Le système de Gentzen pour le calcul des prédicats

Le système $\mathcal{G}$ pour le calcul des prédicats

Axiome : $\Delta; A \vdash \Gamma; A$ (A est une formule du calcul des prédicats)
Règles d'inférence logiques :

$$\frac{\Delta \vdash \Gamma; A}{\Delta; \neg A \vdash \Gamma}\ (\neg\, g) \qquad \frac{\Delta; A \vdash \Gamma}{\Delta \vdash \Gamma; \neg A}\ (\neg\, d)$$

$$\frac{\Delta \vdash A; \Gamma \quad \Delta; B \vdash \Gamma}{\Delta; A \to B \vdash \Gamma}\ (\to\ g) \qquad \frac{\Delta; A \vdash B; \Gamma}{\Delta \vdash A \to B; \Gamma}\ (\to\ d)$$

$$\frac{\Delta; A; B \vdash \Gamma}{\Delta; A \wedge B \vdash \Gamma}\ (\wedge\, g) \qquad \frac{\Delta \vdash A; \Gamma \quad \Delta \vdash B; \Gamma}{\Delta \vdash A \wedge B; \Gamma}\ (\wedge\, d)$$

$$\frac{\Delta; A \vdash \Gamma \quad \Delta; B \vdash \Gamma}{\Delta; A \vee B \vdash \Gamma}\ (\vee g) \qquad \frac{\Delta \vdash A; B; \Gamma}{\Delta \vdash A \vee B; \Gamma}\ (\vee d)$$

Le système $\mathcal{G}$ pour le calcul des prédicats

$$\frac{\Gamma; \{x \leftarrow t\}(A); \forall x{:}A \vdash \Delta}{\Gamma; \forall x{:}A \vdash \Delta}\ (\forall\, g) \qquad \frac{\Gamma \vdash A; \Delta}{\Gamma \vdash \forall x{:}A; \Delta}\ (\forall\, d)$$

$$\frac{\Gamma; A \vdash \Delta}{\Gamma; \exists x{:}A \vdash \Delta}\ (\exists\, g) \qquad \frac{\Gamma \vdash \{x \leftarrow t\}(A); \exists x{:}A; \Delta}{\Gamma \vdash \exists x{:}A; \Delta}\ (\exists\, d)$$

Dans les règles $(\forall\, d)$ et $(\exists\, g)$ x n'est pas libre dans $\Gamma; \Delta$.
Dans les règles $(\forall\, g)$ et $(\exists\, d)$ l'opération $\{x \leftarrow t\}(A)$ ne capture pas des variables (aucune variable de t devient liée)

Dérivation dans $\mathcal{G}$

On note $\Delta \vdash_{\mathcal{G}} \Gamma$ si le séquent $\Delta \vdash \Gamma$ est dérivable dans le système $\mathcal{G}$.

Premier exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(x) \vdash p(x); \exists y \neg p(y)}{\vdash p(x); \neg p(x); \exists y \neg p(y)}}{\vdash p(x); \exists y \neg p(y)}}{\vdash \forall x{:}p(x); \exists y \neg p(y)}}{\vdash (\forall x{:}p(x)) \vee (\exists y \neg p(y))}$$

Deuxième exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{p(a) \vdash p(a); \exists x{:}p(x)}{p(a) \vdash \exists x{:}p(x)} \quad \dfrac{p(b) \vdash p(b); \exists x{:}p(x)}{p(b) \vdash \exists x{:}p(x)}}{p(a) \vee p(b) \vdash \exists x{:}p(x)}$$

Troisième exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p \vdash p; \exists z{:}q(z) \quad \dfrac{p; q(x) \vdash q(x); \exists z{:}q(z)}{p; q(x) \vdash \exists z{:}q(z)}}{p \to q(x); p \vdash \exists z{:}q(z)}}{p \to q(x) \vdash p \to \exists z{:}q(z)}}{\exists x{:}(p \to q(x)) \vdash p \to \exists z{:}q(z)}}{\vdash \exists x{:}(p \to q(x)) \to (p \to \exists z{:}q(z))}$$

Quatrième exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(a); p(f(a)) \vdash p(f(a)); p(f(f(a))); \exists x{:}(p(x) \to p(f(x))}{p(a) \vdash p(f(a)); p(f(a)) \to p(f(f(a))); \exists x{:}(p(x) \to p(f(x))}}{p(a) \vdash p(f(a)); \exists x{:}(p(x) \to p(f(x))}}{\vdash p(a) \to p(f(a)); \exists x{:}(p(x) \to p(f(x)))}}{\vdash \exists x{:}(p(x) \to p(f(x)))}$$

Cinquième exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(x); p(y) \vdash p(y); p(y'); \exists x{:}\forall y{:}(p(x) \to p(y))}{p(x) \vdash p(y); p(y) \to p(y'); \exists x{:}\forall y{:}(p(x) \to p(y))}}{p(x) \vdash p(y); \forall y'{:}(p(y) \to p(y')); \exists x{:}\forall y{:}(p(x) \to p(y))}}{p(x) \vdash p(y); \exists x{:}\forall y{:}(p(x) \to p(y))}}{\vdash p(x) \to p(y); \exists x{:}\forall y{:}(p(x) \to p(y))}}{\vdash \forall y{:}(p(x) \to p(y)); \exists x{:}\forall y{:}(p(x) \to p(y))}}{\vdash \exists x{:}\forall y{:}(p(x) \to p(y))}$$

Sixième exemple de dérivation dans $\mathcal{G}$

Soit $A = \exists x\ \neg(\neg p(x) \wedge \neg Q(x))$, $B = \forall x\ p(x)$ et $C = \forall x\ Q(x)$.

$$\dfrac{\dfrac{\dfrac{p(y); B; \neg q(y) \vdash p(y); A}{p(y); B; \neg p(y); \neg q(y) \vdash A}}{\forall x\ p(x); \neg p(y); \neg q(y) \vdash A} \qquad \dfrac{\dfrac{q(y); C; \neg p(y) \vdash q(y); A}{q(y); C; \neg p(y); \neg q(y) \vdash A}}{\forall x\ q(x); \neg p(y); \neg q(y) \vdash A}}{\dfrac{\dfrac{\dfrac{\forall x\ p(x) \vee \forall x\ q(x); \neg p(y); \neg q(y) \vdash A}{\forall x\ p(x) \vee \forall x\ q(x); \neg p(y) \wedge \neg q(y) \vdash A}}{\forall x\ p(x) \vee \forall x\ q(x) \vdash \neg(\neg p(y) \wedge \neg q(y)); A}}{\forall x\ p(x) \vee \forall x\ q(x) \vdash \exists x\ \neg(\neg p(x) \wedge \neg q(x))}}$$

Remarques

- Retarder au maximum le choix des témoins (règles $\forall\ g$ et $\exists\ d$).
- Renommer des variables (si nécessaire) pour éviter la capture de variables.

Comment transformer quelques dérivations dans $\mathcal{G}$

Théorème : (Affaiblissement) Si $\Delta \vdash \Gamma$ est dérivable dans le système $\mathcal{G}$, alors $\Delta; A \vdash \Gamma$ et $\Delta \vdash A; \Gamma$ le sont aussi.

Théorème : (Contraction) Si $\Delta; A; A \vdash \Gamma$ est dérivable dans le système $\mathcal{G}$, alors $\Delta; A \vdash \Gamma$ l'est aussi. Si $\Delta \vdash \Gamma; A; A$ est dérivable dans le système $\mathcal{G}$, alors $\Delta \vdash \Gamma; A$ l'est aussi.

Rappel

Définition : Un séquent $A_1;:::;A_n \vdash B_1;:::;B_m$ est valide ssi sa formule associée $(A_1 \wedge ::: \wedge A_n) \rightarrow (B_1 \vee ::: \vee B_m)$ est valide.

Propriétés du système $\mathcal{G}$ pour le calcul des prédicats

Théorème : Le système $\mathcal{G}$ est correct, i.e., si $\Delta \vdash_{\mathcal{G}} \Gamma$, alors $\Delta \vdash \Gamma$ est valide.

Théorème : Le système $\mathcal{G}$ est complet, i.e., si $\Delta \vdash \Gamma$ est valide, alors $\Delta \vdash_{\mathcal{G}} \Gamma$.

La théorie de l'unification

Retour sur la notion de substitution

Définition :

- Une substitution est une fonction $: \mathcal{X} \rightarrow \mathcal{T}_{\Sigma,\mathcal{X}}$.
- Le domaine d'une substitution est l'ensemble $Dom( ) = \{x \in \mathcal{X} \mid (x) \neq x\}$.
- Le codomaine d'une substitution est l'ensemble $Codom( ) = \{Vl((x)) \mid x \in Dom( )\}$.
- Un renommage est une substitution injective t.q. $(x) = y$ $\forall x \in Dom( )$.
- Si le domaine d'une substitution est fini on note $= \{x_1 \leftarrow t_1;:::;x_n \leftarrow t_n\}$ si $(x_i) = t_i$ et $x_i \in Dom( )$.
- L'application d'une substitution à un terme est l'extension de aux termes donnée par $(f(t_1;:::;t_n)) = f((t_1);:::; (t_n))$.

Composition de deux substitutions

Soient et deux substitution. La composition de avec est donnée par
 ∘ $(x) =$ ((x)).

Exemple : Soit $= \{x \leftarrow f(y); w \leftarrow g(z; z)\}$ et
 $= \{y \leftarrow f(a); z \leftarrow g(x; b)\}$. La substitution ∘ est donnée par
$\{x \leftarrow f(f(a)); y \leftarrow f(a); w \leftarrow g(g(x; b); g(x; b)); z \leftarrow g(x; b)\}$ et la
substitution ∘ est donnée par
$\{y \leftarrow f(a); z \leftarrow g(f(y); b); x \leftarrow f(y); w \leftarrow g(z; z)\}$.

Comparer deux substitutions

La substitution est une instance de la substitution (ou est plus
générale que), ce que l'on écrit ≤ , ss'il existe une substitution t.q.
pour toute variable $x \in \mathcal{X}$, $(x) = ($ ∘ $)(x)$.

Exemple : $\{x \leftarrow f(y); y \leftarrow z\}$ est plus générale que
$\{x \leftarrow f(b); y \leftarrow h(c); z \leftarrow h(c)\}$

Identifier deux substitutions

Remarque : La relation ≤ n'est pas antisymétrique.

Exemple : Soient $_1 = \{x \leftarrow y\}$ et $_2 = \{y \leftarrow x\}$. On a $_1 \leq _2$ et
$_2 \leq _1$ et $_1 \neq _2$.

Lemme : La relation d'équivalence engendrée par ≤ est donnée par :
 ∼ ′ ssi ∃ un renommage t.q. = ∘ ′.

Alors, $_1 \sim _2$ dans l'exemple précédent car :
$_1 =$ $_1 \circ$ $_2$ et $_2 =$ $_2 \circ$ $_1$.

Substitution(s) principale(s)

Soit $\mathcal{S}$ en ensemble de substitutions et $\in \mathcal{S}$. On dit que est principale
ssi toute substitution $\in \mathcal{S}$ est une instance de .

Exemple : Soit $\mathcal{S} = \{$ $_1$; $_2$; $_3$; $_4$; $_5\}$, où $_1 = \{x \leftarrow y\}$, $_2 = \{y \leftarrow x\}$,
$_3 = \{x \leftarrow y; z \leftarrow x\}$, $_4 = \{x \leftarrow z; y \leftarrow z\}$ et $_5 = \{x \leftarrow a; y \leftarrow a\}$.

Alors $_1$, $_2$ et $_3$ sont principales pour $\mathcal{S}$. En effet,
$_2$; $_3$; $_4$; $_5 \leq _1$ et $_1$; $_3$; $_4$; $_5 \leq _2$ et $_1$; $_2$; $_4$; $_5 \leq _3$
Mais $_1 \not\leq _4$ car $_1 \neq \{x \leftarrow y; z \leftarrow y\} = \{z \leftarrow y\} \circ _4$. De même,
$_1 \not\leq _5$ (entre autres).

Unification comme solution d'un système d'équations

Une équation est une paire de termes de la forme $s \doteq t$, elle est unifiable ssi il existe une substitution σ t.q. $\sigma(s) = \sigma(t)$. Cette substitution est un unificateur ou une solution de l'équation $s \doteq t$.

Un système fini ou problème fini d'équations $\mathcal{P}$ est un ensemble $\{s_1 \doteq t_1; \ldots; s_n \doteq t_n\}$ d'équations, il est unifiable ssi il existe une substitution qui est unificateur de toutes les équations de $\mathcal{P}$. Cette substitution est un unificateur ou une solution de l'ensemble $\mathcal{P}$.

Notations

Définition :

- L'ensemble de variables de $\mathcal{P}$ est notée $Var(\mathcal{P})$.
- L'application d'une substitution σ à $\mathcal{P} = \{s_1 \doteq t_1; \ldots; s_n \doteq t_n\}$ donne le système $\sigma(\mathcal{P}) = \{\sigma(s_1) \doteq \sigma(t_1); \ldots; \sigma(s_n) \doteq \sigma(t_n)\}$.

L'unicité

1. On identifie deux unificateurs σ et σ' d'un problème $\mathcal{P}$ s'ils ne différent que par des renommage de variables, c'est à dire, si $\sigma \sim \sigma'$.
2. On considère uniquement comme unificateurs de $\mathcal{P}$ les substitutions t.q. $Dom(\sigma) \subseteq Var(\mathcal{P})$.

Exemple : Soit $\mathcal{S} = \{x \doteq y\}$. Prenons trois unificateurs principaux de $\mathcal{S}$: $\sigma_1 = \{x \leftarrow y\}$, $\sigma_2 = \{y \leftarrow x\}$ et $\sigma_3 = \{x \leftarrow y; z \leftarrow w\}$.
Alors $\sigma_1 = \sigma_2$ (car $[\sigma_1]_\sim = [\sigma_2]_\sim$) et σ_3 n'est plus considéré comme un unificateur de $\mathcal{S}$.

L'unicité

Module ces considérations, l'unificateur pricipal d'un problème $\mathcal{P}$ est unique modulo renommage, c'est à dire :
Si σ et σ' sont deux unificateurs principaux de $\mathcal{P}$, alors $\sigma \sim \sigma'$.

Les formes résolues

Définition : Un problème d'unification $\mathcal{P}$ est en forme résolue ssi il est de la forme $\{x_1 \doteq t_1; \ldots; x_n \doteq t_n\}$, où

1. toutes les variables x_i sont distinctes ($i \neq j$ implique $x_i \neq x_j$)
2. aucune x_i n'apparaît dans un t_j ($\forall i\ \forall j\ x_i \in VI(t_j)$)

Notation : Si $\mathcal{P}$ est un système en forme résolue $\{x_1 \doteq t_1; \ldots; x_n \doteq t_n\}$ on note $\mathcal{P}$ la substitution $\{x_1 \leftarrow t_1; \ldots; x_n \leftarrow t_n\}$.

Les règles de transformation

$$\frac{\mathcal{P} \cup \{s \doteq s\}}{\mathcal{P}} \quad \text{(effacer)} \qquad \frac{\mathcal{P} \cup \{t \doteq x\} \quad t \in \mathcal{X}}{\mathcal{P} \cup \{x \doteq t\}} \quad \text{(orienter)}$$

$$\frac{\mathcal{P} \cup \{f(s_1; \ldots; s_n) \doteq f(t_1; \ldots; t_n)\}}{\mathcal{P} \cup \{s_1 \doteq t_1; \ldots; s_n \doteq t_n\}} \quad \text{(décomposer)}$$

$$\frac{\mathcal{P} \cup \{x \doteq s\} \quad x \in Var(\mathcal{P}) \quad x \in VI(s)}{\{x \leftarrow s\}(\mathcal{P}) \cup \{x \doteq s\}} \quad \text{(remplacer)}$$

Algorithme d'unification d'un problème $\mathcal{P}$

1. On démarre avec un problème $\mathcal{P}$
2. On applique les règles de transformation tant qu'on peut, on obtient un problème $\mathcal{S}$
3. Si le problème $\mathcal{S}$ est en forme résolue
   - alors renvoyer $\mathcal{S}$
   - sinon échec

Exemple

Soit $\mathcal{P} = \{f(x; h(b); c) \doteq f(g(y); y; c)\}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{f(x; h(b); c) \doteq f(g(y); y; c)}{x \doteq g(y); h(b) \doteq y; c \doteq c}\,\text{d}}{x \doteq g(y); h(b) \doteq y}\,\text{e}}{x \doteq g(y); y \doteq h(b)}\,\text{o}}{x \doteq g(h(b)); y \doteq h(b)}\,\text{r}$$

L'unificateur principal de P est $= \{x \leftarrow g(h(b)\ \ g(y){=}g)$ $[(=)]$

Vers la correction et la complétude de l'algorithme

Lemme :

1. L'algorithme termine.
2. Si est un unificateur d'un problème $\mathcal{P} = \{x_1 \doteq t_1; \ldots; x_n \doteq t_n\}$, alors $= \circ \mathcal{P}$.
3. Si une règle transforme un problème $\mathcal{P}$ dans un problème $\mathcal{S}$, alors les unificateur de $\mathcal{P}$ et $\mathcal{S}$ sont les mêmes.
4. Si $\mathcal{P}$ est en forme résolue, alors $\mathcal{P}$ est solution du problème $\mathcal{P}$.

Correction et complétude de l'algorithme

Théorème : (Correction) Si l'algorithme trouve une substitution $\mathfrak{S}$ pour le problème P, alors P est unifiable et $\mathfrak{S}$ est un unificateur principal de P.
Autrement dit,
Si P n'est pas unifiable, l'algorithme échoue.

Théorème : (Complétude) Si le système P est unifiable, alors l'algorithme calcule l'unificateur principal de P.
Autrement dit,
Si l'algorithme échoue, alors le système P n'est pas unifiable.