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 :

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

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

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

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

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 Γ, Δ.
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 $\mathcal{G}$

$$\dfrac{\dfrac{\dfrac{\dfrac{p(x) \vdash p(x), \exists y \neg p(y)}{\vdash p(x), \neg p(x), \exists y \neg p(y)}}{\vdash p(x), \exists y \neg p(y)}}{\vdash \forall x.p(x), \exists y \neg p(y)}}{\vdash (\forall x.p(x)) \vee (\exists y \neg p(y))}$$

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

$$\dfrac{\dfrac{p(a) \vdash p(a), \exists x.p(x)}{p(a) \vdash \exists x.p(x)} \qquad \dfrac{p(b) \vdash p(b), \exists x.p(x)}{p(b) \vdash \exists x.p(x)}}{p(a) \vee p(b) \vdash \exists x.p(x)}$$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{p \vdash p, \exists z.q(z) \qquad \dfrac{p, q(x) \vdash q(x), \exists z.q(z)}{p, q(x) \vdash \exists z.q(z)}}{p \to q(x), p \vdash \exists z.q(z)}}{p \to q(x) \vdash p \to \exists z.q(z)}}{\exists x.(p \to q(x)) \vdash p \to \exists z.q(z)}}{\vdash \exists x.(p \to q(x)) \to (p \to \exists z.q(z))}$$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{p(a), p(f(a)) \vdash p(f(a)), p(f(f(a))), \exists x.(p(x) \to p(f(x))}{p(a) \vdash p(f(a)), p(f(a)) \to p(f(f(a))), \exists x.(p(x) \to p(f(x))}}{p(a) \vdash p(f(a)), \exists x.(p(x) \to p(f(x))}}{\vdash p(a) \to p(f(a)), \exists x.(p(x) \to p(f(x)))}}{\vdash \exists x.(p(x) \to p(f(x)))}$$

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

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(x), p(y) \vdash p(y), p(y'), \exists x.\forall y.(p(x) \to p(y))}{p(x) \vdash p(y), p(y) \to p(y'), \exists x.\forall y.(p(x) \to p(y))}}{p(x) \vdash p(y), \forall y'.(p(y) \to p(y')), \exists x.\forall y.(p(x) \to p(y))}}{p(x) \vdash p(y), \exists x.\forall y.(p(x) \to p(y))}}{\vdash p(x) \to p(y), \exists x.\forall y.(p(x) \to p(y))}}{\vdash \forall y.(p(x) \to p(y)), \exists x.\forall y.(p(x) \to p(y))}}{\vdash \exists x.\forall y.(p(x) \to p(y))}
$$

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 $C = \forall x\ Q(x)$.

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

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 $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ est valide ssi sa formule associée $(A_1 \wedge \ldots \wedge A_n) \to (B_1 \vee \ldots \vee B_m)$ 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 $\sigma : \mathcal{X} \to \mathcal{T}_{\Sigma,\mathcal{X}}$.
- Le domaine d'une substitution σ est l'ensemble $Dom(\sigma) = \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$.
- Le codomaine d'une substitution σ est l'ensemble $Codom(\sigma) = \{Vl(\sigma(x)) \mid x \in Dom(\sigma)\}$.
- Un renommage est une substitution injective σ t.q. $\sigma(x) = y$ $\forall x \in Dom(\sigma)$.
- Si le domaine d'une substitution σ est fini on note $\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$ si $\sigma(x_i) = t_i$ et $x_i \in Dom(\sigma)$.
- L'application d'une substitution à un terme est l'extension de σ aux termes donnée par $\sigma(f(t_1, \ldots, t_n)) = f(\sigma(t_1), \ldots, \sigma(t_n))$.

Composition de deux substitutions

Soient σ et τ deux substitution. La composition de σ avec τ est donnée par $\sigma \circ \tau(x) = \sigma(\tau(x))$.

Exemple : Soit $\sigma = \{x \leftarrow f(y), w \leftarrow g(z,z)\}$ et $\tau = \{y \leftarrow f(a), z \leftarrow g(x,b)\}$. La substitution $\tau \circ \sigma$ 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 $\sigma \circ \tau$ 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 σ est une instance de la substitution τ (ou τ est plus générale que σ), ce que l'on écrit $\sigma \leq \tau$, ss'il existe une substitution ρ t.q. pour toute variable $x \in \mathcal{X}$, $\sigma(x) = (\rho \circ \tau)(x)$.

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 $\leq$ n'est pas antisymétrique.

Exemple : Soient $\sigma_1 = \{x \leftarrow y\}$ et $\sigma_2 = \{y \leftarrow x\}$. On a $\sigma_1 \leq \sigma_2$ et $\sigma_2 \leq \sigma_1$ et $\sigma_1 \neq \sigma_2$.

Lemme : La relation d'équivalence engendrée par $\leq$ est donnée par : $\sigma \sim \sigma'$ ssi $\exists$ un renommage ρ t.q. $\sigma = \rho \circ \sigma'$.

Alors, $\sigma_1 \sim \sigma_2$ dans l'exemple précédent car : $\sigma_1 = \sigma_1 \circ \sigma_2$ et $\sigma_2 = \sigma_2 \circ \sigma_1$.

Substitution(s) principale(s)

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

Exemple : Soit $\mathcal{S} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, où $\sigma_1 = \{x \leftarrow y\}$, $\sigma_2 = \{y \leftarrow x\}$, $\sigma_3 = \{x \leftarrow y, z \leftarrow x\}$, $\sigma_4 = \{x \leftarrow z, y \leftarrow z\}$ et $\sigma_5 = \{x \leftarrow a, y \leftarrow a\}$.

Alors σ_1, σ_2 et σ_3 sont principales pour $\mathcal{S}$. En effet,
$\sigma_2, \sigma_3, \sigma_4, \sigma_5 \leq \sigma_1$ et $\sigma_1, \sigma_3, \sigma_4, \sigma_5 \leq \sigma_2$ et $\sigma_1, \sigma_2, \sigma_4, \sigma_5 \leq \sigma_3$
Mais $\sigma_1 \not\leq \sigma_4$ car $\sigma_1 \neq \{x \leftarrow y, z \leftarrow y\} = \{z \leftarrow y\} \circ \sigma_4$. De même, $\sigma_1 \not\leq \sigma_5$ (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 σ 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 ($\forall i\ \forall j\ x_i \notin Vl(t_j)$)

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

Les règles de transformation

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

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

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

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 $\vec{\mathcal{S}}$
   - sinon échec

Exemple

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

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

L'unificateur principal de P est $\sigma = \{x \leftarrow g(h(b)), y \leftarrow h(b)\}$.
Ainsi, $\sigma f(x, h(b), c) = f(g(h(b)), h(b), c) = \sigma f(g(y), y, c)$.

Vers la correction et la complétude de l'algorithme

Lemme :

1. L'algorithme termine.
2. Si σ est un unificateur d'un problème $\mathcal{P} = \{x_1 \doteq t_1, \ldots, x_n \doteq t_n\}$, alors $\sigma = \sigma \circ \vec{\mathcal{P}}$.
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 $\vec{\mathcal{P}}$ est solution du problème $\mathcal{P}$.

Correction et complétude de l'algorithme

Théorème : (Correction) Si l'algorithme trouve une substitution $\vec{S}$ pour le problème P, alors P est unifiable et $\vec{S}$ 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.