Règles de déduction

June 2, 2006

Chapter 1

La théorie

1.1 Introduction

1.1.1 Notes préliminaires

Le symbole de l'implication $\Rightarrow$ n'est **plus** défini comme étant la même chose que $\neg A \vee B$. Cette égalité, bien que parfois vraie, peut devenir fausse (cela dépend du cadre logique dans lequel on se place).

Tous les symboles sont donc indépendants. Il y a en outre une proposition spéciale: $\perp$, l'absurdité, la contradiction.

Nous prenons pour convention que l'implication $\Rightarrow$ est associative à droite. C'est à dire qu'on a équivalence stricte entre les propositions $A \Rightarrow (B \Rightarrow C)$ et $A \Rightarrow B \Rightarrow C$,de même, lorsqu'il n'y a pas de parenthèses, $forallxP \vee Q$ est un raccourci pour $(\forall x P) \vee Q$.

1.1.2 Le langage des propositions

Cette section peut être ignorée dans un premier temps. Il est plus utile de s'y référer si l'on a un problème (ou lorsqu'on voudra programmer).

Nous considérons un langage $\mathcal{L}$ formé :

- de symboles de prédicat, notés : $P, Q, R, ...$, d'arité n quelconque (ils ont n arguments).
- de symboles de fonction d'arité n (les constantes sont des symboles de fonction d'arité 0), notés : $a, b, c, ..., f, g, h, ...$

Et un ensemble dénombrable $\mathcal{V}$ de symboles de variables, notés : $x, y, ...$

Enfin, nous avons des symboles de connecteurs, permettant de connecter les propositions entre elles. Trois connecteurs propositionnels :

$$\wedge \quad \vee \quad \Rightarrow$$

d'arité 2 (et sont habituellement respectivement nommés `et`, `ou` et `implique`), et un connecteur propositionnel :

$$\neg$$

d'arité 1 et se nomme `non`.

Il faut ajouter les deux quantificateurs universels et existentiels (`quel que soit`, `il existe`) :

$$\forall \quad \exists$$

que l'on généralise en $\mathcal{Q}$ lorsqu'on veut parler des deux quantificateurs en même temps.

Nous pouvons combiner ces différents éléments ensemble, nous donnons les règles de combinaisons dans les deux définition 1 et 2 ci-dessous. Par exemple si P, Q sont des prédicats à une variable, $+$ un symbole de fonction à deux variables, nous pouvons former la formule $Q \wedge P(+\ 2\ 3)$ mais nous ne pouvons par former $(+P\ Q\ \forall)$ (qui n'est pas un terme bien formé). Pour les fonctions et les prédicats d'arité n, nous représenterons en générale ses arguments entre parenthèses ($P(f(b), a)$ au lieu de $Pfba$), et nous utiliserons une notation infixe pour les connecteurs logiques, quitte à utiliser des parenthèses. Nous noterons $A \vee (B \wedge C)$ au lieu de $\vee A \wedge BC$.

Puisque tous les termes ne sont pas bien formés, voici les définitions de ce que sont un terme bien formé et une formule bien formée:

Définition 1 (Terme bien formé) *Un terme est bien formé si :*

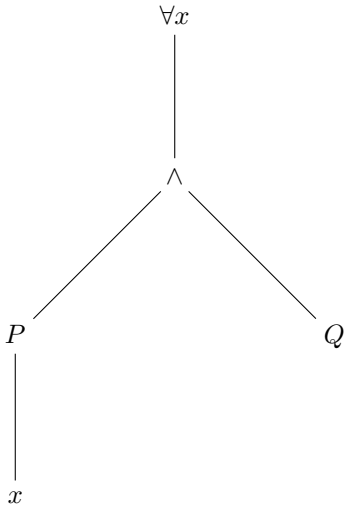
- *c'est une variable,*
- *c'est un symbole de fonction f d'arité n appliqué à n arguments qui sont eux-mêmes des termes bien formés.*

Définition 2 (Formule bien formée) *Une formule est bien formée si :*

- *c'est un symbole de prédicat d'arité n appliqué à n termes bien formés (définition 1),*
- *c'est un connecteur propositionnel d'arité n appliqué à n arguments qui sont eux-même des formules bien formées ($A \vee B$ par ex.),*
- *c'est un quantificateur, suivi d'un symbole de variable, et suivi d'une formule bien formée ($\forall x P$).*

Abus de langage. "proposition" sera souvent utilisé au lieu de "formule bien formée". "atome", "formule atomique" ou "proposition atomique" est une abréviation pour "prédicat d'arité n appliqué à n termes bien formés".

Les deux définitions 1 et 2 définissent formellement un terme (respectivement, une formule) comme un arbre. Par exemple, la proposition $\forall x(P(x) \wedge Q)$ représente en fait l'arbre suivant :



Une variable x est dite libre lorsqu'elle ne dépend d'aucun quantificateur, c'est à dire que dans l'arbre de dérivation de la formule, n'est pas située sous un quantificateur ayant comme argument x.

Si une variable n'est pas libre, on dit qu'elle est liée. Par exemple x est libre dans $\exists y P(x, y)$, mais y y est liée (par le quantificateur $\exists$).

Par exemple, dans la formule :

$$P(x, x) \vee Q(x, y)$$

le symbole de prédicat Q a une occurrence, de même que l'atome $Q(x, y)$. Par contre la variable x en a trois. Nous parlerons de la première occurrence de x, de la deuxième, etc, en fonction de l'ordre d'apparition de x.

Définition 3 (variables libres, liées) *Si x a une occurrence dans P, cette occurrence est dite libre dans P ssi :*

- *P est un atome.*
- *P est une formule du type $\mathcal{Q}yR$ ($\mathcal{Q}$ est un quantificateur), $x \neq y$, et l'occurrence de x est libre dans R.*
- *P est une formule du type QcR, où c est un connecteur propositionnel, et si l'occurrence de x est dans Q, alors celle-ci est libre dans Q (resp. si elle est dans R, alors celle-ci est libre dans R).*

L'occurrence d'une variable qui n'est pas libre est dite liée.

Une formule est close *si et seulement si toutes les occurrences de toutes ses variables sont liées.*

Un terme est clos *si et seulement si il ne comporte pas de variables.*

Une variable z est fraîche *par rapport à une formule ssi elle n'a aucune occurrence (ni libre, ni liée) dans cette formule.*

Une constante c est fraîche *par rapport à une formule ssi elle n'a aucune occurrence dans cette formule.*

Si nous avons une formule du type $P(x) \vee (\forall x Q(x))$, alors la première occurrence de x est libre, mais la seconde est liée. Même si ce genre de formule est bien formé, nous éviterons de les écrire sous cette forme. Il vaudra mieux considérer la formule $P(x) \vee (\forall y Q(y))$. Ces deux formules sont équivalentes, et ce problème est connu sous le nom d'α-équivalence (équivalence alphabétique) en théorie de la démonstration, et sous le nom de variable muette en mathématiques usuelles:

$$\int_1^2 x\,dx \quad \text{est la même chose que} \quad \int_1^2 y\,dy$$

Dans la formule précédente, nous pourrions avoir envie de remplacer les occurrences libres de x par un terme quelconque t. Cela se fait en définissant la notion de *substitution*. Commençons par définir la notion de remplacement, qui ne fonctionne bien que pour les termes t clos :

Définition 4 (Remplacement) *Soit u, t des termes bien formés, x une variable. Nous définissons le terme $\langle u/x\rangle t$ par induction sur la structure de t :*

- *Si t est une variable y différente de x, $\langle u/x\rangle y = y$.*
- *Si t est x, alors $\langle u/x\rangle x = u$.*
- *Si t est un symbole de fonction appliqué à ses arguments $f(t_1, ..., t_n)$ (n peut être nul), alors $\langle u/x\rangle f(t_1, ..., t_n) = f(\langle u/x\rangle t_1, ..., \langle u/x\rangle t_n)$.*

Soit P une proposition bien formée, nous définissons de même :

- *Si P est un prédicat d'arité n, alors nous posons $\langle u/x\rangle P(t_1, ..., t_n) = P(\langle u/x\rangle t_1, ..., \langle u/x\rangle t_n)$.*
- *Si P est une formule du type $\mathcal{Q}yR$, alors $\langle u/x\rangle \mathcal{Q}yR = \mathcal{Q}y\langle u/x\rangle R$. Avec $x \neq y$.*
- *Si P est une formule du type $\mathcal{Q}xR$, alors $\langle u/x\rangle \mathcal{Q}xR = \mathcal{Q}xR$.*
- *Si P est une formule du type QcR, où c est un connecteur propositionnel, alors $\langle u/x\rangle (QcR) = (\langle u/x\rangle Q)c(\langle u/x\rangle R)$.*

Nous remarquons que nous ne remplaçons pas les variables liées. Par contre, le problème suivant peut survenir :
$\langle y/x\rangle (\forall y Q(x, y)) = \forall y Q(y, y)$, ce qui n'est pas la même chose que la proposition initiale, car l'occurrence de x qui était libre devient une occurrence liée

de y. Ce phénomène s'appelle la capture de variable, et pour s'en débarrasser, il faudrait renommer y en z par exemple, pour d'abord obtenir la proposition (alphabétiquement équivalente) $\forall z Q(x, z)$ puis seulement ensuite remplacer x par y.

Ce problème n'apparaîtra nulle part dans notre travail, car nous ne remplacerons x que par des termes t clos, non sujets à la capture de variable. C'est pourquoi une définition comme la définition 4 nous convient tout à fait.

1.1.3 Qu'est-ce qu'une démonstration ?

Depuis vos plus jeunes années, vous êtes amenés en mathématiques ou en physique à démontrer des théorèmes, des propositions, ou certains résultats. Quel est leur point commun, qui fait qu'on peut les appeler *démonstrations* ?

C'est entre autre cette question qui a amené certains mathématiciens du XIX$^{\text{ème}}$ siècle à formaliser cette notion: une démonstration est une suite d'assertions $A_0, ..., A_n$ déduites les unes des autres par un certain nombre de règles, que l'on appelle *règles de déduction*. Certaines assertions, que l'on prend comme hypothèses (et donc n'ont pas besoin d'être démontrées) sont appelées les axiomes.

Ainsi, la suite $A_0, ..., A_n$ est une démonstration si pour tout $i \leq n$, A_i est:

- soit un axiome
- soit déduite de $A_0, ..., A_{i-1}$ par une règle logique.

Ainsi, le théorème de Pythagore est une théorème qui peut être démontré avec les axiomes de la *géométrie euclidienne*. L'abandon d'un de ces axiomes ("deux droites parallèles ne se coupent jamais") rend ce théorème faux (essayez par exemple de dessiner un triangle rectangle sur un globe terrestre).

Il y a aussi d'autres théorèmes, à caractère pratique, tels que "$7*3 = 21$". En effet, ce résultat, que l'on apprend par cœur à l'âge de 8 ans, est la conséquence des axiomes de *l'arithmétique de Peano* si l'on se place dans cette théorie.

Une démonstration se définit donc par deux choix: les axiomes et les règles de déduction. Le choix de ces deux points est absolument crucial, et donne toujours lieu à de très vivantes branches de la logique (même si elle ne se limite pas à cela, et de loin). Il fait l'objet de la section suivante.

1.2 Histoire des systèmes de déduction

1.2.1 Le premier système: la déduction *à la* Hilbert

Il n'y a qu'une seule règle de déduction, le *Modus Ponens*[1]: de A et de $A \Rightarrow B$ j'ai le droit de déduire B.

En revanche, il y a un grand nombre d'axiomes, les *axiomes logiques*, ou encore *axiomes propres*. En logique propositionnelle (c'est à dire lorsqu'on s'autorise uniquement des propositions sans quantificateurs), les voici (pour n'importe quelles propositions A, B, C):

$$(1.1)$$
$$A \Rightarrow B \Rightarrow A \tag{1.2}$$
$$(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \tag{1.3}$$
$$\bot \Rightarrow A \tag{1.4}$$
$$A \Rightarrow (\neg A \Rightarrow \bot) \tag{1.5}$$
$$(A \Rightarrow \bot) \Rightarrow \neg A \tag{1.6}$$
$$(A \wedge B) \Rightarrow A \tag{1.7}$$
$$(A \wedge B) \Rightarrow B \tag{1.8}$$
$$A \Rightarrow (B \Rightarrow (A \wedge B)) \tag{1.9}$$
$$A \Rightarrow (A \vee B) \tag{1.10}$$
$$B \Rightarrow (A \vee B) \tag{1.11}$$
$$(A \vee B) \Rightarrow ((A \Rightarrow C) \Rightarrow ((B \rightarrow C) \Rightarrow C)) \tag{1.12}$$
$$(1.13)$$
$$(1.14)$$

Auquel on rajoute parfois l'axiome du *tiers-exclu*: $A \vee \neg A$, qui ne peut pas être démontré à partir des axiomes précédents (il est possible de prouver ce résultat).

Outre ces axiomes logiques, que l'on a le droit d'utiliser à n'importe quel moment, on peut aussi, selon la théorie dans laquelle on se place, ajouter des *axiomes impropres*, comme ceux de la théorie des nombres de Peano (par ex. $0 + x = x$), ceux de la géométrie euclidienne, ceux de la théorie des ensembles, etc, etc ...

Voyons comment s'articule une démonstration en Déduction *à la* Hilbert. Essayons de prouver la proposition $A \Rightarrow A$. Tout d'abord, notons que ce n'est pas un axiome logique, et que nous n'avons pas d'axiomes impropres. Nous allons devoir travailler un peu:

[1] en fait, il y a une deuxième règle de déduction, la *généralisation* qui n'est pas nécessaire quand on n'utilise pas de quantificateur. Ceci est le cas dans ce petit résumé, qui ne cherche pas à être exhaustif.

1. $A \Rightarrow A \Rightarrow A$ est un axiome logique (1.2 dans lequel on a remplacé B par A).
2. $A \Rightarrow (A \Rightarrow A) \Rightarrow A$ est aussi un axiome logique (1.2 dans lequel on a remplacé B par $A \Rightarrow A$).
3. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ est encore un axiome logique (1.3).
4. on peut appliquer le Modus Ponens (MP) aux propositions 2. et 3. Nous obtenons la proposition $((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$.
5. Nous pouvons encore une fois appliquer le Modus Ponens aux propositions 4. et 1. Nous obtenons alors: $A \Rightarrow A$

Nous venons de toucher le plus gros problème de la déduction à la Hilbert: elle est absolument impraticable. C'est un très beau cadre théorique, encore utilisé de nos jours, mais qui ne se prête pas à l'automatisation.

Passons à une petite amélioration: la notation sous forme d'arbre. Au lieu d'avoir une séquence de propositions, nous allons noter maintenant une démonstration sous la forme d'un arbre. À chaque fois que l'on aura besoin d'appliquer la règle du Modus Ponens, on "affichera" les hypothèses en haut, et la conclusion en dessous:

$$\frac{A \Rightarrow B \qquad A}{B}\ \text{Modus Ponens}$$

Ce qui nous donne la démonstration suivante:

$$\dfrac{\dfrac{2.\quad A \Rightarrow (A \Rightarrow A) \Rightarrow A \qquad 3.\quad (A \Rightarrow (A \Rightarrow A) \Rightarrow A) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))}{4.\quad (A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)} \qquad 1.\quad A \Rightarrow A \Rightarrow A}{A \Rightarrow A}$$

1.2.2 La déduction naturelle — ancienne version

La déduction naturelle a été un autre pas en avant dans ce sens. Le principe est de remplacer les axiomes logiques par des règles de déduction. Ainsi, plus d'axiomes logiques, avec des instanciations abracadabrantes.[2]

C'est la version utilisée en LI214 (du moins dans le livre de cours). On rappelle ici certaines règles. le $[A]$ entre crochets signifie que l'on décharge l'hypothèse A: on l'enlève des hypothèses nécessaires à la démonstration de la proposition $A \Rightarrow B$. Notons que $[A]$ peut apparaître une ou plusieurs fois, voire même **zéro** fois.

La présentation d'une démonstration sera dorénavant faite sous forme d'arbre: le bas du nœud de l'arbre représente la conclusion que l'on a, et le haut (que l'on appelle les prémisses), les hypothèses dont on a besoin. Une démonstration

[2] les axiomes impropres, eux, restent, car ils ne sont pas spécifiques au système de déduction employé, mais à la théorie courante que l'on veut utiliser (arithmétique, géométrie, ensembles, ...)

entière de la proposition P sous l'ensemble des hypothèses Γ est un arbre dont la racine est étiquetée par P et les feuilles par des propositions appartenant de Γ (les hypothèses $[A]$ déchargées ne comptant pas pour des feuilles).

En déduction naturelle, il y a deux types de règles: celles qui introduisent des quantificateurs (il apparaissent dans la conclusion de la règle), et celles qui les éliminent (ils disparaissent dans la conclusion de la règle).

$\dfrac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \Rightarrow B}\ \Rightarrow\text{-intro}$	$\dfrac{A \quad A \Rightarrow B}{B}\ \Rightarrow\text{-elim}$
$\dfrac{A \quad B}{A \wedge B}\ \wedge\text{-intro}$	$\dfrac{A \wedge B}{A}\ \wedge\text{-elim} \qquad \dfrac{A \wedge B}{B}\ \wedge\text{-elim}$

Essayons maintenant de faire une démonstration de $A \Rightarrow A$ sans aucune hypothèse:

$$\frac{[A]}{A \Rightarrow A}$$

1.2.3 Déduction Naturelle — version moderne

Au lieu d'écrire les hypothèses (les axiomes impropres, donc, puisque nous n'avons plus d'axiome propres) dans les feuilles de l'arbre, nous allons les expliciter en les plaçant à côté de la proposition à démontrer.

Elles seront symbolisées par Γ qui représente un ensemble de propositions et séparées de P par le symbole $\vdash$, qui se lit "thèse". L'objet de base sera le séquent: $\Gamma \vdash P$ et a été introduit dans les années 1930. À l'intérieur de Γ, les propositions sont séparées par une virgule.

Cela permet de rendre la démonstration plus explicite. Une démontration de P sous les hypothèses Γ sera donc maintenant un arbre dont la racine est $\Gamma \vdash P$ et les feuilles sont des règles axiome ou tiers-exclu (ce sont les seules qui ne demandent aucune hypothèse), et construit selon les règles de la déduction naturelle.

$$\frac{}{\Gamma \vdash A}\ \text{axiome, si } A \in \Gamma$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-intro} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \Rightarrow B}{\Gamma \vdash B} \Rightarrow\text{-elim}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-elim} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-elim}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\text{-intro} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\text{-intro} \quad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-elim}$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A} \neg\text{-intro} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash C} \neg\text{-elim, } C\text{quelconque}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash C} \bot\text{-elim}$$

$$\frac{\Gamma \vdash \langle c/x \rangle P}{\Gamma \vdash \forall x P} \forall\text{-intro}^* \qquad \frac{\Gamma \vdash \forall x P}{\Gamma \vdash \langle t/x \rangle P} \forall\text{-elim}$$

$$\frac{\Gamma \vdash \langle t/x \rangle P}{\Gamma \vdash \exists x P} \exists\text{-intro} \qquad \frac{\Gamma \vdash \exists x P \quad \Gamma, \langle c/x \rangle P \vdash A}{\Gamma \vdash A} \exists\text{-elim}^*$$

(*). À condition que la constante c n'apparaisse ni dans Γ, ni dans A. Cette condition est nécessaire, sinon nous pourrions avoir une preuve de:

$$\vdash \exists x P(x) \Rightarrow \forall x P(x)$$

ce qui n'est évidemment pas le but souhaité.

La démonstration de $A \Rightarrow A$ se déroule maintenant de la façon suivante:

$$\frac{\dfrac{}{A \vdash A}\ \text{axiome}}{\vdash A \Rightarrow A} \Rightarrow\text{-intro}$$

Remarquons aussi la forte analogique entre les règles d'introduction et d'élimination de $\wedge$ et $\vee$ de la Déduction Naturelle et les axiomes logiques correspondant de Hilbert. C'est cette analogie qui permet de démontrer l'équivalence entre les deux systèmes:

Théorème 1 *Une proposition P est démontrable à partir des hypothèses Γ en déduction à la Hilbert si et seulement si elle l'est en Déduction Naturelle.*

1.2.4 La règle du tiers-exclu

Avec les règles précédentes, il est impossible de démontrer la proposition $A \vee \neg A$ (que l'on appelle le tiers-exclu). Ceci n'est pas un mal, et donne naissance à de nombreuses de logiques dont certaines propriétés sont très utiles (et que la logique classique n'a pas). Cette règle est soumise à de nombreuses controverses,

et peut être utile ou non. Le tout est de savoir ce que l'on fait, et ce dont on a besoin.

Par exemple, en français, avons nous équivalence entre les deux phrases suivantes:
"L'accès est interdit à toute personne non autorisée"
"L'accès est autorisé à toute personne non interdite"

Le tiers-exclu permet typiquement de démontrer leur équivalence. De même, doit-on pouvoir démontrer des phrases comme le principe des buveurs: "Dans un bar, il existe une personne qui, si elle boit, alors tout le monde boit.". Y compris en mathématiques, cela a des répercussions non négligeables: ne pas s'autoriser le tiers-exclu permet d'avoir des démonstrations constructives, c'est à dire qu'elle construit un objet qui répond aux critères. Voir sur ce sujet l'article d'Alexandre Miquel dans le numéro hors-série de Pour la Science (Les chemins de la Logique).

Puisque nous voulons nous en servir, nous devons donc le rajouter explicitement, ce qui donne naissance à une règle supplémentaire:

$$\frac{}{\Gamma \vdash A \vee \neg A}\ \text{tiers-exclu}$$

Elle peut aussi être exprimée sous la forme de la règle suivante:

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ \text{tiers-exclu}$$

Si on dispose d'une de ces deux règles, alors on peut prouver l'autre.

Enfin, un dernier exemple: avec la règle du tiers-exclu, on peut démontrer facilement l'assertion suivante: il existe deux nombres irrationnels a et b tels que a^b (a à la puissance b) soit rationnel. (indication: considérer $\sqrt{2}$ et $\sqrt{2}^{\sqrt{2}}$). Ne pas utiliser le tiers-exclu requiert de trouver explicitement les nombres a et b, ce qu'évite l'utilisation de ce principe.

1.3 Le calcul des séquents

1.3.1 Démonstration automatique

Le but du projet est de construire un programme permettant de prouver automatiquement une proposition P sous des hypothèses Γ (si celle-ci est prouvable).[3]

Le problème de la recherche automatique de démonstration en déduction naturelle est que l'on ne sait pas par quel bout commencer: doit on déstructurer la proposition P dans $\Gamma \vdash P$ (on part alors du séquent que l'on doit démontrer: c'est le chaînage arrière), on bien doit-on essayer de combiner les propositions de Γ (que l'on récupère à droite du séquent avec la règle axiome) jusqu'à arriver à P ?

Par exemple, si l'on essaye de démontrer:

$$P \Rightarrow Q \Rightarrow (P \wedge Q)$$

sans hypothèse de départ en chaînage arrière, alors la seul règle qui puisse s'appliquer (mis à part le tiers-exclu) est la règle d'introduction de $\Rightarrow$ (on énumère toutes les règles possibles. Par exemple $\vee$-intro ne peut s'appliquer qu'à des propositions de la forme $A \vee B$).

Ainsi, la démonstration se termine donc de cette manière:

$$\dfrac{\dfrac{\dfrac{\vdots}{P, Q \vdash P \wedge Q}}{P \vdash Q \Rightarrow (P \wedge Q)}}{\vdash P \Rightarrow Q \Rightarrow (P \wedge Q)}$$

Puis, l'on voit que la seule règle applicable est l'introduction de $\wedge$, et donc on se ramène à la preuve (partielle) suivante:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{P, Q \vdash P} \quad \dfrac{\vdots}{P, Q \vdash Q}}{P, Q \vdash P \wedge Q}}{P \vdash Q \Rightarrow (P \wedge Q)}}{\vdash P \Rightarrow Q \Rightarrow (P \wedge Q)}$$

et la fin est laissée au lecteur ...

En fait, on peut montrer que l'on a besoin des deux étapes ensemble, et que chacune des deux amène ses problèmes. En particulier, l'étape qui part des hypothèses pour arriver aux conclusions est très problématique car elle implique

[3] Des résultats concernant l'indécidabilité assurent que c'est le mieux que l'on puisse faire: chercher une preuve jusqu'à ce qu'on la trouve. Si on ne la trouve pas, il est possible que nous n'ayions pas cherché assez longtemps. Ce résultat négatif peut être tempéré de deux manières: on peut tout d'abord chercher en même temps une démonstration de P et de $\neg P$. Ceci n'est pas toujours suffisant. L'autre résultat positif est que lorsque ni P, ni les propositions de Γ n'ont de quantificateur, la recherche termine.

une énumération de toutes les propositions disponibles: pour démontrer P sous les hypothèses $P \wedge Q$, que devons nous faire?

$$\frac{\vdots}{P \wedge Q \vdash P}$$

En chaînage arrière, il faudrait énumérer toutes les règles applicables: aucune règle d'introduction n'est possible. Et toutes les règles d'élimination: quelle proposition choisir pour effectuer une élimination ? Il faut faire une énumération plus que longue ...

Au contraire, en partant de $P \wedge Q$, l'hypothèse, et donc du séquent $P \wedge Q \vdash P \wedge Q$, on peut voir qu'on arrive plus facilement à la conclusion qu'il faut appliquer une règle $\wedge$-elim. Cependant, ce n'est pas encore la panacée: quelle est la proposition que l'on doit supprimer ? Ici encore se cache une énumération, laquelle des deux règles doit-on appliquer: $\frac{P \wedge Q \vdash P \wedge Q}{P \wedge Q \vdash Q}$ ou $\frac{P \wedge Q \vdash P \wedge Q}{P \wedge Q \vdash P}$?

Ce problème est lié au fait que la déduction naturelle travaille uniquement sur les propositions à la droite du séquent, et qu'on ne touche surtout pas aux sacro-saintes hypothèses. À chaque fois qu'on veut en utiliser une, on est obligé de passer par une règle axiome pour la mettre à droite du séquent ... puis d'utiliser des règles d'élimination pour accéder à ce qui nous intéresse, comme dans l'exemple précédent.

1.3.2 Le calcul des séquents: première version

L'idée absolument novatrice introduite par Gentzen a été la suivante: au lieu de travailler uniquement sur les propositions à droite d'un séquent $\Gamma \vdash P$, comme cela est le cas dans la déduction naturelle, travaillons aussi sur les propositions qui sont à gauche (donc, celles appartenant à Γ).

De cette manière, toutes les règles d'élimination sont transformées en règles "gauches" sur les hypothèses et toutes les règles d'introduction sont transformées en règles droites.

Par exemple, on aura maintenant la règle suivante:

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge\text{-gauche}$$

En effet: supposer $A \wedge B$, c'est la même chose que supposer A et B indépendamment.

Ce calcul est beaucoup plus adapté à la démonstration automatique, car il ne fait que déstructurer les propositions. Le voici présenté figure 1.1.

On y ajoute parfois la règle du tiers-exclu:

$$\frac{\Gamma \vdash \neg\neg P}{\Gamma \vdash P}$$

$\dfrac{}{\Gamma \vdash P}$ axiome si $P \in \Gamma$

$\dfrac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}$ coupure

$\dfrac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}$ contr-g

$\dfrac{}{\Gamma, \bot \vdash Q}\bot$-g

$\dfrac{\Gamma \vdash Q}{\Gamma, P \vdash Q}$affaiblissement-g

$\dfrac{\Gamma \vdash}{\Gamma \vdash P}$ affaiblissement-d

$\dfrac{\Gamma, P, Q \vdash R}{\Gamma, P \wedge Q \vdash R} \wedge$-g

$\dfrac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q} \wedge$-d

$\dfrac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R} \vee$-g

$\dfrac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \vee$-d $\qquad\qquad$ $\dfrac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \vee$-d

$\dfrac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R} \Rightarrow$-g

$\dfrac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q} \Rightarrow$-d

$\dfrac{\Gamma \vdash P}{\Gamma, \neg P \vdash Q}\neg$-g

$\dfrac{\Gamma, P \vdash}{\Gamma \vdash \neg P}\neg$-d

$\dfrac{\Gamma, \langle t/x \rangle P \vdash Q}{\Gamma, \forall x P \vdash Q}\forall$-g, t clos

$\dfrac{\Gamma \vdash \langle c/x \rangle P}{\Gamma \vdash \forall x P}\forall$-d, c constante fraîche, i.e. qui n'apparaît pas dans $\Gamma \vdash \forall x P$

$\dfrac{\Gamma, \langle c/x \rangle P \vdash Q}{\Gamma, \exists x P \vdash Q}\exists$-g, c constante fraîche, qui n'apparaît pas dans $\Gamma \vdash \exists x P$

$\dfrac{\Gamma \vdash \langle t/x \rangle P}{\Gamma \vdash \exists x P}\exists$-d, t clos

Figure 1.1: Règles d'inférence du calcul des séquents intuitionniste

La règle de coupure:

$$\frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q} \text{ coupure}$$

est une règle nécessaire pour prouver (facilement) l'équivalence de la Déduction Naturelle et du calcul des séquents. Cependant, on peut démontrer (et c'est un résultat central de la théorie de la démonstration, qui mène à beaucoup d'autres résultats) qu'elle est redondante et que finalement, on n'en a pas besoin.[4]

De même, la règle de contraction, qui dit qu'on a le droit de supposer deux fois la même chose est nécessaire pour montrer l'équivalence entre les deux systèmes de déduction. Comme on le verra plus tard, elle est est rendue nécessaire par la présence des quantificateurs.

1.3.3 Le tiers-exclu: version définitive du calcul des séquents

On peut supprimer la règle du tiers-exclu si l'on autorise plusieurs propositions à droite. Voici une idée du pourquoi:

Prouvons $A \vee \neg A$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A \vee \neg A}\vee\text{-d}}{\neg(A \vee \neg A), A \vdash}\neg\text{-g}}{\neg(A \vee \neg A) \vdash \neg A}\neg\text{-d}}{\neg(A \vee \neg A) \vdash A \vee \neg A}\vee\text{-g}}{\neg(A \vee \neg A), \neg(A \vee \neg A) \vdash}\neg\text{-g}}{\neg(A \vee \neg A) \vdash}\text{contraction-g}}{\vdash \neg\neg(A \vee \neg A)}\neg\text{-d}}{\vdash A \vee \neg A}\text{Tiers-Exclu}$$

on s'est servi du tiers-exclu de manière à stocker à gauche du séquent la proposition que l'on voulait, de manière à la dupliquer par la règle de contraction. Ensuite, on la repasse à droite de nouveau, mais maintenant, nous avons des hypothèses, ce que nous n'avions pas au départ.

On peut éviter tous ces détours en autorisant directement plusieurs propositions à droite du séquent. On peut montrer que ces deux versions sont équivalentes (si on autorise le tiers-exclu dans la première version).

Le calcul des séquents aura donc la forme de la figure 1.2.

1.4 Le problème du zèbre

On considère cinq maisons, toutes de couleur différente (rouge, bleu, jaune, blanc, vert), dans lesquelles logent cinq professionnels (peintre, sculpteur, diplo-

[4] Cela sera très utile de savoir s'en passer, en démonstration automatique. En chaînage arrière, il faudrait énumérer toutes les propositions P, ce qui prendrait un certain temps ... il y aurait encore beaucoup à dire au sujet de la règle de coupure.

$$\frac{}{\Gamma \vdash \Delta}\text{axiome si il existe } P \in \Gamma \cap \Delta$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta}\text{coupure}$$

$$\frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\text{contr-g}$$

$$\frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\text{contr-d}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, P \vdash \Delta}\text{affaiblissement-g}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash P, \Delta}\text{affaiblissement-d}$$

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \wedge\text{-g}$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \wedge\text{-d}$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta} \vee\text{-g}$$

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta} \vee\text{-d}$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta} \Rightarrow\text{-g}$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \Rightarrow Q, \Delta} \Rightarrow\text{-d}$$

$$\frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\neg\text{-g}$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\neg\text{-d}$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\bot\text{-g}$$

$$\frac{\Gamma, \langle t/x \rangle P \vdash \Delta}{\Gamma, \forall x P \vdash \Delta}\forall\text{-g, } t \text{ clos}$$

$$\frac{\Gamma \vdash \langle c/x \rangle P, \Delta}{\Gamma \vdash \forall x P, \Delta}\forall\text{-d, } c \text{ constante fraîche}$$

$$\frac{\Gamma, \langle c/x \rangle P \vdash \Delta}{\Gamma, \exists x P \vdash \Delta}\exists\text{-g, } c \text{ constante fraîche}$$

$$\frac{\Gamma \vdash \langle t/x \rangle P, \Delta}{\Gamma \vdash \exists x P, \Delta}\exists\text{-d, } t \text{ clos}$$

Figure 1.2: règles d'inférence du calcul des séquents classique

mate, docteur et violoniste) de nationalité différente (anglaise, espagnole, japonaise, norvégienne et italienne) ayant chacun une boisson favorite (thé, jus de fruits, café, lait et vin) et un animal favori (chien, escargot, renard, cheval et zèbre).

On dispose des faits suivants:

1. l'Anglais habite la maison rouge.
2. l'Espagnol possède un chien.
3. le Japonais est peintre.
4. l'Italien boit du thé.
5. le Norvégien habite la première maison à gauche.
6. le propriétaire de la maison verte boit du café.
7. la maison verte est juste à droite de la blanche.
8. le sculpteur élève un escargot.
9. le diplomate habite la maison jaune.
10. on boit du lait dans la maison du milieu.
11. le Norvégien habite à côté de la maison bleue.
12. le violoniste boit du jus de fruit.
13. le renard est dans une maison voisine du médecin.
14. le cheval est à coté de la maison du diplomate.

Trouver le possesseur du zèbre et le buveur de vin. Une fois votre programme de preuve automatique écrit, le tester sur cet exemple.

1.5 Autres systèmes logiques

D'autres logiques sont utilisées, qui font appel à des extensions de la logique du premier ordre que nous venons de voir. Parmi celles-ci on peut citer les *logiques modales*, qui font appel à deux connecteurs $\Box$, $\diamond$ (la nécessité et la possibilité). Elles sont utilisées surtout en Intelligence Artificielle (avec d'autres formes de raisonnement "exotiques" qui ne ressemblent plus vraiment à de la logique).

On peut aussi citer la Déduction Modulo, qui a pour objet de combiner déduction et règles de calcul. Par exemple, dans le système axiomatique de Peano, il est très long et très fastidieux de démontrer l'assertion $2 + (3 * 4) = 14$ alors que n'importe quel programme de type Maple, ou même votre petit frère, vous répondra immédiatement que c'est vrai.

La raison est qu'à formaliser à tout va, on a oublié que la majeur partie des mathématiques était une question de calcul, et non pas de raisonnement. La Déduction Modulo a vocation à remplacer tout ce qui peut être calculé par sa "vraie" valeur. Ainsi, $2 + (3 * 4)$ est remplacé par 14 et nous obtenons la proposition $14 = 14$, qui est évidemment (pourquoi ?) vraie.

L'avantage de cette technique est que les axiomes sont transformés en règles de calcul, par exemple, l'axiome:

$$x + s(y) = s(x + y)$$

est transormé en règle de calcul:

$$x + s(y) \rightarrow s(x + y)$$

En orientant ainsi notre théorie, on obtient beaucoup d'avantages.

Enfin, on peut citer la logique linéaire, qui analyse très finement les règles logiques, et en un sens, étend les logiques modales, classiques, intuitionnistes. Pour en expliquer rapidement la teneur, nous pouvons faire la remarque suivante. Soit la proposition "J'ai 1 Euro", et les axiomes "si j'ai 1 Euro, je peux acheter un café", "si j'ai 1 Euro, je peux acheter un croissant". Alors, en déduction naturelle, je peux prouver la proposition "paradoxale" suivante: "Avec un Euro, je peux acheter un café et un croissant":

$$\frac{\text{J'ai 1E, Un éclair vaut 1E, Un café vaut 1E} \vdash \text{J'achète un café} \qquad \text{J'ai 1E, Un éclair vaut 1E, Un café vaut 1E} \vdash \text{J'achète un éclair}}{\text{J'ai 1E, Un éclair vaut 1E, Un café vaut 1E} \vdash \text{J'achète un café} \wedge \text{J'achète un éclair}}$$

Le problème ici est que l'hypothèse "J'ai 1E" est consommée lorsque je l'utilise, et donc qu'elle n'est utilisable que dans une seule des deux branche de ma démonstration (et pas les deux). C'est ce problème (sa version mathématisée à l'extrême, avec des fonction linéaires, des catégories, etc.) qui est à la source de la Logique Linéaire de Jean-Yves Girard. Et c'est pour cela qu'elle est très bien adaptée à la modélisation des ressources.

Pour terminer, parlons un peu de la logique d'ordre supérieur: en logique du premier ordre, nous ne pouvons pas exprimer la proposition $Impl := \forall P(P \Rightarrow P)$ (pour toute proposition P, P implique P), car nous n'avons aucun moyen d'utiliser un quantificateur sur les propositions, nous ne pouvons le faire que sur les termes.

La logique d'ordre supérieur autorise ce genre de manipulations, mais il faut faire très attention: dans la proposition $\forall P(P \Rightarrow P)$ on peut par exemple décider d'instancier P par $Impl$, ce qui nous donne:

$$Impl \Rightarrow Impl$$

ou, en clair:

$$(\forall P(P \Rightarrow P)) \Rightarrow (\forall P(P \Rightarrow P))$$

ce qui est une sorte de circularité, qui s'appelle l'imprédicativité. Celle-ci n'est pas gênante, mais provoque beaucoup de complications pour prouver toutes les bonnes propriétés du nouveau système logique. La gestion de l'imprédicativité

dans les systèmes logiques reste cependant mal comprise et peut très rapidement conduire à des incohérence (plus que subtiles, mais une seule suffit !).

L'avantage de ce genre de logique (sur laquelle est basé λ-prolog) est qu'il procure beaucoup plus de puissance et de souplesse bien qu'il soit plus difficile à gérer pour la démonstration automatique. Bref, un champ de recherche très vaste.

Chapter 2

La pratique

2.1 Le calcul des séquents

Le calcul des séquents effectivement implémenté sera celui présenté figure 2.1. On peut prouver qu'il est équivalent au calcul des séquents précédent, de la figure 1.2: on supprime la règle de coupure (qui est redondante), ainsi que les règles d'affaiblissement (la règle axiome contient plusieures propositions dans Γ, Δ, on peut donc s'en passer). On restreint aussi la contraction à ne s'appliquer qu'à des propositions quantifiées existentiellement quand elles sont à droite et universellement quand elles sont à gauche. Cela est dû au fait que ces deux règles (et uniquement ces deux règles) ne vérifient pas le lemme de Kleene 1 ci dessous. Elles ne sont pas inversibles pour deux raisons: premièrement parce que nous pouvons avoir besoin de deux témoins (essayez de démontrer par exemple le séquent $\forall x P(x) \vdash P(0) \wedge P(1)$, d'abord en commençant par la règle $\forall$-gauche, puis en commençant par la règle de contraction. Deuxièmement à cause des conditions de fraîcheur de constantes, sur lesquelles nous reviendrons.

Nous cherchons à savoir si un séquent $\Gamma \vdash \Delta$ a une preuve (ce qui revient à dire que nous cherchons une preuve de Δ à partir des hypothèses Γ). Le calcul des séquent présenté figure 2.1 se prête très bien à ce genre de calcul par la méthode du chaînage arrière: on cherche quelle est la dernière règle appliquée, et une fois qu'on l'a trouvée, on cherche l'avant-dernière, etc, etc.

2.2 Cas propositionnel

Dans le cas propositionnel, on considère des formules qui ne comportent pas de quantificateurs. On ne sait cependant pas encore quelle est la règle à appliquer en premier dans notre recherche de preuve. Mais le lemme d'inversion de Kleene nous dit alors:

$\dfrac{}{\Gamma \vdash \Delta}$ axiome si il existe P atomique $\in \Gamma \cap \Delta$

$\dfrac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}$ contr-g, si P de la fome $\forall x Q$

$\dfrac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}$ contr-d, si P de la forme $\exists x Q$

$\dfrac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge$-g

$\dfrac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}\ \wedge$-d

$\dfrac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}\ \vee$-g

$\dfrac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}\ \vee$-d

$\dfrac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta}\ \Rightarrow$-g

$\dfrac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \Rightarrow Q, \Delta}\ \Rightarrow$-d

$\dfrac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg$-g

$\dfrac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\ \neg$-d

$\dfrac{}{\Gamma, \bot \vdash \Delta}\ \bot$-g

$\dfrac{\Gamma, \langle t/x \rangle P \vdash \Delta}{\Gamma, \forall x P \vdash \Delta}\ \forall$-g, t clos

$\dfrac{\Gamma \vdash \langle c/x \rangle P, \Delta}{\Gamma \vdash \forall x P, \Delta}\ \forall$-d, c constante fraîche

$\dfrac{\Gamma, \langle c/x \rangle P \vdash \Delta}{\Gamma, \exists x P \vdash \Delta}\ \exists$-g, c constante fraîche

$\dfrac{\Gamma \vdash \langle t/x \rangle P, \Delta}{\Gamma \vdash \exists x P, \Delta}\ \exists$-d, t clos

Figure 2.1: calcul des séquents à implanter

Lemme 1 (Kleene)

- *Si on a une preuve du séquent* $\Gamma, A \wedge B \vdash \Delta$*, alors il existe une preuve commençant par la règle* $\wedge$*-gauche sur cette proposition:*

$$\dfrac{\dfrac{\pi}{\Gamma, A, B \vdash \Delta}}{\Gamma, A \wedge B \vdash \Delta}$$

- *Si on a une preuve du séquent* $\Gamma \vdash A \wedge B, \Delta$*, alors il existe une preuve commençant par la règle* $\wedge$*-droite sur cette proposition:*

$$\dfrac{\dfrac{\pi}{\Gamma \vdash A, \Delta} \quad \dfrac{\pi'}{\Gamma \vdash B, \Delta}}{\Gamma \vdash A \wedge B, \Delta}$$

- *et ainsi de suite pour toutes les autres règles faisant intervenir les connecteurs logiques. Si on a une preuve du séquent* $\Gamma, A \vee B \vdash \Delta$*, alors il existe une preuve commençant par la règle* $\vee$*-gauche sur cette proposition.*
- *Si on a une preuve du séquent* $\Gamma \vdash A \vee B, \Delta$*, alors il existe une preuve commençant par la règle* $\vee$*-droite sur cette proposition.*
- *Si on a une preuve du séquent* $\Gamma, A \Rightarrow B \vdash \Delta$*, alors il existe une preuve commençant par la règle* $\Rightarrow$*-gauche sur cette proposition.*
- *Si on a une preuve du séquent* $\Gamma \vdash A \Rightarrow B, \Delta$*, alors il existe une preuve commençant par la règle* $\Rightarrow$*-droite sur cette proposition.*
- *Si on a une preuve du séquent* $\Gamma, \neg A \vdash \Delta$*, alors il existe une preuve commençant par la règle* $\neg$*-gauche sur cette proposition.*
- *Si on a une preuve du séquent* $\Gamma \vdash \neg A, \Delta$*, alors il existe une preuve commençant par la règle* $\neg$*-droite sur cette proposition.*

Preuve. Par induction sur la preuve originale, en considérant la dernière règle appliquée. □

Une autre vision de ce lemme peut être la suivante: si on a une preuve de la forme suivante:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash C, D, \Delta} \quad \dfrac{\pi'}{\Gamma, B \vdash C, D, \Delta}}{\Gamma, A \vee B \vdash C, D, \Delta} \vee\text{-g}}{\Gamma, A \vee B \vdash C \vee D, \Delta} \vee\text{-d}$$

alors on peut permuter les deux règles et avoir la démonstration suivante:

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash C, D, \Delta}}{\Gamma, A \vdash C \vee D, \Delta} \vee\text{-d} \quad \dfrac{\dfrac{\pi'}{\Gamma, B \vdash C, D, \Delta}}{\Gamma, B \vdash C \vee D, \Delta} \vee\text{-d}}{\Gamma, A \vee B \vdash C \vee D, \Delta} \vee\text{-g}$$

Ce lemme justifie le fait que, cherchant une démonstration du séquent $\Gamma \vdash \Delta$, on peut commencer par n'importe quelle règle sur n'importe quelle proposition, cela n'a pas d'importance. Ainsi, la stratégie sera d'appliquer une règle à chaque fois que l'on rencontre une proposition non atomique. Lorsque (dans les feuilles de l'arbre) on aura des séquents "atomiques" (qui ne contiennent que des propositions atomiques: des symboles de prédicat), on pourra essayer d'appliquer la règle axiome à chacun des séquents-feuille tour à tour. Si on y arrive, on a construit une démonstration.

2.3 Ajout des quantificateurs

Nous allons dans un premier temps nous concentrer sur des propositions quantifiées existentiellement à droite (ou, équivalemment, universellement à gauche). Ainsi, nous laissons pour plus tard le problème de l'introduction des contraintes de fraîcheur de constantes.

Quelques exemples récurrents nous servirons: le séquent $\vdash \exists x(P(x) \Rightarrow P(f(x))$, le séquent $\forall x P(x) \vdash \exists x P(x)$.

2.3.1 Substitution dans un terme/dans une proposition

Lorsqu'on applique une règle $\forall$-g ou $\exists$-d, elle remplace x par t dans P:

$$\frac{A(2) \vdash A(2) \vee B(f(2))}{A(2) \vdash \exists x(A(x) \vee B(f(x))} \exists\text{-d}$$

dans ce cas-la, nous avons $\langle 2/x \rangle (A(x) \vee B(f(x)) = A(2) \vee B(f(2))$. Ceci implique l'écriture de deux fonctions:

- substitution d'une variable par un terme dans une formule.($\langle 2/x \rangle (A(x) \vee B(f(x)))$
- substitution d'une variable par un terme dans un terme.($\langle 2/x \rangle (f(x))$).

2.3.2 Algorithme d'unification

Pour l'instant, on ne tient pas compte de la règle de contraction, de plus, on considère que tous les termes sont *clos*, c'est à dire ne comportent pas de variables libres (qui sont assimilables à des constantes).

Lorsqu'on essaie de prouver le séquent $P(a) \vdash \exists x P(x)$, quel terme doit-on introduire à la place de x:

$$\frac{A(2) \vdash A(\mathbf{??}) \vee B(f(\mathbf{??}))}{A(2) \vdash \exists x(A(x) \vee B(f(x))} \exists\text{-d}$$

L'*intuition* nous indique qu'il faut substituer les points d'interrogation par 2. Mais l'algorithme, lui, n'a *aucun* moyen de le savoir. L'idée est donc de différer

le moment de ce choix jusqu'à l'application de la règle axiome. C'est pourquoi, au lieu des points d'interrogation "??", on va mettre un "trou", qui aura un nom *frais* à chaque nouvelle application de la règle ∃-d: une métavariable. On aboutira donc à un *schéma de démonstration*:

$$\dfrac{\dfrac{A(2) \vdash A(X), B(f(X))}{A(2) \vdash A(X) \vee B(f(X))}}{A(2) \vdash \exists x(A(x) \vee B(f(x))} \exists\text{-d}$$

En effet, nous ne savons pas encore par quoi remplacer X pour obtenir une démonstration valide du calcul des séquents (c'est à dire pour que toutes les feuilles de l'arbre de démonstration soient des atomes): c'est l'algorithme d'unification qui va nous l'indiquer. Nous passerons le reste de cette section à le décrire.

Dans la feuille précédente, on peut essayer d'appliquer la règle axiome entre les deux formules atomiques $A(2)$ et $B(f(X))$. Comme les deux symboles de prédicats sont différents, cela échoue (mais il faut quand-meme faire l'essai, jusqu'à trouver la bonne paire de propositions).

La deuxième possibilité est d'appliquer la règle axiome entre $A(2)$ et $A(X)$. Dans ce cas il faut que $X = 2$. On dit qu'on a réussi à unifier X et 2. L'algorithme général décrit dans la figure ci-dessous donne la solution dans tous les cas (et lève une exception si l'on ne peut pas unifier). Il nous donne une *substitution* qui est telle que les deux atomes sont identiques après application de cette substitution.

Mais avant de décrire l'algorithme, intéressons nous à d'autres exemples. Dans la démonstration précédente, il fallait donc remplacer X par 2. Alors, il faut faire la substitution dans *toute* la démonstration. C'est en particulier le cas si on a plusieurs feuille à l'arbre.

Essayons par exemple de démontrer le séquent suivant:

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

Si l'on prend la feuille de gauche, $P(X) \vdash P(b), P(a), Q(b)$, on peut unifier $P(X)$ et $P(a)$, ce qui donne la substitution $X = a$. On peut appliquer la règle axiome dans le séquent de gauche, mais dans ce cas, il faut subsituer X par a partout dans la démonstration. Ainsi, la deuxième feuille devient: $Q(a) \vdash P(b), P(a), Q(b)$ auquel on ne peut pas appliquer la règle axiome. La démonstration échoue.

Cependant, si on revient en arrière et qu'on essaie d'unifier $P(X)$ et $P(b)$ dans la première feuille, alors on trouve la substitution $X = b$. Cette substitution marche, c'est à dire qu'en remplaçant la métavariable X par b dans le

schéma de démonstration précédent, toutes les feuilles sont effctivement des axiomes, car il est trivial d'unifier $Q(b)$ à $Q(b)$. Et on obtient la démonstration suivante:

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

On voit donc qu'il est important de:

1. tester toutes les unification possibles lorsqu'on veut appliquer la règle axiome.
2. penser à substituer dans toutes la démonstration (ou au moins dans toutes les feuilles) X par σX, avec σ la substitution donnée par l'algorithme d'unification.
3. continuer à essayer d'appliquer la règle axiome aux séquents atomiques pour lesquels on ne sait pas encore si on peut appliquer la règle axiome ou non.

Description de l'algorithme

Notre point de départ sera une équation $P(t_1, ..., t_n) = Q(t'_1, ..., t'_m)$ avec P symbole de prédicat.

- Si P est différent de Q, alors le système n'est pas unifiable.
- Si $P = Q$, mais que $m \neq n$, le système n'est pas unifiable non plus (arités différentes).
- dans le cas contraire, on doit résoudre le système $\{t_1 = t'_1, \ ... \ , t_n = t'_n\}$. On a donc n équations entre termes.

Nous devons maintenant résoudre un système d'équations: $\mathcal{S} = \{u_1 = u'_1, \ ... \ , u_p = u'_p\}$ entre termes, qui comportent des méta-variables. Si ce système est vide (ne comporte pas d'équation), alors la solution est déjà trouvée, puisque n'importe quoi (donc en particulier la substitution vide) est solution. Sinon, on choisit une équation du système et on l'analyse, supposons que c'est $u_1 = u'_1$:

- Si cette équation est de la forme $f(t_1, ..., t_n) = t$ et que t n'est ni une fonction, ni une métavariable, alors l'unification est impossible.
- Si cette équation est de la forme $f(t_1, ..., t_n) = g(t'_1, ..., t'_m)$ et que $f \neq g$, ou que $n \neq m$ alors l'unification est impossible.
- Si cette équation est de la forme $f(t_1, ..., t_n) = f(t'_1, ..., t'_n)$ alors on résoud le système $\{t_1 = t'_1, ..., t_n = t'_n, u_2 = u'_2, ..., u_p = u'_p\}$

- Si cette équation est de la forme $c = t$ avec c symbole de constante, et t n'est ni une constante, ni une métavariable, alors l'unification est impossible.
- Si cette équation est de la forme $c = d$ avec d symbole de constante $\neq c$, alors l'unification est impossible.
- Si cette équation est de la forme $c = c$ alors on supprime cette équation du système, et on résoud le système restant, c'est à dire $\{u_2 = u'_2,\ \ldots\ , u_p = u'_p\}$. Notons que les cas où l'on a une constante sont **exactement** les mêmes que ceux où l'on aurait une fonction à 0 variables. On peut donc supprimer dans le type Caml le constructeur pour les constantes, et autoriser les fonction de 0 variables. C'est pourquoi nous ne détaillerons plus le cas des constantes dans la suite.
- Nous ne nous intéresserons pas au cas où l'on a des variables, car dans notre algorithme, cela n'arrivera pas (on essaiera toujours d'unifier des termes clos, c'est à dire ne comportant pas de variables).
- Si cette équation est de la forme $X = t$ ou bien $t = X$ alors si X apparaît dans t, le système n'a pas de solution.
- Si cette équation est de la forme $X = t$ ou bien $t = X$ et que X n'apparaît pas dans t, alors il faut:
  1. Résoudre le système d'équations $\{\langle t/X\rangle u_2 = \langle t/X\rangle u'_2, ..., \langle t/X\rangle u_p = \langle t/X\rangle u'_p\}$, qui est le système où l'on a substitué partout t à X.
  2. on obtient une substitution σ' (ne comportant donc pas la métavariable X).
  3. la substitution solution est $\sigma = \langle \sigma' t/X\rangle \cup \sigma'$. En effet, il ne faut pas oublier d'appliquer σ' à t, qui peut comporter encore des métavariables qui sont substituées par σ'.

Ces règles sont résumées dans la figure 2.2. La règle d'inversion n'est pas une règle nécéssaire, mais elle est utile (pour ne pas avoir à réaliser deux fois le même travail). elle permet d'économiser des cas dans le filtrage.

Pour aller plus loin

En fait, étant donné les feuilles d'un schéma de démonstration :

$$\dfrac{\dfrac{\Gamma_1 \vdash \Delta_1, \cdots, \Gamma_n \vdash \Delta_n}{\ddots\ \vdots}}{\Gamma \vdash \Delta}$$

on cherche si on peut la transformer en démonstration, c'est à dire on cherche une substitution τ telle que pour tous les séquents $\tau\Gamma_1 \vdash \tau\Delta_1$, ..., $\tau\Gamma_n \vdash \tau\Delta_n$ on puisse appliquer la règle axiome. ($\tau\Gamma$ représente les propositions de Γ après application de la substitution τ). S'il en existe une, rien ne nous assure que:

$\{f(t_1,...,t_n) = g(t'_1,...,t'_m)\} \bigcup \mathcal{S}$	$\overset{\text{conflit}}{\rightsquigarrow}$	`erreur` si $f \neq g$ ou $n \neq m$
$\{f(t_1,...,t_n) = f(t'_1,...,t'_n)\} \bigcup \mathcal{S}$	$\overset{\text{décomposition}}{\rightsquigarrow}$	$\{t_1 = t'_1, ..., t_n = t'_n\} \bigcup \mathcal{S}$
$\{t = t\} \bigcup \mathcal{S}$	$\overset{\text{effacement}}{\rightsquigarrow}$	$\mathcal{S}$
$\{X = t\} \bigcup \mathcal{S}$	$\overset{\text{occurrence}}{\rightsquigarrow}$	`erreur`, si X apparaît dans t
$\{X = t\} \bigcup \mathcal{S}$	$\overset{\text{élimination}}{\rightsquigarrow}$	$\langle \sigma' t/X \rangle \cup \sigma'$, avec σ' solution de $\langle t/X \rangle \mathcal{S}$ si X n'apparaît pas dans t
$\{t = X\} \bigcup \mathcal{S}$	$\overset{\text{inversion}}{\rightsquigarrow}$	$\{X = t\} \bigcup \mathcal{S}$ si t n'est pas une métavariable

Figure 2.2: Algorithme d'unification

- La substitution σ_1 donnée par l'algorithme d'unification sur $\Gamma_1 \vdash \Delta_1$ (sur le bon couple de propositions) convient.
- si celle-ci convient, que la substitution $\sigma_2 \circ \sigma_1$, avec σ_2 calculée par l'algorithme d'unification sur $\Gamma_2 \vdash \Delta_2$, encore une fois sur le bon couple de propositions, convient.
- etc, etc ...

La réponse est bien sûr oui, mais cela n'est pas évident. Pour ce faire, on doit prouver le résultat suivant:

Théorème 2 (L'unification donne un mgu (*most general unifier*)) *Si τ est un unificateur des séquents $\Gamma_1 \vdash \Delta_1$, ..., $\Gamma_n \vdash \Delta_n$, alors l'algorithme d'unification appliqué:*

- *à $\Gamma_1 \vdash \Delta_1$ (sur le bon couple de proposition) réussit et donne σ_1,*
- *à $\sigma_1\Gamma_2 \vdash \sigma_1\Delta_2$ (sur le bon couple de propositions réussit et donne σ_2,*
- $\cdots$
- *à $(\sigma_{n-1} \circ ... \circ \sigma_1)\Gamma_n \vdash (\sigma_{n-1} \circ ... \circ \sigma_1)\Delta_n$ réussit et donne σ_n.*

De plus, la substitution $\sigma = \sigma_n \circ \cdots \circ \sigma_1$ obtenue est une généralisation de τ, c'est à dire que $\tau = \tau' \circ \sigma$.

Preuve. De manière plus concrète, on doit prouver que si τ est une solution du système d'équations $\mathcal{S}_1$ alors σ, qui est la substitution calculée par l'algorithme d'unification est une généralisation de τ (de la même manière que précédemment). □

Note sur le choix du bon couple de propositions: comme on ne le connaît pas a priori, on est obligé de tester tous les couples possibles (récursivement).

2.3.3 Gestion de la contraction

Essayons de démontrer la proposition $\vdash \exists x(P(x) \Rightarrow P(f(x)))$ sans utiliser la règle de contraction. On obtient le schéma de preuve suivant:

$$\dfrac{\dfrac{P(X) \vdash P(f(X))}{\vdash P(X) \Rightarrow P(f(X))}\,\Rightarrow\text{-d}}{\vdash \exists x(P(x) \Rightarrow P(f(x)))}\,\exists\text{-d}$$

Mais on ne peut pas transformer ce schéma en démonstration du calcul des séquents, car on ne peut pas unifier $P(X)$ et $P(f(X))$.

Pourtant, on peut avoir la preuve informelle de cette proposition: soit a une constante quelconque. Soit $P(f(a))$ est vraie, donc l'implication $P(a) \Rightarrow P(f(a))$ est vraie. Soit $P(f(a))$ est fausse, et on ne peut pas en dire autant (à moins que $P(a)$ soit fausse, mais on n'en sait rien). Maaaais, dans ce cas, $P(f(a)) \Rightarrow P(f(f(a)))$ est vraie. On a donc besoin d'instancier *deux* fois la proposition $\exists x(P(x) \Rightarrow P(f(x)))$, pour se tirer d'affaire.

En calcul des séquents on doit donc utiliser la règle de contraction, avant d'appliquer la règle $\exists$-droite:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(X_1), P(X_2) \vdash P(f(X_1)), P(f(X_2))}{P(X_1) \vdash P(f(X_1)), P(X_2) \Rightarrow P(f(X_2))}\,\Rightarrow\text{-d}}{\vdash P(X_1) \Rightarrow P(f(X_1)), P(X_2) \Rightarrow P(f(X_2))}\,\Rightarrow\text{-d}}{\vdash P(X_1) \Rightarrow P(f(X_1)), \exists x(P(x) \Rightarrow P(f(x)))}\,\exists\text{-d}}{\vdash \exists x(P(x) \Rightarrow P(f(x))), \exists x(P(x) \Rightarrow P(f(x)))}\,\exists\text{-d}}{\vdash \exists x(P(x) \Rightarrow P(f(x)))}\,\text{contraction}$$

Ce schéma de preuve est, lui, unifiable (on doit prendre soit $X_1 = f(X_2)$ et X_2 quelconque, soit $X_2 = f(X_1)$ et X_1 quelconque). Notons au passage qu'il est très important de prendre deux meta-variables $X_1 \neq X_2$, sinon l'unification serait toujours impossible.

On peut montrer:

- que certaines démonstrations peuvent nécessiter de contracter 3 fois, 4 fois, ..., n fois une proposition quantifiée existentiellement à droite.
- qu'on a besoin de la règle de contraction uniquement sur les propositions quantifiées universellement à gauche et existentiellement à droite.
- que les règles restent toujours inversibles: si on a une démonstration du séquent $\Gamma \vdash P, \Delta$ alors (si P n'est pas un atome), il existe une démonstration de ce séquent qui commence par une règle sur P.
- dans le cas précédent, si $P = \exists xQ$, alors la règle sur P est en fait une suite de règles de contraction, suivie du même nombre de règles $\exists$-droites.

Par exemple, si on a une démonstration de $\Gamma, \exists xQ$, alors on peut construire la démonstration suivante (n est donné par l'algorithme de construction: on ne le connaît pas a priori):

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \vdash \langle X_1/x\}Q, ..., \{X_n/x\rangle Q}\ \exists\text{-d}}{\dfrac{\vdots}{\Gamma \vdash \exists xQ, ..., \exists xQ}\ \exists\text{-d}}\ \text{contraction}}{\dfrac{\vdots}{\Gamma \vdash \exists xQ}\ \text{contraction}}}$$

Tout cet ensemble de règle peut être regroupé dans une seule règle, qui généralise la règle $\exists$-d:

$$\dfrac{\Gamma \vdash \langle X_1/x\}Q, ..., \{X_n/x\rangle Q}{\Gamma \vdash \exists xQ}\exists\text{-d}(n)$$

n est appelé la *multiplicité* de la règle $\exists$-d (n) et représente le nombre de fois que l'on contracte la proposition, avant d'appliquer les règles $\exists$-d sur ces mêmes propositions.

Encore un exemple:

$$\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a) \vdash \exists xP(x)} \quad \dfrac{P(b) \vdash P(b)}{P(b) \vdash \exists xP(x)}}{P(a) \vee P(b) \vdash \exists xP(x)}\ \exists(1)$$

Ici, la multiplicité des règles $\exists$-d est de 1. Si on essaie d'appliquer la règle $\exists$-d en premier, il nous faut cependant l'utiliser avec la multiplicité 2:

$$\dfrac{\dfrac{P(a) \vdash P(a), P(b) \qquad P(b) \vdash P(a), P(b)}{P(a) \vee P(b) \vdash P(a), P(b)}\ \exists\text{-d}}{P(a) \vee P(b) \vdash \exists xP(x)}\ (2)$$

Ainsi, lorsqu'on cherche à appliquer la règle $\exists$-d, on doit chercher à l'appliquer avec une certaine multiplicité, inconnue à l'avance. L'idée est de cherche d'abord une démonstration où toutes les règles $\exists$-d et $\forall$-g ont la multiplicité 1, puis si on n'y arrive pas, d'en chercher une où toutes ces règles ont la multiplicité 2, etc, etc.

Si nous reprenons l'exemple du début:

$$\dfrac{\dfrac{\dfrac{P(X) \vdash P(f(X))}{\vdash P(X) \Rightarrow P(f(X))}\ \Rightarrow\text{-d}}{\vdash \exists x(P(x) \Rightarrow P(f(x)))}\ \exists\text{-d}}\ (1)$$

L'algorithme d'unification échoue car X a une occurence dans $f(X)$. Cependant, nous reprenons maintenant le calcul avec toutes les règles $\exists$-d et $\forall$-g de multiplicité 2:

$$\dfrac{\dfrac{\dfrac{P(X_1), P(X_2) \vdash P(f(X_1)), P(f(X_2))}{P(X_1) \vdash P(f(X_1)), P(X_2) \Rightarrow P(f(X_2))}\ \Rightarrow\text{-d}}{\vdash P(X_1) \Rightarrow P(f(X_1)), P(X_2) \Rightarrow P(f(X_2))}\ \Rightarrow\text{-d}}{\vdash \exists x(P(x) \Rightarrow P(f(x)))}\ \exists\text{-d}}\ (2)$$

Ici, l'algorithme d'unification réussit (il trouve soit $X_1 = f(X_2)$, soit $X_2 = f(X_1)$, mais pas les deux en même temps, selon les propositions que l'on cherche à unifier).

Notons que maintenant, si un séquent n'est pas démontrable (par exemple $\vdash \exists x A(x)$), on ne le saura jamais, car l'algorithme ne termine plus.

Rappelons aussi que des résultats théoriques prouvent que c'est le meilleur résultat auquel on puisse arriver: le calcul des séquents est semi-décidable, et c'est justement à cause des règles de contraction.

Il faut donc modifier l'algorithme de recherche de preuve pour commencer à chercher d'abord des preuves de multiplicité 1, puis 2, puis 3, ... et on s'arrête quand on a trouvé une preuve.

2.4 La skolémisation

On veut maintenant rajouter tous les types de règle: il nous manque encore les règles ∀-d et ∃-g. Le problème de ces règles est qu'elles impliquent des conditions de fraîcheur sur les constantes introduites.

2.4.1 analyse du problème

Essayons de prouver (naïvement) le séquent (qui n'est pas prouvable) : $\forall y_1 \exists x_1 P(x_1, y_1) \vdash \exists x_2 \forall y_2 P(x_2, y_2)$. On obtient le schéma de démonstration suivant:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(c, Y_1) \vdash P(X_2, d)}{P(c, Y_1) \vdash \forall y_2 P(X_2, y_2)}\,\forall\text{-d}}{P(c, Y_1) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\exists\text{-d}}{\exists x_1 P(x_1, Y_1) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\exists\text{-g}}{\forall y_1 \exists x_1 P(x_1, y_1) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\forall\text{-g}$$

(Notons que l'on n'a pas de méta-variables pour ∃-g et ∀-d, puisqu'on sait très bien ce que l'on doit introduire: des constantes fraîches)

En unifiant, on obtient: $c = X_2$ et $d = Y_1$. Cela nous donnerait la "démonstration" suivante:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(c, d) \vdash P(c, d)}{P(c, d) \vdash \forall y_2 P(c, y_2)}\,\forall\text{-d}}{P(c, d) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\exists\text{-d}}{\exists x_1 P(x_1, d) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\exists\text{-g}}{\forall y_1 \exists x_1 P(x_1, y_1) \vdash \exists x_2 \forall y_2 P(x_2, y_2)}\,\forall\text{-g}$$

Or, cette démonstration ne vérifie pas la condition de fraîcheur des constantes! (lors de l'application de la règle ∀-d, on ne peut pas choisir d pour remplacer y_2, car il apparaît déjà).

Ici donc, l'unification réussit, mais ne nous donne pas une démonstration valide du calcul des séquents. Ce, à cause des conditions de fraîcheur.

Voyons un autre exemple. Tentons de démontrer le séquent (sans utiliser la règle axiome sur des formules non atomiques) suivant:

$$\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(X_1, d) \vdash P(c, Y_2)}{\exists y_1 P(X_1, y_1) \vdash P(c, Y_2)}\exists\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash P(c, Y_2)}\forall\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \exists y_2 P(c, y_2)}\exists\text{-d}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)}\forall\text{-d}$$

Cette fois-ci, on obtient après unification $c = X_1$ et $Y_2 = d$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(c, d) \vdash P(c, d)}{\exists y_1 P(c, y_1) \vdash P(c, d)}\exists\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash P(c, d)}\forall\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \exists y_2 P(c, y_2)}\exists\text{-d}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)}\forall\text{-d}$$

Ceci n'est pas une démonstration, car la condition de fraîcheur des constantes n'est toujours pas vérifiée (question: où ?).

Cependant, si on essaie le schéma de démonstration suivant:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(X_1, d) \vdash P(c, Y_2)}{P(X_1, d) \vdash \exists y_2 P(c, y_2)}\exists\text{-d}}{\exists y_1 P(X_1, y_1) \vdash \exists y_2 P(c, y_2)}\exists\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \exists y_2 P(c, y_2)}\forall\text{-g}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)}\forall\text{-d}$$

Lorsqu'on unifie, on obtient bien une démonstration du calcul des séquents. Ainsi, l'ordre des règles a une importance, et ce, à cause de la condition de fraîcheur des constantes des deux règles $\forall$-d et $\exists$-g.

Plusieurs solutions sont envisageables à ce problème:

1. Une solution très coûteuse en termes d'efficacité est d'essayer toutes les ordres de règles possibles, jusqu'à obtenir une démonstration (et si on n'y arrive pas, alors on n'a pas de démonstration). Le problème qui se rajoute à cela est le fait qu'on ne peut plus utiliser la règle $\exists$-d avec de la multiplicité, car il se peut qu'on doive intancier les copies de $\exists xQ$ pas au même instant (à cause des conditions de fraîcheur de constantes).

2. Une deuxième solution serait de mémoriser pour *chaque formule* d'un séquent l'ordre dans lesquels doivent être introduites les meta-variables, et quelle est leur précédence par rapport à l'introduction des constantes fraîches. Par exemple, dans la formule $\forall x \exists y P(x, y)$, la règle $\forall$-g doit être appliquée avant $\exists$-d, ce qui se traduira par $X < c$, avec c le nom de la constante fraîche introduite par $\exists$-d, et X la méta-variable introduite par la règle $\forall$-g (de multiplicité 1). Autrement dit: c ne *peut* pas apparaître dans X.

   L'unification, elle aussi, introduit des conditions de précédence: si on obtient $Y = d$, alors d est une constante qui doit être introduite avant Y et doit vérifier $d < Y$. De manière plus générale, si on a $Y = t$, alors toutes les constantes apparaissant dans t doivent être introduites avant Y.

   Une fois que toutes ces contraintes auront été construites, il suffit de vérifer qu'elles ne sont pas circulaires: si on a $c < X$ et $X < c$, alors l'unification doit échouer. Ce problème se ramène à la recherche d'un chemin cyclique dans un graphe: à cauqe fois que l'on a une contrainte $X < c$, on place une flèche qui part du noeud X vers le noeud c: $X \longrightarrow c$. Si le graphe construit est acyclique, alors l'algorithme d'unification a réussi.

Pour illustrer la seconde méthode, voici quelques exemples de schéma de preuve: on garde maintenant en indice de chaque proposition le nom des méta-variables qui ont été introduites. Voici un exemple de réussite (bien que les règles ne soient pas faites dans le bon ordre):

$$\dfrac{\dfrac{\dfrac{\dfrac{P(X_1, d) \vdash P(c, Y_2)}{(\exists y_1 P(X_1, y_1))^{X_1} \vdash P(c, Y_2)^{Y_2}}\ \exists\text{-g},\ X_1 < d}{(\exists y_1 P(X_1, y_1))^{X_1} \vdash \exists y_2 P(c, y_2)}\ \exists\text{-d}}{(\exists y_1 P(X_1, y_1))^{X_1} \vdash \forall x_2 \exists y_2 P(x_2, y_2)}\ \forall\text{-d}}{\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)}\ \forall\text{-g}$$

L'algorithme d'unification trouve: $X_1 = c$ et $Y_2 = d$. Ce qui induit les contraintes suivantes: $c < X_1$ et $d < Y_2$. Ainsi on obtient l'ordre suivant, qui n'est pas contradictoire:

$$c < X_1 < d < Y_2$$

Grâce à l'ordre obtenu on remet les règles dans le bon sens. Si on veut appliquer une règle de quantificateur, on vérifie auparavant que *toutes* les règles précédentes (par l'ordre que l'on a) ont bien été appliquées: on sait que c'est possible grâce à l'ordre:

- $c < X_1 = c$ introduit avant X_1: $\forall$-d doit être faite avant $\forall$-g.
- X_1 introduite avant d: $\forall$-g doit être faite avant $\exists$-g.
- $d < Y_2$: $\exists$-g doit être faite avant $\exists$-d.

Ce qui donne la démonstration suivante:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(c,d) \vdash P(c,d)}{P(c,d) \vdash \exists y_2 P(c,y_2)}\exists\text{-d}}{\exists y_1 P(c,y_1) \vdash \exists y_2 P(c,y_2)}\exists\text{-g}}{\forall x_1 \exists y_1 P(x_1,y_1) \vdash \exists y_2 P(c,y_2)}\forall\text{-g}}{\forall x_1 \exists y_1 P(x_1,y_1) \vdash \forall x_2 \exists y_2 P(x_2,y_2)}\forall\text{-d}$$

Voici maitenant un exemple d'échec:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(X,d)^X \vdash P(c,Y)^Y}{P(X,d)^Y \vdash (\forall x P(x,Y))^Y}\forall\text{-d, } Y<c}{(\exists y P(X,y))^X \vdash (\forall x P(x,Y))^Y}\exists\text{-g, } X<d}{(\exists y P(X,y))^X \vdash \exists y \forall x P(x,y)}\exists\text{-d}}{\forall x \exists y P(x,y) \vdash \exists y \forall x P(x,y)}\forall\text{-g}$$

L'unification donne: $X = c$ et $Y = d$. Ce qui se traduit par les contraintes suivantes: $c < X$ et $d < Y$. Ainsi, en rassemblant toutes les contraintes introduites, on obtient:

$$c < X < d < Y < c$$

c'est une impossibilité (il y a une circularité). Ce séquent n'a donc pas de preuve (remarque: avec la multiplicité 1, il faudrait essayer avec toutes les multiplicités possibles).

Et enfin, un exemple légèrement plus évolué:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(X,d)^X, Q(X,e)^X \vdash P(c,X')^{X',X''} \qquad P(X,d)^X, Q(X,e)^X \vdash Q(c,X'')^{X',X''}}{P(X,d)^X, Q(X,e)^X \vdash (P(c,X') \wedge Q(c,X''))^{X',X''}}\wedge\text{-d}}{P(X,d)^X, (\exists z Q(X,z))^X \vdash (P(c,X') \wedge Q(c,X''))^{X',X''}}\exists\text{-g, } X<e}{(\exists y P(X,y))^X, (\exists z Q(X,z))^X \vdash (P(c,X') \wedge Q(c,X''))^{X',X''}}\exists\text{-g, } X<d}{(\exists y P(X,y) \wedge \exists z Q(X,z))^X \vdash (P(c,X') \wedge Q(c,X''))^{X',X''}}\wedge\text{-g}}{\forall x(\exists y P(x,y) \wedge \exists z Q(x,z)) \vdash (P(c,X') \wedge Q(c,X''))^{X',X''}}\forall\text{-g}}{\forall x(\exists y P(x,y) \wedge \exists z Q(x,z)) \vdash \exists x''(P(c,X') \wedge Q(c,x''))^{X'}}\exists\text{-d}}{\forall x(\exists y P(x,y) \wedge \exists z Q(x,z)) \vdash \exists x' \exists x''(P(c,x') \wedge Q(c,x''))}\exists\text{-d}$$

L'unification impose $X = c$, $X' = d$ et $X'' = e$, ainsi, nous obtenons les contraintes (résolubles):

$$c < X < d < X' \qquad X < e < X''$$

Remarque: l'ordre est un ordre partiel: parfois le classement de priorité des règles de quantificateurs n'est pas total (c'est à dire que l'ordre de certaines règles n'est pas important).

2.4.2 Solution la plus simple: supprimer ces quantificateurs

Une dernière possibilité existe: ne plus avoir à appliquer les règles $\exists$ à gauche et $\forall$ à droite. Ainsi, plus de condition de fraîcheur des variables. Il faut donc supprimer tous ces quantificateurs des formules.

L'idée de cette partie est le principe suivant: si en hypothèse on a une formule $\forall x \exists y P(x, y)$ (l'intuition est que cette formule est *vraie*) il est équivalent de dire qu'on a une fonction f telle que $\forall x P(x, f(x))$ est vraie aussi.

Une restriction cependant: le nom f de la fonction doit être *frais* (sinon, on se met sur les bras des hypothèses supplémentaires sur la fonction f). f est appelé un symbole de Skolem.

Par exemple, si on prend le prédicat $\forall x \exists y (x + y = 0)$, alors sa forme skolémisée sera $\forall x (x + f(x) = 0)$, et f représente intuitivement la fonction qui a x associe son opposée $-x$[1]. Si d'autre part on skolémise $\forall x \exists y (x + x = y)$, cela donne $\forall x (x + x = g(x))$. Intuitivement, g est la fonction qui à x associe $2 * x$. On voit donc qu'il faut prendre pour g un nouveau symbole, et non pas f comme précédemment.

La dernière remarque est que f est une fonction qui dépend de *toutes* les variables quantifiées universellement qui sont situées à un niveau supérieur. Voyons le sur les exemples suivants:

$$\begin{aligned} \forall x_1 \exists y \forall x_2 P(x_1, y, x_2) &\xrightarrow{sko} \forall x_1 \forall x_2 P(x_1, f(x_1), x_2) \\ \exists x \forall y P(x, y) &\xrightarrow{sko} \forall y P(c, y) \\ \forall x_1 \forall x_2 \exists y P(x_1, y, x_2) &\xrightarrow{sko} \forall x_1 \forall x_2 P(x_1, f(x_1, x_2), x_2) \end{aligned}$$

2.4.3 La mise en forme prénexe

Avant de commencer à skolémiser toutes les formules, il faut les transformer un peu, de manière à ce que tous les quantificateurs soient en tête de la proposition:

Définition 5 (Forme prénexe) *Une formule P est en* forme prénexe *si et seulement si elle est de la forme:*

$$\forall x_1^1 ... \forall x_{n_1}^1 \exists y_1^1 ... \exists y_{m_1}^1 ... \forall x_1^p ... \forall x_{n_p}^p \exists y_1^p ... \exists y_{m_p}^p Q$$

où Q est une formule sans quantificateurs.

L'alternance des quantificateurs est purement arbitraire: la formule pourrait très bien commencer par $\exists$, terminer par $\forall$, etc.

Il est possible de transformer n'importe quelle formule P en une formule en forme prénexe qui est *équivalente*. Les règles de transformation sont les

[1] à condition d'avoir tous les axiomes concernant l'égalité et le signe + en hypothèse

suivantes:

$$\begin{aligned}
(\forall x P) \vee Q \text{ ou } Q \vee \forall x P &\xrightarrow{pre} \forall x (P \vee Q) \\
(\forall x P) \wedge Q \text{ ou } Q \wedge \forall x P &\xrightarrow{pre} \forall x (P \wedge Q) \\
(\forall x P) \Rightarrow Q &\xrightarrow{pre} \exists x (P \Rightarrow Q) \\
Q \Rightarrow (\forall x P) &\xrightarrow{pre} \forall x (Q \Rightarrow P) \\
\neg(\forall x P) &\xrightarrow{pre} \exists x (\neg P)
\end{aligned}$$

Les règles qui concernent le quantificateur existentiel ont été ignorées: ce sont absolument les mêmes.

Lorsqu'on ne peut plus appliquer les règles de transformation, on a obtenu une proposition en forme prénexe.

Une remarque très importante: il est crucial d'avoir à chaque fois des noms de variable différents, sinon on court à la catastrophe: la forme prénexe de $(\exists x((x = 0)) \wedge (\exists x(x = 1))$ n'est PAS $\exists x \exists x((x = 0) \wedge (x = 1))$! Il faut commencer par renommer une des deux variables pour obtenir la proposition $(\exists x(x = 0)) \wedge (\exists y(y = 0))$ puis skolémiser ensuite pour obtenir $\exists x \exists y((x = 0) \wedge (y = 1))$, ce qui est la bonne forme prénexe. Vous pourrez vous intéresser à ce problème (dit α-conversion, ou équivalence alphabétique) dans un second temps, car ce n'est pas le point central de l'algorithme.

En d'autres termes, il faut absolument que x n'apparaisse pas (en tant que variable libre) dans Q si on veut appliquer l'algorithme sur $(\forall x P) \wedge Q$. Sinon, il faut renommer x en une nouvelle variable.

2.4.4 La mise en forme de Skolem

Une fois qu'on a une formule en forme prénexe, il est aisé de la mettre en forme de Skolem (faire la skolémisation) (à condition, bien sûr de choisir avec soin les noms des fonctions, puisqu'il faut qu'ils soient tous différents).

Un détail qui a son importance: pour les formules en conclusion d'un séquent, la skolémisation se fait "à l'envers", c'est à dire que c'est les quantificateurs universels $\forall$ que l'on fait disparaître. En effet, $\forall$ à gauche est le dual de $\exists$ à droite, de même pour $\wedge$ et $\vee$: les règles sont exactement les même, mais dans un cas se passent à droite, et dans l'autre, à gauche.

Ainsi, pour les formules situées à *gauche*, l'algorithme de skolémisation sera:

Définition 6 (Skolémisation à gauche)

$$\forall x_1 ... \forall x_n \exists y P \xrightarrow{sko} \forall x_1 ... \forall x_n (\langle f(x_1, ..., x_n)/y \rangle P)$$

où f est un symbole de fonction frais.

Alors que pour les formules situées à *droite*, l'algorithme de Skolémisation sera:

Définition 7 (Skolémisation à droite)

$$\exists x_1 ... \exists x_n \forall y P \xrightarrow{sko} \exists x_1 ... \exists x_n (\langle f(x_1, ..., x_n)/y \rangle P)$$

où f est un symbole de fonction frais.

Essayons par exemple de trouver la forme skolémisée du séquent $\forall x_1 \exists y_1 P(x_1, y_1) \vdash \forall x_2 \exists y_2 P(x_2, y_2)$. Il s'agit du séquent:

$$\forall x_2 P(x_2, f(x_2)) \vdash \exists y_2 P(c, y_2)$$

avec f et c des symboles de fonction frais à une et zéro variables (c est donc une constante).

Prouvons maintenant ce dernier séquent (on connaît déjà une preuve de ce séquent dans sa forme non skolémisée):

$$\dfrac{\dfrac{P(X_2, f(X_2)) \vdash P(c, Y_2)}{P(X_2, f(X_2)) \vdash \exists y_2 P(c, y_2)} \exists\text{-d}}{\forall x_2 P(x_2, f(x_2)) \vdash \exists y_2 P(c, y_2)} \forall\text{-g}$$

et l'algorithme d'unification nous donne $X_2 = x$ et $Y_2 = f(c)$. On a donc aussi une preuve du séquent skolémisé, ce qui est plutôt rassurant. Enfin, essayons de prouver le principe des buveurs:

Dans un bar, il existe une personne qui, si elle boit, alors tout le monde boit.

Ce principe, qui peut paraître paradoxal, a la preuve suivante (qui fait appel au tiers-exclu): dans ce bar, soit tout le monde boit, soit au moins une personne ne boit pas. Si tout le monde boit, alors on peut choisir n'importe qui, ainsi, la phrase est juste. Si au moins une personne ne boit pas, alors on choisit cette personne-ci, et puisqu'elle ne boit pas, la phrase est encore juste.

Rappelons que l'utilisation du tiers-exclu (on a soit A soit $\neg A$), est fortement lié à la possibilité de contracter les propositions situées à *droite* dans un séquent.

La proposition à démontrer est la suivante:

$$\exists x (B(x) \Rightarrow \forall y B(y))$$

Sa fome prénexe est:

$$\exists x \forall y (B(x) \Rightarrow B(y))$$

Comme on doit démontrer le séquent $\vdash \exists x \forall y (B(x) \Rightarrow B(y))$, la forme de Skolem en est:

$$\vdash \exists x (P(x) \Rightarrow P(f(x)))$$

C'est un séquent que nous avons beaucoup étudié à la section 2.3.3 et dont nous connaissons la preuve par cœur.

2.4.5 Équiprouvabilité, complexité

Une chose reste à savoir: si l'on a une preuve de la forme skolémisée de $\Gamma \vdash \Delta$, peut-on pour autant construire une preuve de $\Gamma \vdash \Delta$?

Encore une fois, des résultats théoriques nous affirment que les séquents suivants sont équiprouvables: si l'un l'est, alors les autres le sont (et on est capable de reconstruire une preuve de l'un à partir d'une preuve de l'autre).

$\frac{\pi}{\Gamma_{sk} \vdash \Delta_{sk}}$ $\frac{\pi'}{\Gamma_{pre} \vdash \Delta_{pre}}$ $\frac{\pi''}{\Gamma \vdash \Delta}$

Nous venons de voir trois algorithmes de recherche de preuve en calcul des séquents:

- L'un essaie toutes les combinaisons de règles de quantificateur possible.
- L'autre les fait dans un ordre quelconque, en mémorisant les contraintes associées.
- Le dernier enfin, commence par transformer un séquent dans sa forme prénexe skolémisée, puis n'applique plus les règles $\forall$-d et $\exists$-g.

La première méthode est beaucoup moins efficace que les deux dernières. En effet, dès lors qu'on a une énumération de combinaisons, cela revient à rajouter une complexité exponentielle.

Les deux méthodes suivantes sont de complexité équivalentes. Néanmoins la dernière est en général préférée dans les prouveurs "de compétition", car la règle de skolémisation peut être améliorée de multiples façons (qui ne sont toutefois pas toujours très claires).

2.5 Poser des questions

La dernière étape de notre programme de recherche de preuve est la suivante: nous aimerions lui "poser des question", comme à un système expert. Autrement dit, si nous devons démontrer $\Gamma \vdash \exists x P$, nous aimerions bien connaître le témoin existentiel t correspondant, tel que $\Gamma \vdash \langle t/x \rangle P$.

Premièrement, notons que ce n'est pas toujours possible: on ne peut trouver de témoin ni pour le séquent $\exists x A(x) \vdash \exists x A(x)$, ni pour le séquent $\vdash \exists x (B(x) \Rightarrow B(f(x)))$ (à cause de la règle de contraction).

Néanmoins, lorsqu'un témoin existe, on peut essayer de le faire apparaître de la manière suivante: si on a une preuve de $\Gamma \vdash \exists x P$, on permute les règles de manière à avoir une démonstration de cette forme:

$$\dfrac{\dfrac{\pi}{\Gamma \vdash \langle t/x \rangle P}}{\Gamma \vdash \exists x P}\ \exists\text{-d}$$

Dans notre algorithme cependant, nous commençons par introduire des méta-variables, puis nous effectuons l'unification. Nous aurons donc le schéma suivant:

$$\dfrac{\dfrac{\dfrac{\Gamma_1 \vdash \Delta_1 ... \Gamma_n \vdash \Delta_n}{\vdots}\ \text{axiome (unificateur } \sigma)}{\Gamma \vdash \langle X/x \rangle P}}{\Gamma \vdash \exists x P}\ \exists\text{-d}$$

Il nous suffira donc, lors de l'unification, d'extraire en plus le terme par lequel on doit substituer X, soit σX. Mais comment peut-on le savoir ? L'idée est de chercher directement une démonstration de $\Gamma \vdash \langle X/x \rangle P$. La présence d'une métavariable indique que l'on s'intéresse à l'obtention du témoin. Par exemple on peut chercher une démonstration du séquent suivant:

$$\begin{array}{rl} Pere(\text{Charlemagne}, \text{Pepin le bref}), & \\ Pere(\text{Pepin le bref}, \text{Charles Martel}) & \\ \forall x \forall y \forall z((Pere(x,y) \wedge Pere(y,z)) \Rightarrow GrandPere(x,z)) & \vdash \\ & GrandPere(\text{Charlemagne}, X) \end{array}$$

Les hypothèse composent ce que l'on pourrait appeler:

- La base de données: $Pere(\text{Charlemagne}, \text{Pepin le bref})$, $Pere(\text{Pepin le bref}, \text{Charles Martel})$.
- Les définitions: $\forall x \forall y \forall z((Pere(x,y) \wedge Pere(y,z)) \Rightarrow GrandPere(x,z))$.

Et la conclusion forme la "requête", la question que l'on pose au système, qui bien que ne sachant pas qui est le grand-père de qui, trouve la bonne réponse.

Cette séparation a plusieurs avantages. Tout d'abord, la base de donnée est moins grosse: au lieu d'avoir des couples pour toutes les relations de parenté entre les personnes, nous avons maintenant seulement les relations de filiation directe. Cela induit des bases de données plus petites, plus sûres: si Pépin le Bref est en fait le fils de Robert le Fort, on n'a pas besoin de modifier le nom du grand-père de Charlemagne, de même si on veut ajouter que Pépin le jeune est le père de Charles Martel. Deuxièmement, les règles de déduction peuvent elles aussi changer en fonction de la connaissance que nous avons (par exemple, on peut apprendre que la bru est la femme du fils, et rajouter cette définition dans la base de données).

2.6 Quelques exercices

2.6.1 Preuves en calcul des séquents

Prouver les séquents suivants (sans utiliser ni méta-variables, ni skolémisation):

$$\exists y \forall x P(x,y) \vdash \forall x \exists y P(x,y)$$
$$\vdash \exists x (B(x) \Rightarrow \forall y B(y))$$
$$B, A, (A \vee B) \wedge (B \Rightarrow \neg A) \vdash$$

2.6.2 Unification

Unifier les systèmes d'équations suivants:

$\{X = f_1(Y), g_1(Y) = g_2(X)\}$
$\{f_1(X_1, c) = f_1(c, X_1), g_1(d, X_1) = g_1(X_2, X_3), h_1(X_2) = c\}$
$\{f_1(X_1, c) = f_1(c, X_1), g_1(d, X_1) = g_1(X_2, X_3), h_1(X_2) = X_4\}$
$\{f_1(X_1, c) = f_1(c, X_1), g_1(f_1(X_3), X_1) = g_1(X_2, X_3), h_1(e, X_2) = h_1(X_4, g_1(X_1))\}$

2.6.3 Mise en forme prénexe puis de Skolem

Mettre en forme prénexe, puis de Skolem:

$\forall x_1(A \vee (\exists x_2(B(x_1, x_2) \Rightarrow \forall x_3 C))) \vdash$
$((\forall x_1 A) \Rightarrow (\exists x_2 \forall x_3 P(x_2, x_3))) \vdash ((\forall x_4 \exists x_5 P(x_4, x_5)) \Rightarrow B) \Rightarrow (\forall x_6 \exists x_7 \exists x_8 \forall x_9 Q(x_6, x_7, x_8, x_9))$
$\forall x \exists y \exists z P(x, y) \vdash (\exists x A) \wedge \forall y B(y)$