

1 Définitions

- Les **règles d'inférence** permettent de définir la plus petite relation (rappel : il faut voir une relation comme une partie de l'espace produit) qui vérifie un certain nombre de règles précises. Une règle d'inférence se note $\frac{t_1 \in R \dots t_n \in R}{t \in R}$ avec les hypothèses au numérateur et la conclusion au dénominateur.

- Les **expressions** sont construites à partir de **symboles primitifs** et éventuellement de **variables**.

- Pour définir les expressions correctes (on dira aussi terme), on part de symboles et de contraintes sur ces symboles.

- \mathcal{S} ensemble fini de symboles (appelés **sortes**) qui permettent de classer les expressions (syntaxiquement).
- \mathcal{F} ensemble (fini ou infini) de symboles primitifs, chaque symbole est associé à une **arité** de la forme $\langle s_1, \dots, s_n, s \rangle$ avec $n \in \mathbb{N}$ (le nombre d'arguments du symbole) et $s_i, s \in \mathcal{S}$. La sorte s résultat, représente la sorte de l'objet qui est construit par le symbole. L'ensemble \mathcal{F} s'appelle la **signature** du langage.
- \mathcal{X} ensemble infini de **variables**, à chaque variable est associée une sorte. On notera \mathcal{X}_s l'ensemble des variables de sorte s .

- Au lieu de définir un ensemble particulier pour les propositions, on peut les traiter comme un cas particulier d'expression. On ajoute une sorte spécifique PROP, et on ajoute des symboles pour les opérateurs logiques :

- \perp (absurde, faux), \top (tautologie, vrai) ont pour arité $\langle \text{PROP} \rangle$
- \neg (négation, non) a pour arité $\langle \text{PROP}, \text{PROP} \rangle$
- \wedge (conjonction, et), \Rightarrow (implication, si/alors), \vee (disjonction, ou) ont pour arité $\langle \text{PROP}, \text{PROP}, \text{PROP} \rangle$

2 Règles de la déduction naturelle

Hyp	$\overline{\Gamma \vdash A} (A \in \Gamma)$	
	Introduction	Élimination
\top	$\overline{\Gamma \vdash \top}$	
\perp		$\frac{\Gamma, \{\neg C\} \vdash \perp}{\Gamma \vdash C}$
\wedge	$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$	$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$
\vee	$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$	$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$
\neg	$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A}$	$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash C}$
\Rightarrow	$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$
\forall	$\frac{\Gamma \vdash P}{\Gamma \vdash \forall x, P} (x \notin V_l(\Gamma))$	$\frac{\Gamma \vdash \forall x, P}{\Gamma \vdash P[x \leftarrow t]}$
\exists	$\frac{\Gamma \vdash P[x \leftarrow t]}{\Gamma \vdash \exists x, P}$	$\frac{\Gamma \vdash \exists x, P \quad \Gamma, P \vdash C}{\Gamma \vdash C} (x \notin V_l(\Gamma, C))$

3 Logique dans une théorie

- Une **théorie** est définie par un ensemble de symboles de fonctions et de prédicats (la **signature** de la théorie) et un ensemble de formules closes (sans variables libres) construites sur ce langage, appelés les **axiomes** de la théorie. Formules prouvables dans une théorie \mathcal{A} : $\Gamma \vdash_{\mathcal{A}} A$ ou $\Gamma, \mathcal{A} \vdash A$.
Ajout de la règle Axiome : $\frac{}{\Gamma \vdash_{\mathcal{A}} A} (A \in \mathcal{A})$

- Une théorie est **récursive** s'il existe un algorithme qui étant donné une formule P détermine si $P \in \mathcal{A}$

- Une théorie est **contradictoire** si elle vérifie l'une des trois propriétés équivalentes suivantes :

- Il existe une formule A telle que $\mathcal{A} \vdash A$ et $\mathcal{A} \vdash \neg A$.
- Il existe une preuve de l'absurde : $\mathcal{A} \vdash \perp$.
- Toutes les propositions sont démontrables : $\mathcal{A} \vdash A$.

Une théorie qui n'est pas contradictoire est dite **cohérente**.

- Une théorie est **décidable** s'il existe un algorithme qui étant donné une formule P détermine si P est démontrable dans la théorie ou non.

- Une théorie est **complète** si pour toute formule P , P ou $\neg P$ est démontrable dans la théorie.

4 Théorie de l'égalité

- On considère un symbole binaire quelconque, noté $=$ de manière infixé, qui :

- est réflexif, symétrique, transitif (relation d'équivalence)
- Vérifie la congruence/symboles de fonction f (d'arité n quelconque) :
 $\forall x_1, \dots, x_n y_1 \dots y_n (x_1 = y_1 \wedge \dots \wedge x_n = y_n) \Rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$
- Vérifie la congruence/symboles de prédicat P (d'arité n quelconque) :
 $\forall x_1, \dots, x_n y_1 \dots y_n (x_1 = y_1 \wedge \dots \wedge x_n = y_n) \Rightarrow P(x_1, \dots, x_n) = P(y_1, \dots, y_n)$

5 Théorie arithmétique de Peano

- On se munit d'un symbole 0 , d'une opération unaire de successeur S , d'un prédicat d'égalité, et des axiomes suivants :

- Axiomes pour l'infini : $\begin{cases} \forall x, S(x) \neq 0 \\ \forall x, y S(x) = S(y) \Rightarrow x = y \end{cases}$
- Pas d'autres objets que ceux construits par 0 et S : $\forall x, x = 0 \vee \exists y, x = S(y)$
- Schéma d'axiome de récurrence (pour chaque formule Φ) :
 $\forall x_1, \dots, x_n \Phi[x \leftarrow 0] \Rightarrow (\forall x, \Phi \Rightarrow \Phi[x \leftarrow S(x)]) \Rightarrow \forall x, \Phi$
- Axiome de minimalité (dans une sur-théorie/théorie des classes) :
 $\forall_{\kappa} C, 0 \in C \Rightarrow (\forall x, (x \in C \Rightarrow S(x) \in C) \Rightarrow \forall x, x \in C$

- On se munit des opérations binaires usuelles $+$ et \times , définies par :

- $\forall x, x + 0 = x$
- $\forall x, y, x + S(y) = S(x + y)$
- $\forall x, x \times 0 = 0$
- $\forall x, y, x \times S(y) = (x \times y) + x$

6 Interprétation et environnement

- On se munit des **booléens** $\mathbb{B} = \{V, F\}$

- On parle de **sémantique** (sens de la formule) par opposition à la **syntaxe** (forme). On ne connaît la vérité d'une formule qu'après avoir défini l'interprétation des symboles (sémantique).

- Si on connaît les formules atomiques vraies alors la logique nous dit si une **formule propositionnelle** est vraie ou fausse.

- On note \mathcal{R} l'ensemble des symboles de prédicats (= fonction dont l'arité est $\langle \dots, \text{PROP} \rangle$)

- Une **interprétation** I de la signature $(\mathcal{S}, \mathcal{F}, \mathcal{R})$ est donnée par :

- Pour chaque sorte s , un ensemble \mathcal{D}_s non vide, appelé **domaine** d'interprétation (de la sorte s).
- Pour chaque symbole de fonction f d'arité $\langle s_1, \dots, s_n, s \rangle$, une fonction $f_I \in \mathcal{D}_{s_1} \times \dots \times \mathcal{D}_{s_n} \rightarrow \mathcal{D}_s$
- Pour chaque symbole de prédicat R d'arité $\langle s_1, \dots, s_n, \text{PROP} \rangle$, une relation $R_I \subseteq \mathcal{D}_{s_1} \times \dots \times \mathcal{D}_{s_n}$

On parlera aussi de **modèle** ou de **structure**.

- Un **environnement** (ou **valuation**) est une application ρ qui associe un élément de \mathcal{D}_s à chaque variable de \mathcal{X} de sorte s .

On note $\mathcal{D} := \bigcup_{s \in \mathcal{S}} \mathcal{D}_s$, et on a $\rho \in \mathcal{X} \rightarrow \mathcal{D}$. On note $\rho + \{x \rightarrow d\}$ l'environnement qui vaut d pour la variable x , et $\rho(y)$ pour toute autre variable y .

- Le **domaine de Herbrand** d'un langage logique de signature \mathcal{F} est donné pour chaque sorte s par l'ensemble $\mathcal{T}(\mathcal{F}, s)$ des termes clos de sorte s formés à partir des symboles de \mathcal{F} .

Si il n'y a pas de constante dans la signature (i.e de termes d'arité 1), alors cet ensemble est vide. Dans la suite, on suppose donc que \mathcal{F} contient au moins une constante de chaque sorte s .

- Une **interprétation de Herbrand** est une interprétation H construite sur le domaine $\mathcal{T}(\mathcal{F}, s)$ dans laquelle chaque symbole de fonction f , d'arité $\langle s_1, \dots, s_n, s \rangle$ est interprété par une fonction f_H définie par : $f_H(t_1, \dots, t_n) := f(t_1, \dots, t_n)$, avec $t_i \in \mathcal{T}(\mathcal{F}, s_i)$.

- La **base de Herbrand** est l'ensemble des formules atomiques closes construites sur le langage.

- Un **modèle de Herbrand** est défini en assignant des valeurs de vérité à chacune des formules de la base de Herbrand (i.e à chaque formule atomique close).

Exemples : On se donne a et b des constantes, f un symbole de fonction.

- Pour la formule : $\forall x, y \ R(x, a) \wedge \neg R(b, y)$, on a $\begin{cases} D_H = \{a, b\} \\ B_H = \{R(a, a), R(a, b), R(b, a), R(b, b)\} \end{cases}$
- Pour la formule : $\forall x, y \ R(x, a) \Rightarrow R(y, f(y))$, on a $\begin{cases} D_H = \{a, f(a), f^2(a), \dots\} \\ B_H = \{R(a, a), R(a, f(a)), R(f(a), a), R(f(a), f(a)), \dots\} \end{cases}$
- Soit $\rho \in \mathcal{X} \rightarrow \mathcal{D}$ un environnement.

On définit $\text{val}_I(\rho, t)$ la **valeur d'un terme** $t \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ de sorte s dans l'interprétation I et l'environnement ρ . C'est un élément du domaine \mathcal{D}_s :

$$\text{val}_I(\rho, x) := \rho(x) \quad ; \quad \text{val}_I(\rho, f(t_1, \dots, t_n)) := f_I(\text{val}_I(\rho, t_1), \dots, \text{val}_I(\rho, t_n))$$

On définit $\text{val}_I(\rho, P)$ la **valeur d'une formule** P dans l'interprétation I et l'environnement ρ :

- $\text{val}_I(\rho, \perp) = F$
- $\text{val}_I(\rho, \top) = V$
- $\text{val}_I(\rho, P[x \leftarrow t]) = \text{val}_I(\rho + \{x \rightarrow \text{val}_I(\rho, t)\}, P)$
- $\text{val}_I(\rho, R(t_1, \dots, t_n)) = \begin{cases} V & \text{si } R_I(\text{val}_I(\rho, t_1), \dots, \text{val}_I(\rho, t_n)) \\ F & \text{sinon} \end{cases}$
- $\text{val}_I(\rho, \neg A) = \begin{cases} V & \text{si } \text{val}_I(\rho, A) = F \\ F & \text{sinon} \end{cases}$
- $\text{val}_I(\rho, A \wedge B) = \begin{cases} \text{val}_I(\rho, B) & \text{si } \text{val}_I(\rho, A) = V \\ F & \text{sinon} \end{cases}$
- $\text{val}_I(\rho, A \Rightarrow B) = \begin{cases} \text{val}_I(\rho, B) & \text{si } \text{val}_I(\rho, A) = V \\ V & \text{sinon} \end{cases}$
- $\text{val}_I(\rho, \forall x \ A) = \begin{cases} V & \text{si } \{\text{val}_I(\rho + \{x \rightarrow d\}, A) \mid d \in \mathcal{D}\} = \{V\} \\ F & \text{sinon} \end{cases}$
- $\text{val}_I(\rho, \exists x \ A) = \begin{cases} V & \text{si } V \in \{\text{val}_I(\rho + \{x \rightarrow d\}, A) \mid d \in \mathcal{D}\} \\ F & \text{sinon} \end{cases}$

On note $I, \rho \models A$ lorsque la formule A est vraie dans l'interprétation I et l'environnement ρ (resp. $I, \rho \not\models A$ lorsque A est fausse). Si A est close, alors sa valeur dans une interprétation ne dépend pas de l'environnement et on écrira simplement $I \models A$.

- Si \mathcal{E} est un ensemble de formules, on note $I, \rho \models \mathcal{E}$ le fait que : $\forall P \in \mathcal{E}, I, \rho \models P$.

Si A est une formule, on dit que A est une **conséquence logique** de \mathcal{E} si pour toute interprétation I et environnement ρ , on a $I, \rho \models \mathcal{E} \Rightarrow I, \rho \models A$.

A et B sont des formules logiques **équivalentes** si l'une est conséquence de l'autre et réciproquement.

7 Correction et complétude

Théorème (Correction) : Soient Γ est un ensemble fini de formules, et P une formule. Si $\Gamma \vdash P$ est prouvable en déduction naturelle, alors $\Gamma \models P$.

Rq : Cela reste trivialement vrai si l'on rajoute des axiomes.

Rq : Si une théorie a un modèle, alors elle est cohérente.

Théorème (Complétude) : Soient une théorie \mathcal{A} , et une formule P . Si P est vraie dans toute interprétation qui rend vraies les formules de \mathcal{A} , alors la formule P admet une preuve en déduction naturelle dans la théorie \mathcal{A} .

Rq : Il s'agit de la réciproque du théorème précédent.

Rq : On déduit à partir d'une remarque précédente que : \mathcal{A} est cohérente $\Leftrightarrow \mathcal{A}$ admet un modèle.

Rq : La preuve de ce dernier théorème repose entièrement sur le fait qu'il y ait un nombre dénombrable de formules atomiques.

- Soit A une formule sur une signature $(\mathcal{S}, \mathcal{F}, \mathcal{R})$. On a les définitions suivantes :

- A est **valide** si pour toute interprétation I et environnement ρ , on a que : $I, \rho \models A$.
On écrit alors $\models A$.
- A est **satisfaisable** si il existe une interprétation I et un environnement ρ tels qu'on ait : $I, \rho \models A$.
Une interprétation et un environnement qui rendent vraie la formule forment un **modèle** de la formule.
- A est **contradictoire** (ou **insatisfaisable**) si pour toute interprétation I et environnement ρ , on a que : $I, \rho \not\models A$.

Ces définitions s'étendent au cas d'un ensemble de formules \mathcal{E} .

Rq : P est valide $\Leftrightarrow \neg P$ est insatisfaisable $\Leftrightarrow \neg P$ n'est pas satisfaisable.

- Une formule est dite en **forme normale de négation** si elle ne contient que les connecteurs logiques \wedge, \vee , les quantificateurs \forall, \exists et que le symbole de négation \neg n'apparaît que devant une formule atomique $R(t_1, \dots, t_n)$.

8 Skolemisation

- Soit A en forme normale de négation dans laquelle apparaît une sous-formule $\exists y, B$. On procède de la manière suivante pour **éliminer le quantificateur existentiel** :

1. Indentification des variables libres de $\exists y, B : \{x_1, \dots, x_n\}$
2. On introduit un nouveau symbole de fonction f à n arguments
3. On remplace la formule $\exists y, B$ par $B[y \leftarrow f(x_1, \dots, x_n)]$

Alors, si on note A' la formule obtenue, on a que $A' \models A$. De plus, tout modèle de A peut être transformé en un modèle de A' qui coïncide avec celui de A , sauf pour l'interprétation du nouveau symbole f .

- Soit A une formule en forme normale de négation, et B une formule obtenue par élimination des quantificateurs existentiels de A . Alors on a que si B est valide (resp. satisfiable) (resp. insatisfiable) alors A l'est aussi.

- Soit A une formule *close*, alors il existe une formule B en forme normale de négation, et sans quantificateurs, telle que si $Vl(B) = \{x_1, \dots, x_n\}$, on a :

- $\forall x_1, \dots, x_n B \models A$
- Si A a un modèle, alors $\forall x_1, \dots, x_n B$ aussi.

Cette transformation s'appelle la **skolémisation**, et $\forall x_1, \dots, x_n B$ est la **forme de Skolem** de A .

Rq : On a ainsi que : A est valide \Leftrightarrow La forme skolémisée de $\neg A$ est insatisfiable.

Rappel : Une formule propositionnelle est sans quantificateurs, un prédicat est une formule quelconque.

9 Compacité et satisfaisabilité

Théorème (Compacité) : Soit \mathcal{E} un ensemble de formules propositionnelles. Si \mathcal{E} est insatisfiable, alors il existe un sous-ensemble fini de \mathcal{E} qui est insatisfiable.

Rq : Ce théorème est aussi valide dans le cas de formule du calcul des prédicats, grâce au théorème de Herbrand.

Rq : La preuve est ridicule, on utilise au moins deux fois l'axiome du choix (dont une fois passée sous silence ...), en gros il faut considérer d'abord le cas dénombrable et se représenter l'hypothèse sous la forme d'un arbre binaire, puis König. Généralisation avec zornette.

- Une formule logique est dite **universelle** si elle est de la forme

$$\forall x_1, \dots, x_n A$$

avec A une formule sans quantificateurs.

Lemme : Une formule universelle close est satisfaisable si et seulement si il existe une interprétation de Herbrand qui rend vraie la formule.

- Si A est une formule dont les variables libres sont $\{x_1, \dots, x_n\}$, alors une formule $A[x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n]$ où $t_1, \dots, t_n \in \mathcal{T}(\mathcal{F})$ est appelée **instance close** de A .

Théorème (Herbrand) : Si $B := \forall x_1, \dots, x_n A$ est une *formule universelle close* avec A sans quantificateurs, alors :

B satisfaisable \Leftrightarrow Tout sous-ensemble fini $\{A_1, \dots, A_p\}$ d'instances closes de A est satisfaisable.

- Si P est une formule logique dont les variables libres sont $\{x_1, \dots, x_n\}$, on note $\forall(P)$ la **fermeture universelle** de P , qui correspond à la formule $\forall x_1, \dots, x_n P$.

Théorème (Lowenheim-Skolem) : Si une théorie \mathcal{A} admet un modèle infini, alors elle a des modèles avec des cardinaux arbitrairement grands.

10 Indécidabilité et incomplétude

Théorème (Indécidabilité de la logique du 1er ordre) : Les problèmes de satisfaisabilité ainsi que de validité d'une formule du calcul des prédicats sont indécidables dans une théorie sans axiomes.

Rq : La preuve consiste à se ramener à un problème indécidable, typiquement Halt ou Post (cf slides).

11 Système G

Définition : Un séquent à conclusions multiples est formé de deux ensembles finis de formules : Γ (les hypothèses), et Δ (les conclusions). On le note $\Gamma \vdash \Delta$.

La formule associée à $P_1, \dots, P_n \vdash Q_1, \dots, Q_n$ est : $(P_1 \wedge \dots \wedge P_n) \Rightarrow (Q_1 \vee \dots \vee Q_n)$.

Rq : Le séquent $\Gamma \vdash \Delta$ est dit **valide** si sa formule associée l'est, i.e : pour toute interprétation I telle que $I \models \Gamma$, il existe $Q \in \Delta$ tel que $I \models Q$.

Rq : Si Δ (resp. Γ) = \emptyset , le membre de droite (resp. gauche) est remplacée par \perp (resp. \top).

- Le système G est composé des règles suivantes :

Hyp	$\overline{A, \Gamma \vdash \Delta, A}$	
Axiome	$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta} \quad (A \in \mathcal{A})$	
	Cas hypothèse	Cas conclusion
\perp	$\overline{\perp, \Gamma \vdash \Delta}$	$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \perp}$
\top	$\frac{\Gamma \vdash \Delta}{\top, \Gamma \vdash \Delta}$	$\overline{\Gamma \vdash \Delta, \top}$
\neg	$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}$	$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}$
\wedge	$\frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}$	$\frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}$
\vee	$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}$	$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$
\Rightarrow	$\frac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{A \Rightarrow B, \Gamma \vdash \Delta}$	$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \Rightarrow B}$

Rq : Le tier exclu est directement déductible du système ci-dessus : $\text{Hyp} \frac{}{P \vdash P}$
 $\neg_d \frac{}{\vdash P, \neg P}$
 $\vee_d \frac{}{\vdash P \vee \neg P}$

Propriété : Toutes les règles du système G sont **correctes** et **inversibles**, i.e une conclusion est vraie ssi toutes les hypothèses qui permettent d'y aboutir sont vraies.

Propriété : Le système G est **complet**

Propriété (Automatisation) : Soit un arbre de dérivation suivant les règles du système G pour un séquent $\Gamma \vdash \Delta$ dont les feuilles ne contiennent plus de connecteurs logiques. Le séquent $\Gamma \vdash \Delta$ est valide (dans la théorie vide) ssi la règle hypothèse s'applique à chacune des feuilles.

Rq : Cela permet d'automatiser les preuves dans le système en G, car chaque séquent en prémisses d'une règle d'inférence contient moins de connecteurs logiques que celui qui est en conclusion, donc il suffit de construire l'arbre de preuve jusqu'à ce qu'aucune règle ne s'applique, et vérifier si toutes les feuilles sont des tautologies.

- On peut de plus rajouter les règles suivantes qui permettent de manipuler les quantificateurs classiques :

	Cas hypothèse	Cas conclusion
\forall	$\frac{P[x \leftarrow t], (\forall x P), \Gamma \vdash \Delta}{(\forall x P), \Gamma \vdash \Delta}$	$\frac{\Gamma \vdash \Delta, P}{\Gamma \vdash \Delta, (\forall x P)} (x \notin \text{Vl}(\Gamma, \Delta))$
\exists	$\frac{P, \Gamma \vdash \Delta}{(\exists x P), \Gamma \vdash \Delta} (x \notin \text{Vl}(\Gamma, \Delta))$	$\frac{\Gamma \vdash (\exists x P), P[x \leftarrow t]}{\Gamma \vdash \Delta, (\exists x P)}$
Contraction	$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$	$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}$

Rq : On peut "oublier" la propriété initiale quand on remonte dans les \forall_g et \exists_d .

- On peut aussi rajouter les règles dérivées suivantes :

- **Affaiblissement** : si $\Gamma \vdash \Delta$ alors $\Gamma, \Gamma' \vdash \Delta, \Delta'$
- **Substitution** : si $\Gamma \vdash \Delta$ alors $\Gamma[x \leftarrow t] \vdash \Delta[x \leftarrow t]$

Définition : Une **substitution** est une application $\sigma \in \mathcal{X} \rightarrow \mathcal{T}(\mathcal{F}, \mathcal{X})$ à support fini, i.e $\sigma(x) = x$ sauf pour un nombre fini de variables.

Rq : On peut donc représenter un substitution par $\{x \leftarrow \sigma(x) \mid x \in \mathcal{X} \wedge \sigma(x) \neq x\}$.

Rq : Une substitution définit une application de $\mathcal{T}(\mathcal{F}, \mathcal{X}) \rightarrow \mathcal{T}(\mathcal{F}, \mathcal{X})$ qui à un terme t associe $t[\sigma]$, dans lequel chaque variable x est remplacée par $\sigma(x)$.

On note $t[\sigma_1 \sigma_2] := (t[\sigma_1])[\sigma_2]$.

Définition : Un problème d'**unification** noté $t \stackrel{?}{=} u$, consiste à chercher σ telle que $t[\sigma] = u[\sigma]$, ou de manière plus générale, pour un ensemble $\{(t_i \stackrel{?}{=} u_i) \mid i \in I\}$ avec $t_i[\sigma] = u_i[\sigma]$.

Définition : Une substitution σ est **plus générale** que τ si il existe σ' telle que $\sigma\sigma' = \tau$.

Rq : Si un problème d'unification a une solution, alors il existe une solution qui est plus générale que toutes les autres, appelée **unificateur principal**.

Algorithme de Robinson : On peut de plus calculer récursivement cet unificateur principal. Pour un problème d'unification $E = \{t_i \stackrel{?}{=} u_i \mid i \in I\}$ donné, on procède de la manière suivante :

1. $\text{unif}(\emptyset) = \{\}$
2. $\text{unif}(\{x \stackrel{?}{=} t\} \cup E) = \text{unif}(E)$
3. $\text{unif}(\{x \stackrel{?}{=} t\} \cup E) = \text{echec}$ $x \in \text{vars}(t), t \neq x$
4. $\text{unif}(\{x \stackrel{?}{=} t\} \cup E) = \{x \leftarrow t\} \text{unif}(E[x \leftarrow t])$ $x \notin \text{vars}(t)$

$$5. \text{unif}(\{t \stackrel{?}{=} x\} \cup E) = \text{unif}(\{x \leftarrow t\} \cup E) \quad t \notin \mathcal{X}$$

$$6. \text{unif}(\{f(t_1, \dots, f_n) \stackrel{?}{=} g(u_1, \dots, u_n)\} \cup E) = \text{echec} \quad f \neq g$$

$$7. \text{unif}(\{f(t_1, \dots, f_n) \stackrel{?}{=} f(u_1, \dots, u_n)\} \cup E) = \text{unif}(\{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\} \cup E)$$

Théorème : Ça marche (si une solution est trouvée, il s'agit bien de l'unificateur principal).

Rq : On peut généraliser à des formules atomiques, en ajoutant les symboles de prédicats à la signature de la théorie.

Rq : Dans le pire cas, l'algo est exponentiel (cf. slides), pour un algo plus efficace, voir la méthode des tableaux (c le projet logique mdr).

12 Transformation de preuves

- On note $\Gamma \vdash_N P$ un séquent prouvable en déduction naturelle, et $\Gamma \vdash_G \Delta$ un séquent (généralisé) prouvable dans le système G. On aimerait relier ces deux systèmes de preuve de la manière suivante :

- Si $\Gamma \vdash_N P$ alors $\Gamma \vdash_G P$
- Si $\Gamma \vdash_G \Delta$ alors $\Gamma, \neg\Delta \vdash_N \perp$

En gros ça se fait avec la règle de coupure mais j'ai pas compris du coup flemme d'écrire la démo.