Université Paris Diderot - L3 Année 2016-2017

Devoir Maison de Logique n° 3
(Correction)

Théorie de la preuve, Unification et Résolution dans le calcul des prédicats

À rendre le 27/4 à votre chargée de TD.

Exercice 1 [TD8, exercice 6]

- Prouvez les séquents suivants dans $\mathcal{G}$:

  1. $\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$
     Correction:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall y P(x,y), P(x,y) \vdash P(x,y), \exists x P(x,y)}}{\forall y P(x,y), P(x,y) \vdash \exists x P(x,y)}\;\exists\text{-d}}{\forall y P(x,y) \vdash \exists x P(x,y)}\;\forall\text{-g}}{\forall y P(x,y) \vdash \forall y \exists x P(x,y)}\;\forall\text{-d}}{\exists x \forall y P(x,y) \vdash \forall y \exists x P(x,y)}\;\exists\text{-g}$$

  2. $\forall x.(P \vee Q(x)) \vdash P \vee \forall x.Q(x)$
     Correction:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(P \vee Q(x)), P \vdash P, Q(x)} \qquad \dfrac{}{\forall x(P \vee Q(x)), Q(x) \vdash P, Q(x)}}{\forall x(P \vee Q(x)), P \vee Q(x) \vdash P, Q(x)}\;\vee\text{-g}}{\forall x(P \vee Q(x)) \vdash P, Q(x)}\;\forall\text{-g}}{\forall x(P \vee Q(x)) \vdash P, \forall x Q(x)}\;\forall\text{-d}}{\forall x(P \vee Q(x)) \vdash P \vee \forall x Q(x)}\;\vee\text{-d}$$

- Énoncer et démontrer la correction de la règle $\exists g$ du système $\mathcal{G}$.
  Correction: (Par contradiction) Soit $F1$ et$F2$ les deux formules suivantes :

$$\begin{array}{rcl} F1 & = & (\overline{\Delta} \wedge A) \to \underline{\Gamma} \\ F2 & = & (\overline{\Delta} \wedge \exists x.A) \to \underline{\Gamma} \end{array}$$

où $\overline{\Delta}$ dénote la conjonction des formules de Δ, $\underline{\Gamma}$ la disjonction des formules de Γ, et x n'est libre ni dans Δ, ni dans Γ.
On veut montrer que $F1$ valide implique $F2$ valide.
Soit donc $F1$ valide, c'est à dire toute interprétation $\mathcal{I}$ est un modèle de $F1$. Soit $\mathcal{I} = \langle D, I \rangle$ un modèle quelconque de $F1$.
On raisonne par contradiction en supposant que $\mathcal{I}$ n'est pas un modèle de $F2$, ce qui implique qu'il existe une valuation τ (adaptée à $F2$) telle que $[F2]_{\mathcal{I},\tau} = F$. Par construction $[\overline{\Delta}]_{\mathcal{I},\tau} = V$, $[\exists x.A]_{\mathcal{I},\tau} = V$ et $[\underline{\Gamma}]_{\mathcal{I},\tau} = F$, et donc en particulier $[A]_{\mathcal{I},\tau[x:=d]} = V$ pour un $d \in D$.
Soit $\sigma = \tau[x := d]$ (adaptée à $F1$). Nous avons $[\overline{\Delta}]_{\mathcal{I},\sigma} = [\overline{\Delta}]_{\mathcal{I},\tau}$ car x n'est pas libre dans Δ, donc $[\overline{\Delta}]_{\mathcal{I},\sigma} = V$. De la même manière $[\underline{\Gamma}]_{\mathcal{I},\sigma} = [\underline{\Gamma}]_{\mathcal{I},\tau} = F$. car x n'est pas libre dans Γ. On obtient ainsi $[\overline{\Delta} \wedge A \to \underline{\Gamma}]_{\mathcal{I},\sigma} = F$, ce qui veut dire que $\mathcal{I}$ n'est pas un modèle de $F1$, et que $F1$ n'est donc pas valide. Contradiction.
On conclut que $F1$ valide implique $F2$ valide.
Correction: (Raisonnement alternatif)

$$\begin{array}{rcl} F1 & = & (\overline{\Delta} \wedge A) \to \underline{\Gamma} \\ F2 & = & (\overline{\Delta} \wedge \exists x.A) \to \underline{\Gamma} \end{array}$$

où $\overline{\Delta}$ dénote la conjonction des formules de Δ, $\underline{\Gamma}$ la disjonction des formules de Γ, et x n'est libre ni dans Δ, ni dans Γ.
On veut montrer que $F1$ valide implique $F2$ valide.
Soit $\mathcal{I} = \langle D, I \rangle$ un modèle de $F1$. On veut montrer que $\mathcal{I}$ est aussi un modèle de $F2$. Soit τ une valuation quelconque adaptée à $F2$. On veut montrer $[F2]_{\mathcal{I},\tau} = V$.
Remarquons que pour tout $d \in D$, la valuation $\sigma = \tau[x := d]$ est adaptée à $F1$. Comme $\mathcal{I}$ est un modèle de $F1$ nous avons que pour tout $d \in D$, $[F1]_{\mathcal{I},\tau[x:=d]} = V$. On raisonne par cas :
- Si il existe d tel que $[\underline{\Gamma}]_{\mathcal{I},\tau[x:=d]} = V$, comme x n'est pas libre dans Γ, alors $[\underline{\Gamma}]_{\mathcal{I},\tau} = [\underline{\Gamma}]_{\mathcal{I},\sigma} = V$. D'où, $[F2]_{\mathcal{I},\tau} = V$
- Sinon, pour tout d, $[\overline{\Delta} \wedge A]_{\mathcal{I},\tau[x:=d]} = F$, alors $[\overline{\Delta} \wedge A]_{\mathcal{I},\tau[x:=d]} = [\overline{\Delta}]_{\mathcal{I},\tau[x:=d]} \cdot [A]_{\mathcal{I},\tau[x:=d]} = F$. On raisonne à nouveau par cas :
  - si il existe d tel que $[\overline{\Delta}]_{\mathcal{I},\tau[x:=d]} = F$, comme x n'est pas libre dans Δ, $[\overline{\Delta}]_{\mathcal{I},\tau} = [\overline{\Delta}]_{\mathcal{I},\tau[x:=d]} = F$.
  - sinon, pour tout d, on a $[A]_{\mathcal{I},\tau[x:=d]} = F$, alors on peut conclure $[\exists x.A]_{\mathcal{I},\tau} = F$.

  Dans les deux cas, $[(\Delta \wedge \exists x.A)]_{\mathcal{I},\tau} = F$ et donc $[F2]_{\mathcal{I},\tau} = V$.

Exercice 2 [TD9, exercice 4 : **(Terminaison)**]
Étant donné un problème d'unification $\mathcal{P}$, on associe à $\mathcal{P}$ le triplet d'entiers décrit comme suit :

$$\mathsf{Comp}(\mathcal{P}) = \langle \textit{nb. de variables non résolues},\ \ \textit{taille du problème},\ \ \textit{nb. d'équations } t \doteq x \rangle$$

où

- *nb. de variables non résolues* désigne le nombre de variables non résolues qui apparaissent dans le problème. Une variable x est résolue dans un problème $\mathcal{P}$ si elle apparaît dans une équation $x \doteq t$ de $\mathcal{P}$ sans apparaître ni dans t ni dans aucune autre équation de $\mathcal{P}$.
- *taille du problème* désigne le nombre d'**occurences** total de variables et de symboles de fonctions qui apparaissent dans le problème (chaque occurrence d'un même symbole compte pour 1).
- *nb. d'équations* $t \doteq s$ désigne le nombre d'équations de la forme $t = s$ où t n'est pas une variable, s pouvant être une variable.

Par exemple, soit le problème $\mathcal{P} = \{x \doteq f(y), h(g(a)) \doteq h(z), z \doteq u\}$, où a, f, g et h sont des symboles de fonctions, alors $\mathsf{Comp}(\mathcal{P}) = (3, 10, 1)$.
(Seule la variable x est résolue, en effet z apparaît dans l'équation $z \doteq u$ mais apparaît aussi dans la deuxième équation, et u est du mauvais côté de la troisième équation, quant à y elle n'est évidemment pas résolue.)

1. Soit le problème $\mathcal{P} = \{f(g(a), h(x,y)) \doteq f(x, h(z, g(b)))\}$. Résolvez-le, et calculez pour chaque étape le triplet Comp correspondant.
2. On considère l'ordre lexicographique sur de tels triplets.
   (a) Montrez que pour toute transformation d'un problème $\mathcal{P}$ en un problème $\mathcal{S}$ différent, on a $\mathsf{Comp}(\mathcal{P}) >_{lex} \mathsf{Comp}(\mathcal{S})$. La preuve se fera par induction sur la longueur de la transformation.
   (b) Concluez-en que l'algorithme d'unification termine.

3. La condition de bord de la règle « orienter » (qui impose que le membre gauche de l'équation à orienter n'est pas une variable) est-elle nécessaire pour assurer la terminaison ? Si oui, donnez un contre-exemple qui sans cette condition ne terminerait pas.
4. Même question pour chacune des deux conditions de bord de la règle « remplacer ».

Correction:

1. La valeur de la fonction Comp est indiquée à droite

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{f(g(a),h(x,y)) \doteq f(x,h(z,g(b))) \qquad (3,12,1)}{g(a) \doteq x, h(x,y)) \doteq h(z,g(b)) \qquad (3,10,2)}\,(d)}{g(a) \doteq x, x \doteq z, y \doteq g(b) \qquad (2,8,1)}\,(d)}{x \doteq g(a), x \doteq z, y \doteq g(b) \qquad (2,8,0)}\,(o)}{x \doteq g(a), g(a) \doteq z, y \doteq g(b) \qquad (1,9,1)}\,(r)$$
$$\dfrac{x \doteq g(a), g(a) \doteq z, y \doteq g(b) \qquad (1,9,1)}{x \doteq g(a), z \doteq g(a), y \doteq g(b) \qquad (0,9,0)}\,(o)$$

2. Il faut prouver que pour toute application d'une seule règle qui fait passer du problème $\mathcal{P}$ au problème $\mathcal{P}'$, la valeur de Comp va diminuer strictement. On note $\mathcal{P} = (v,t,e)$ et $\mathcal{P}' = (v',t',e')$.
   - si la règle est (effacer) : on suppose qu'on efface l'équation $s \doteq s$, alors le nombre de variables non résolues n'a pas changé mais la taille du problème a diminué.
     On a donc $v = v'$ et $t > t'$, ce qui donne $(v,t,e) >_{lex} (v',t',e')$.
   - Si la règle est (orienter) : on suppose qu'on oriente l'équation $t \doteq x$, alors x est éventuellement passé de non-résolue à résolue et donc $v \geqslant v'$. Par ailleurs $t = t'$, mais $e' = e - 1$. On obtient donc $(v,t,e) >_{lex} (v',t',e')$.
   - Si la règle est (décomposer) : on suppose qu'on décompose l'équation $f(s_1,\ldots,s_n) \doteq f(t_1,\ldots,t_n)$. Là encore on a $v \geqslant v'$ (il est possible qu'une ou plusieurs des nouvelles équations soient du type $y_i \doteq t_i$ et que ce y_i n'apparaisse nulle part ailleurs). On a aussi $t' = t - 2$, donc $(v,t,e) >_{lex} (v',t',e')$.
   - Si la règle est (remplacer) : on suppose que l'on remplace avec l'équation $x \doteq s$. On obtient $v > v'$ car x devient résolue. De plus, si une variable y était déjà résolue, l'équation $y \doteq t$ ne contenait pas de x, et donc cette équation restera résolue après substitution, et il n'est pas possible que le s du $x \doteq s$, contienne un y.
     On a donc encore une fois $(v,t,e) >_{lex} (v',t',e')$.

   Après on passe à l'induction (ou on donne la preuve ci-dessus dans l'induction).
3. Les conditions de bord des règles « remplacer » sont toutes nécessaires pour assurer la terminaison. Si on enlève la condition $x \notin VI(s)$, on peut, par exemple, boucler avec l'équation $x \doteq f(x)$ et le problème $\mathcal{P} = \{x \doteq f(x), y \doteq g(x)\}$.
   Si on enlève la condition $x \in Var(\mathcal{P})$, on peut, par exemple, boucler avec l'équation $x \doteq f(y)$ et le problème $\mathcal{P} = \{x \doteq f(y), z \doteq g(t)\}$.
4. La condition de bord de la règle « orienter » est nécessaire également. Sinon, on peut boucler sur le problème $\mathcal{P} = \{x \doteq y\}$.

Exercice 3 [TD10, exercice 4 : (**Résolution**)]

1. Soit $\Sigma_F = \{a/0, f/1\}$ et $\Sigma_P = \{q/1, r/1, p/2, s/2\}$. En utilisant le système de preuve par résolution, montrez que l'ensemble de formules $\{H_1, H_1, H_3\}$ est insatisfaisable, où
   - $H_1 = \exists z.\ (q(f(z)) \wedge s(f(z),a))$
   - $H_2 = \forall x. \forall y. \neg \exists z.\ (p(x,y) \wedge s(x,z))$
   - $H_3 = \forall x.[[q(x) \wedge \exists y.s(x,y)] \rightarrow [\exists y.(r(y) \wedge p(x,y))]]$

   Correction:
   On obtient les clauses suivantes :
   - $C_1 = q(f(b))$

   - $C_2 = s(f(b),a)$
   - $C_3 = \neg p(x,y) \vee \neg s(x,z)$
   - $C_4 = \neg q(x) \vee \neg s(x,y) \vee r(g(x))$
   - $C_5 = \neg q(x) \vee \neg s(x,y) \vee p(x,g(x))$

   Résolution :

$$\dfrac{\dfrac{\dfrac{C_2 \qquad \dfrac{q(f(b)) \qquad C_5}{\neg s(f(b),y) \vee p(f(b),g(f(b)))}\,(x/f(b))}{p(f(b),g(f(b)))}\,(y/a) \qquad C_3}{\neg s(f(b),z)}\,(x/f(b), y/g(f(b))) \qquad s(f(b),a)}{\texttt{False}}\,(z/a)$$

2. Montrer que la formule $F = (\forall x.(p(a) \wedge (p(x) \rightarrow p(f(x))))) \rightarrow \exists x.p(f(f(x)))$ est valide.
   Correction: Il suffit de montrer que sa négation est contradictoire. On a ainsi

$$\begin{aligned} \neg F &\equiv (\forall x.(p(a) \wedge (p(x) \rightarrow p(f(x))))) \wedge \neg(\exists x.\neg p(f(f(x)))) \\ &\equiv (\forall x.(p(a) \wedge (p(x) \rightarrow p(f(x))))) \wedge (\forall y.\neg p(f(f(y)))) \\ &\equiv \forall x.\forall y.[p(a) \ \wedge \ (\neg p(x) \vee p(f(x))) \ \wedge \ \neg p(f(f(y)))] \end{aligned}$$

   Pas besoin de Skolémiser, car il n'y a pas de quantificateur existentiel dans la forme prénexe. L'ensemble de clauses associé à $\neg F$ est $\{p(a), \neg p(x) \vee p(f(x)), \neg p(f(f(y)))\}$.
   Résolution :

$$\dfrac{\dfrac{\dfrac{p(a) \qquad \neg p(x) \vee p(f(x))}{p(f(a))}\,(x/a) \qquad \neg p(x) \vee p(f(x))}{p(f(f(a)))}\,(x/f(a)) \qquad \neg p(f(f(y)))}{\texttt{False}}\,(y/a)$$

   Ce qui montre que l'ensemble de clauses est contradictoire, donc que $\neg F$ est contradictoire, donc F est valide.