\Gamma \vdash u : F$, où Γ est un ensemble de couples $y : G$, avec y des variables distinctes deux à deux et G une formule (c'est-à-dire que l'on peut dériver $\triangleright G : Prop$). On notera que ce ne sont pas exactement les règles de typage du système F_ω du poly.

$$\frac{\triangleright F_1 : Prop \quad \ldots \triangleright F_n : Prop}{x_1 : F_1, \ldots, x_n : F_n \vdash x_i : F_i}\ (Ax) \qquad \frac{\Gamma \vdash u : F_1 \quad \triangleright F_2 : Prop \quad F_1 =_\beta^* F_2}{\Gamma \vdash u : F_2}\ (=_\beta)$$

$$\frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2}\ (\Rightarrow E) \qquad \frac{\Gamma, x : F_1 \vdash u : F_2}{\Gamma \vdash \lambda x \cdot u : F_1 \Rightarrow F_2}\ (\Rightarrow I)$$

$$\frac{\Gamma \vdash u : \forall X : K \cdot F \quad \triangleright S : K}{\Gamma \vdash u : F[X_K := S]}\ (\forall E) \qquad \frac{\Gamma \vdash u : F}{\Gamma \vdash u : \forall X : K \cdot F}\ (\forall I)$$

(X_K non libre dans aucune formule de Γ)

On observera, ce qui ne nécessitera pas de démonstration, que, si l'on peut dériver $\Gamma \vdash u : F$, alors on peut dériver $\triangleright F : Prop$; de plus, si Γ s'écrit $x_1 : F_1, \ldots, x_n : F_n$, alors on peut dériver $\triangleright F_i : Prop$ pour tout i, $1 \leq i \leq n$.

On rappelle qu'un *candidat* C est un ensemble de λ-termes vérifiant:

CR1 tout élément de C est dans SN, l'ensemble des λ-termes fortement normalisants;

CR2 si $u \in C$ et $u \to u'$, alors $u' \in C$;

CR3 si u est neutre, et si (pour tout u' tel que $u \to u'$, $u' \in C$), alors $u \in C$; (parenthèses ajoutées pour bien montrer la portée du quantificateur universel sur u'.)

Un terme est neutre s'il ne commence pas par λ. On note $\mathcal{CR}$ l'ensemble de tous les candidats, et Λ l'ensemble des λ-termes (les termes de preuve).

On définit une interprétation des sortes et des expressions logiques comme suit.

Sortes $[\![Prop]\!] = \mathcal{CR}$, $[\![\iota]\!] = SN$, $[\![K \to K']\!]$ est l'ensemble de toutes les fonctions (totales) de $[\![K]\!]$ vers $[\![K']\!]$;

Expressions logiques Une expression logique S de sorte K est interprétée dans un *contexte* ρ, qui à chaque variable $X_{K'}$ associe un élément de $[\![K']\!]$. Formellement, on définit une interprétation d'une expression logique $S : K$ dans ρ, notée $[\![S : K]\!]\rho$. On pose:

$$\begin{array}{rcl}[\![X_K : K]\!]\rho & = & \rho(X_K) \\ [\![\mathrm{Imp} : Prop \to Prop \to Prop]\!]\rho & = & (C_1 \in \mathcal{CR} \mapsto (C_2 \in \mathcal{CR} \mapsto C_1 \Rrightarrow C_2)) \\ \text{où } C_1 \Rrightarrow C_2 & = & \{u \in \Lambda \mid \forall v \in C_1 \cdot uv \in C_2\} \\ [\![\mathrm{All}_K : (K \to Prop) \to Prop]\!]\rho & = & (f \in [\![K \to Prop]\!] \mapsto \bigcap_{a \in [\![K]\!]} f(a)) \\ \text{où } \bigcap_{a \in A} f(a) & = & \{u \in \Lambda \mid \forall a \in A \cdot u \in f(a)\} \\ [\![ST : K']\!]\rho & = & [\![S : K \to K']\!]\rho([\![T : K]\!]\rho) \\ [\![\lambda X_K \cdot T : K \to K']\!]\rho & = & (a \in [\![K]\!] \mapsto [\![T : K']\!](\rho[X_K \mapsto a]))\end{array}$$

où la notation $(a \in A \mapsto f(a))$ dénote la fonction qui à tout élément a de A associe la quantité $f(a)$, et $\rho[X_K \mapsto a]$ est le contexte qui à X_K associe a, et à toute autre variable Y associe $\rho(Y)$. Dans le cas de $ST : K'$, K est l'unique sorte telle que $\triangleright T : K$ soit dérivable.

On notera que l'on a:

$$[\![F_1 \Rightarrow F_2]\!]\rho \quad = \quad \{u \in \Lambda \mid \forall v \in [\![F_1]\!]\rho \cdot uv \in [\![F_2]\!]\rho\}$$

C'est une vérification élémentaire, qui ne dépend que du fait que $[\![F_1]\!]\rho$ et $[\![F_2]\!]\rho$ soient effectivement des candidats (ce que l'on demandera de montrer plus bas). On rapprochera cette formule de la formule définissant l'ensemble $RED^{\rho}_{F_1 \Rightarrow F_2}$ dans le cours, où ρ était un contexte de candidats: $RED^{\rho}_{F_1 \Rightarrow F_2} = \{u \in \Lambda \mid \forall v \in RED^{\rho}_{F_1} \cdot uv \in RED^{\rho}_{F_2}\}$.

On notera que l'on a aussi:

$$[\![\forall X_K \cdot F]\!]\rho \quad = \quad \{u \in \Lambda \mid \forall a \in [\![K]\!] \cdot u \in [\![F]\!](\rho[X_K \mapsto a])\}$$

dès que l'on peut assurer que $[\![F]\!](\rho[X_K \mapsto a])$ est bien dans $[\![Prop]\!] = \mathcal{CR}$ pour tout $a \in [\![K]\!]$. En particulier,

$$\left[\!\!\left[\forall X_{Prop} \cdot F\right]\!\!\right]\rho \quad = \quad \{u \in \Lambda \mid \forall C \in \mathcal{CR} \cdot u \in [\![F]\!](\rho[X_{Prop} \mapsto C)\}$$

ce que l'on rapprochera de la formule du cours $RED^{\rho}_{\forall\alpha \cdot F} = \{u \in \Lambda \mid \forall C \in \mathcal{CR} \cdot u \in RED^{\rho[\alpha \mapsto C]}_{F}\}$.

1. Montrer que $[\![K]\!]$ n'est pas vide, pour aucune sorte K.

2. Montrer que pour toute expression logique $T : K$, pour tout contexte ρ, $[\![T : K]\!]\rho$ est un élément de $[\![K]\!]$. (Indication: attention, lorsque A est vide, on a $\bigcap_{a \in A} f(a) = \Lambda$. Si vous ne voyez pas pourquoi je dis ça à la fin de la question, vous avez raté un point important.)

3. Montrer que, pour tous candidats C_1 et C_2, pour tout λ-terme u tel que (pour tout $v \in C_1$, $u[x := v]$ est dans C_2), alors $\lambda x \cdot u$ est dans $C_1 \Rrightarrow C_2$.

4. On admettra le lemme de substitution classique: si $\triangleright \forall X : K \cdot F : Prop$ et $\triangleright S : K$ sont dérivables, alors $[\![F[X_K := S] : Prop]\!]\rho = [\![F : Prop]\!](\rho[X_K \mapsto [\![S]\!]\rho])$. On admettra aussi que $[\![F : Prop]\!]\rho$ ne dépend que des variables libres de F, autrement dit que si $\rho(X_K) = \rho'(X_K)$ pour toute variable X_K libre dans F, alors $[\![F : Prop]\!]\rho = [\![F : Prop]\!]\rho'$.

   Démontrer que, si $x_1 : G_1, \ldots, x_n : G_n \vdash u : F$ est dérivable, alors pour tout contexte ρ, pour tous termes $v_1 \in [\![G_1 : Prop]\!], \ldots, v_n \in [\![G_n : Prop]\!]$, on a $u[x_1 := v_1, \ldots, x_n := v_n] \in [\![F : Prop]\!]$.

5. En déduire que tout terme typable en F_ω est fortement normalisant. Autrement dit, si $\Gamma \vdash u : F$ est dérivable en F_ω, alors u est fortement normalisant.

6. En déduire que F_ω est cohérente, au sens où il n'existe pas de terme de preuve u tel que $\vdash u : \bot$, où le faux logique, $\bot$, est défini comme $\forall X_{Prop} \cdot X$.