Devoir de λ-calcul 2016

Autour des types union

David Baelde

À rendre le 3 mai

Nous allons considérer plusieurs extensions du λ-calcul simplement typé, en étendant les termes et/ou les types et/ou la réduction $\to$ considérée sur les termes. On dira, dans tous les cas, qu'un terme est *neutre* s'il n'est pas de la forme $\lambda x.u$. Enfin, comme dans le cours, un ensemble S est un candidat de réductibilité ($S \in \mathbf{CR}$) quand :

(CR1) $S \subseteq \mathbf{SN}$;

(CR2) si $u \in S$ et $u \to v$ alors $v \in S$;

(CR3) si u est neutre et $v \in S$ pour tout $u \to v$, alors $u \in S$.

Si un terme n'est pas neutre, on dira que c'est une *valeur* (attention, une valeur n'est pas forcément une forme normale pour $\to$). On notera $\mathcal{V}$ l'ensemble des valeurs. Étant donné un ensemble de termes S, on définit de plus

$$\mathcal{V}(S) = \{\ v \in \mathcal{V}\ :\ u \to^* v \text{ pour un } u \in S\ \}$$

et, pour un terme u, on écrira $\mathcal{V}(u)$ pour $\mathcal{V}(\{u\})$.

1 Réécriture simple

Dans cette section, on étend le λ-calcul simplement typé avec des constructeurs équipés de réductions simples, et on adapte aisément deux résultats clés : la réduction du sujet et la normalisation forte des termes bien typés. Étant donné un ensemble de symboles du premier ordre Σ, on définit les termes du λ-calcul étendu avec Σ (noté Λ_Σ) ainsi :

$$u, v ::= x \mid u\ v \mid \lambda x.u \mid \mathsf{f}(u_1, \ldots, u_n) \qquad \mathsf{f} \in \Sigma \text{ d'arité } n$$

On se donne de plus un ensemble de règles de réécriture de la forme $\mathsf{f}(x_1, \ldots, x_n)\ R\ u$ où les x_i sont des variables distinctes et u est un terme de Λ_Σ. On définit $\to_{\beta R}$ comme la plus petite relation de réécriture contenant β et R.

Côté typage, on ajoute la règle suivante aux trois règles du λ-calcul simplement typé :

$$\frac{\{\ \Gamma \vdash u_i : T_i\ \}_{1 \leq i \leq n} \quad \{\ \Gamma, x_1 : T_1, \ldots, x_n : T_n \vdash r : T\ \}_{\mathsf{f}(x_1,\ldots,x_n) R r}}{\Gamma \vdash \mathsf{f}(u_1, \ldots, u_n) : T}\ \textsc{Fun}_R$$

Étant donné un symbole f d'arité n et pour lequel on a k réductions possibles dans R, la règle ci-dessus a $n+k$ prémisses.

Question 1
On prend $\Sigma = \{\mathsf{d}\}$ avec d d'arité 2, équipé des réductions $\mathsf{d}(x,y)\ R\ (x\ y)$ et $\mathsf{d}(x,y)\ R\ y$. On pose $I = \lambda x.x$. Parmi les termes suivants, lesquels sont typables ? Justifier.

(a) $\mathsf{d}(I, I)$
(b) $\lambda x.\mathsf{d}(x, x)$

Correction 1
Le premier est typable, le second non ; je ne justifie pas.

Question 2
Montrer la réduction du sujet : si $\Gamma \vdash u : T$ et $u \to_{\beta R} v$ alors $\Gamma \vdash v : T$. On se concentrera sur la nouveauté dans l'argument par rapport au cas vu en cours.

Correction 2
Non corrigé.

Nous allons voir que les termes bien typés sont de plus fortement normalisants, en adaptant l'argument de réductibilité vu en cours. Les types étant les types simples du λ-calcul, on peut les interpréter comme dans le cours. On obtient, pour tout T, $\mathrm{RED}_T \in \mathbf{CR}$.

Question 3
Montrer le lemme d'adéquation : si $x_1 : T_1, \ldots, x_n : T_n \vdash u : T$ et $\sigma(x_i) \in \mathrm{RED}_{T_i}$ pour tout i, alors $u\sigma \in \mathrm{RED}_T$. On ne détaillera que le seul nouveau cas, celui de la règle $\textsc{Fun}_R$.

Correction 3
Non corrigé.

2 Unions implicites

On oublie provisoirement l'extension précédente, en reprenant donc les termes usuels du λ-calcul :

$$u, v ::= x \mid u\ v \mid \lambda x.u$$

Par contre, on étend les types avec les constructions d'union et d'intersection :

$$T, T' ::= \alpha \mid T \Rightarrow T' \mid T \sqcup T' \mid T \sqcap T'$$

On considère la β-réduction usuelle sur les termes, et le système de types obtenu en ajoutant les règles suivantes aux règles du λ-calcul simplement typé :

$$\frac{\Gamma \vdash u : T_1 \quad \Gamma \vdash u : T_2}{\Gamma \vdash u : T_1 \sqcap T_2}\ \sqcap I \qquad \frac{\Gamma \vdash u : T_1 \sqcap T_2}{\Gamma \vdash u : T_i}\ \sqcap E$$

$$\frac{\Gamma \vdash u : T_i}{\Gamma \vdash u : T_1 \sqcup T_2}\ \sqcup I \qquad \frac{\Gamma \vdash v : T_1 \sqcup T_2 \quad \Gamma, x : T_1 \vdash u : T \quad \Gamma, x : T_2 \vdash u : T}{\Gamma \vdash u[x := v] : T}\ \sqcup E$$

Dans la règle $\sqcup E$, on exige que x ne soit pas déja présent dans Γ (et donc pas libre dans v).

Nous allons d'abord voir que le système est fortement normalisant.

Question 4
Soit u neutre et $v \in \mathcal{V}$ tel que $u \to_\beta^* v$. Montrer que u a un redex de tête et que sa réduction $u \to_t u'$ donne un terme u' tel que $u' \to_\beta^* v$. (Indication : pensez à la réduction standard $\Rightarrow_s$.)

Correction 4
On a vu en cours que $u \to_\beta^* v$ entraîne $u \Rightarrow_s v$. Comme v est une valeur, il s'écrit en forme de tête $\lambda x_1 \dots x_n .\ v_1 \dots v_m$ avec $n > 0$. Par définition de $\Rightarrow_s$, on a donc $u \to_t^* \lambda x_1 \dots x_n .\ u_1 \dots u_m$ (forme de tête) avec $u_i \Rightarrow_s v_i$ pour tout $1 \leq i \leq m$. Puisque u est neutre, et que $n > 0$, on peut même dire $u \to_t^+ \lambda x_1 \dots x_n .\ u_1 \dots u_m$ avec $u_i \Rightarrow_s v_i$ pour tout i. Enfin, puisque $\Rightarrow_s$ et $\to_t$ sont incluses dans $\to_\beta^*$, on a comme attendu $u \to_t u' \to_\beta^* v$.

Question 5
Soit $X \in \mathbf{CR}$ et $u \in \mathbf{SN}$. Montrer que $\mathcal{V}(u) \subseteq \mathcal{V}(X)$ entraîne $u \in X$.

Correction 5
On procède par induction sur $u \in \mathbf{SN}$. Si u n'est pas neutre, on conclut par hypothèse et CR2 : $u \in \mathcal{V}(u) \subseteq \mathcal{V}(X) \subseteq X$. Sinon, par CR3 il suffit de montrer que $u \to_\beta v$ entraîne $v \in X$. C'est évident : $u \to_\beta v$ entraîne $\mathcal{V}(v) \subseteq \mathcal{V}(u) \subseteq \mathcal{V}(X)$, ce qui permet de conclure par hypothèse d'induction.

Question 6
En s'appuyant sur les deux questions précédentes, montrer que $X, Y \in \mathbf{CR}$ entraîne $X \cup Y \in \mathbf{CR}$.

Correction 6
Seule CR3 est non triviale. Soit u neutre dont tous les réduits sont dans $X \cup Y$. On en déduit que $u \in \mathbf{SN}$. Si $\mathcal{V}(u) = \emptyset$ alors par la question précédente $u \in X$ (et même $u \in Y$) ce qui permet de conclure : $u \in X \cup Y$. Sinon, u a un redex de tête, $u \to_t v$, et $\mathcal{V}(u) \subseteq \mathcal{V}(v)$. On a, par hypothèse, $v \in X \cup Y$. Supposons, par symétrie, que $v \in X$. Alors $\mathcal{V}(u) \subseteq \mathcal{V}(v) \subseteq \mathcal{V}(X)$ donc $u \in X$, et $u \in X \cup Y$.

On étend l'interprétation des types en posant $\mathrm{RED}_{T \sqcap T'} = \mathrm{RED}_T \cap \mathrm{RED}_{T'}$ et $\mathrm{RED}_{T \sqcup T'} = \mathrm{RED}_T \cup \mathrm{RED}_{T'}$. On a vu en TD que la première construction donne bien un candidat, et la question précédente nous l'assure pour la deuxième construction.

Question 7
Montrer le lemme d'adéquation pour notre système, en ne détaillant que les cas non traités en cours et TD.

Correction 7
Non corrigé.

Malgré ce bon départ, nous allons voir que notre système laisse à désirer : il ne jouit pas de la réduction du sujet.

Question 8
On pose $I = \lambda x.x$ et $\Gamma = \big(x : T,\ y : T \Rightarrow T_1 \sqcup T_2,\ z : (T_1 \Rightarrow T_1 \Rightarrow T') \sqcap (T_2 \Rightarrow T_2 \Rightarrow T')\big)$.
Montrer $\Gamma \vdash z\ (y\ (I\ x))\ (y\ (I\ x)) : T'$ au moyen de la règle $\sqcup E$.

Correction 8
Non corrigé.

Question 9
Étant donné un ensemble de types L, on note L^* le plus petit ensemble de types contenant L et clos par $\sqcap$ et $\sqcup$.

(a) Montrer que $\Gamma \vdash z : A$ ssi $A \in \{T_1 \Rightarrow T_1 \Rightarrow T', T_2 \Rightarrow T_2 \Rightarrow T'\}^*$.

(b) Montrer que $\Gamma, w : B \vdash z\ t_1\ t_2 : C$ ssi il existe un $1 \le i \le 2$ tel que pour tout $1 \le j \le 2$ on a $\Gamma, w : B \vdash t_j : T_i$.

(c) Montrer que $z\ (y\ x)\ (y\ (I\ x))$ n'est pas typable dans l'environnement Γ.

Correction 9
Cette question est annulée : les deux premiers points sont faux ; le dernier est vrai mais je n'ai pas preuve simple.

Encore pire, nous montrons maintenant que ce système de types union n'est pas compatible avec l'ajout de réécritures comme vues en première partie. On considère l'extension du langage des termes avec le constructeur binaire $+$ équipé des réduction $u + v \mathcal{R} u$ et $u + v \mathcal{R} v$.

Question 10
On pose $\delta = \lambda x.x\ x$, $t_1 = \lambda z.z\ y\ \delta$ et $t_2 = \lambda z.\delta$.

(a) Montrer que $(t_1\ t_1) \in \mathbf{SN}$, $(t_2\ t_2) \in \mathbf{SN}$ mais $(t_1\ t_2) \notin \mathbf{SN}$.

(b) Montrer qu'il existe T_1, T_2, Y et U tel que $y : Y \vdash t_i : T_i$ (pour tout $1 \le i \le 2$) et $y : Y, x : T_i \vdash x\ x : U$. (On rappelle que les types intersection permettent de typer tout terme fortement normalisant.)

(c) En déduire qu'on peut typer $(t_1 + t_2)\ (t_1 + t_2)$ dans l'environnement $y : Y$, conclure que les termes typables ne sont pas tous fortement normalisables.

Correction 10
Non corrigé.

Question 11
L'observation précédente implique qu'en présence de réécriture (i.e., avec la réduction $\rightarrow_{\beta R}$) l'union de deux candidats n'est plus forcément un candidat. Le démontrer explicitement en considérant les candidats X_1 et X_2, où X_i est le plus petit candidat contenant le terme t_i de la question précédente.

Correction 11
Non corrigé.

3 Une réunion possible

Nous allons maintenant réunir les deux extensions vues précédemment, de façon à obtenir réduction du sujet et forte normalisation. Pour cela on ajoute une construction aux termes :

$$u, v ::= x \mid u\ v \mid \lambda x.u \mid \mathsf{f}(u_1, \ldots, u_n) \mid \mathsf{let}\ x = v\ \mathsf{in}\ u$$

On considère la réduction $\to_{\beta R\,\mathsf{let}}$, plus petite relation de réécriture contenant $\to_{\beta R}$ et telle que

$$\mathsf{let}\ x = v\ \mathsf{in}\ u \to_{\beta R\,\mathsf{let}} u[x := v] \quad \text{si } v \text{ est une valeur.}$$

Étant donné $X, Y \in \mathbf{CR}$, on définit $X \sqcup Y$ comme le plus petit $Z \in \mathbf{CR}$ tel que $X \cup Y \subseteq Z$. On étend ensuite l'interprétation des types en posant $\mathrm{RED}_{T \sqcap T'} = \mathrm{RED}_T \cap \mathrm{RED}_{T'}$ et $\mathrm{RED}_{T \sqcup T'} = \mathrm{RED}_T \sqcup \mathrm{RED}_{T'}$.

Question 12
Soit $X, Y \in \mathbf{CR}$. Montrer que $u \in X \sqcup Y$ entraîne $\mathcal{V}(u) \subseteq \mathcal{V}(X \cup Y)$.

Correction 12
On observe que $X \sqcup Y = X \cup Y \cup Z$ où Z est l'ensemble des termes neutres et fortement normalisants dont tous les réduits (pas forcément en un pas) non neutres sont dans $X \cup Y$. On vérifie aisément que $X \cup Y \cup Z$ vérifie CR1, CR2 et CR3. De plus, tout candidat contenant $X \cup Y$ contient aussi Z (par induction sur la forte normalisation de $z \in Z$) donc $X \cup Y \cup Z$ est bien le plus petit candidat contenant $X \cup Y$, c'est à dire $X \sqcup Y$ par définition.

Soit maintenant $u \in X \sqcup Y$. Si $u \in X$, alors on a $\mathcal{V}(u) \subseteq \mathcal{V}(X) \subseteq \mathcal{V}(X \cup Y)$ par CR2. On conclut de même quand $u \in Y$. Enfin, si $u \in Z$, alors par définition de Z on a $\mathcal{V}(u) \in \mathcal{V}(X \cup Y)$.

Question 13
Montrer le lemme d'adéquation pour notre système.

Correction 13
On reprend la preuve usuelle par induction sur une dérivation de typage, en distinguant les cas en fonction de la dernière règle. Les seules règles problématiques (non nouvelles) sont celles liées à l'union. On a déja vu que l'introduction ne pose pas de problème, car $X \subseteq X \sqcup Y$. Considérons l'élimination :

$$\frac{\Gamma \vdash v : T_1 \sqcup T_2 \quad \Gamma, x : T_1 \vdash u : T \quad \Gamma, x : T_2 \vdash u : T}{\Gamma \vdash \mathsf{let}\ x = v\ \mathsf{in}\ u : T}$$

Soit σ tel que $\sigma(y) \in \mathrm{RED}_A$ pour tout $(y : A) \in \Gamma$. Par hypothèse d'induction $u\sigma[x := x] \in \mathrm{RED}_T$ et $v\sigma \in \mathrm{RED}_{T_1 \sqcup T_2}$, donc $u\sigma$ et $v\sigma$ sont fortement normalisants. On procède alors par induction sur $u\sigma \in \mathbf{SN}$ et $v\sigma \in \mathbf{SN}$ (l'un puis l'autre, dans un ordre indifférent) et en utilisant (CR3) pour montrer $(\mathsf{let}\ x = v\ \mathsf{in}\ u)\sigma \in \mathrm{RED}_T$. Les réduits de ce terme sont de la forme $\mathsf{let}\ x = v'\ \mathsf{in}\ u\sigma$ ou $\mathsf{let}\ x = v\sigma\ \mathsf{in}\ u'$ (avec $v\sigma \to v'$ et $u\sigma \to u'$) ou bien $u\sigma[x := v\sigma]$. Dans les deux premiers cas on conclut par hypothèse d'induction sur u' ou v'. Pour le dernier cas, on a vu que $v\sigma \in \mathrm{RED}_{T_1 \sqcup T_2}$. Comme c'est une valeur on conclut $v\sigma \in \mathcal{V}(T_i)$ pour un i, par la question précédente. A fortiori, $v\sigma \in \mathrm{RED}_{T_i}$, ce qui nous permet de conclure, de nouveau par hypothèse d'induction, que $u\sigma[x := v\sigma] \in \mathrm{RED}_T$.

Question 14
Soit v une valeur. Montrer que si $\Gamma \vdash v : (T_1 \sqcup T_2) \sqcap T'$ alors $\Gamma \vdash v : T_i$ pour un $1 \leq i \leq 2$. (On s'autorisera ici à travailler modulo associativité et commutativité sur l'intersection.)

Correction 14
Les valeurs sont les termes de la forme $\lambda x.u$. On procède par induction sur la dérivation de typage, qui ne peut commencer que par trois règles étant donné la forme du type et du terme :

- Si c'est un $\sqcup I$ (possible uniquement si T' est vide) on conclut immédiatemment.
- Si c'est un $\sqcap E$ on conclut par hypothèse d'induction sur la sous-dérivation, avec un T' enrichi.
- Si c'est un $\sqcap I$ on a forcément $T' = T'_1 \sqcap T'_2$ et on conclut par hypothèse d'induction, indifféremment, sur l'une des deux sous-dérivations, de type $(T_1 \sqcup T_2) \sqcap T'_i$.

Question 15
Montrer la réduction du sujet.

Correction 15
Le seul nouveau cas est la réduction du let. On considère donc $\mathsf{let}\ x = v\ \mathsf{in}\ u \to_{\mathsf{let}} u[x := v]$ avec :

$$\frac{\Gamma \vdash v : T_1 \sqcup T_2 \quad \Gamma, x : T_1 \vdash u : T \quad \Gamma, x : T_2 \vdash u : T}{\Gamma \vdash \mathsf{let}\ x = v\ \mathsf{in}\ u : T}$$

Par la question précédente, on a $\Gamma \vdash v : T_i$. Cela permet de conclure, par substitution, que $\Gamma \vdash u[x := v] : T$.