La théorie de la démonstration

- Objectif : formaliser les *objets* que manipulent les mathématiciens et les *démonstrations* qu'ils font
- Les objets :
  - Ils énoncent des assertions mathématiques (des conjectures) qu'ils cherchent à démontrer
  - Au cours de la démonstration on peut être amené à introduire des hypothèses. Ainsi l'objet d'une démonstration devient un énoncé P conjecturé sous certaines hypothèses H_1, H_2 … H_n
  - On représente une telle conjecture par un séquent composé d'énoncés :

$$H_1, H_2 \ldots H_n \vdash P$$

les énoncés hypothèses *l'énoncé conclusion*

La théorie de la démonstration

- Les raisonnements :
  - Ils réalisent des démonstrations en enchainant des pas élémentaires de raisonnement permettant de passer d'un *séquent* à l'autre
  - Ces pas élémentaires peuvent être **schématisés** en quelques types élémentaires de raisonnement formalisés par des règles d'inférence composées de séquents :

*Les (schémas) séquents **antécédents***

$$\frac{S_1 \quad S_2 \quad \ldots \quad S_n}{S}\ R_i$$

← *Le nom de la règle*

*Le (schéma) **conséquent***

La théorie de la démonstration

- Les séquents peuvent ne pas avoir d'hypothèses, ils représentent donc des propriétés assertées sans aucune condition (quand ils sont démontrés, on parle de tautologie)

$$\vdash P$$

- Les règles d'inférence peuvent n'avoir aucun antécédent, elles représentent donc des énoncés considérés comme toujours démontrés, on les appelle des axiomes.

$$\frac{}{H_1, H_2 \ldots H_n \vdash P}\ \text{Ax}$$

- Un séquent que l'on peut produire (à partir des axiomes) en utilisant les règles d'inférences est appelé un théorème, il représente une **conjecture démontrée**. L'enchainement des règles ayant permis leur production constitue une preuve de ce théorème.
  - Remarque : tout séquent *correspondant* à un axiome est donc un théorème !

La théorie de la démonstration

- Dans ce cadre, une théorie mathématique est composée :
  - D'un langage formel définissant l'ensemble des énoncés (ou formules) syntaxiquement corrects
  - D'un ensemble de règles d'inférences définies pour ces énoncés définissant l'ensemble des pas élémentaires de raisonnement admis dans cette théorie

- Ces deux éléments définissent l'ensemble des théorèmes de cette théorie
  - *Remarque : Il faut au moins un axiome pour produire des théorèmes*

Un système à la Hilbert (début XX^{e}) pour les fbf n'utilisant que $\wedge, \Rightarrow$

- Un système de déduction dont les séquents n'ont pas d'antécédent composé de 4 règles (3 sont axiomes) dont les énoncés sont des fbf :

$$\frac{}{\vdash P \Rightarrow (Q \Rightarrow P)}\ \text{Ax1} \qquad \frac{}{\vdash (P \Rightarrow Q \Rightarrow R) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))}\ \text{Ax2}$$

$$\frac{}{\vdash (\neg P \Rightarrow \neg Q) \Rightarrow (Q \Rightarrow P)}\ \text{Ax3} \qquad \frac{\vdash P \qquad \vdash (P \Rightarrow Q)}{\vdash Q}\ \text{MP}$$

  - L'axiome 1 signifie : *soit P et Q deux formules bien formées quelconques de la LP, le séquent* $\vdash (P \Rightarrow (Q \Rightarrow P))$ *est un théorème.*
    - *Ex. :* $\vdash a \Rightarrow (a \Rightarrow a)$ *avec* $P=Q=a$

Utilisation d'une règle d'inférence

- Une règle peut s'utiliser de deux manières : $\dfrac{\vdash P \qquad \vdash (P \Rightarrow Q)}{\vdash Q}$ MP

1. En **analyse** (de bas en haut) : pour prouver la conclusion il faut prouver les antécédents
   - Pour la règle **M**odus **P**onens cela signifie : soit P et Q deux fbf quelconques de la LP, pour prouver le séquent $\vdash Q$ par utilisation de la règle MP, il faut prouver les séquents $\vdash P$ et $\vdash (P \Rightarrow Q)$
   - Exemple : *pour prouver* $\vdash a \Rightarrow b$ *par MP,*
     il suffit d'avoir une preuve de $\vdash (a \Rightarrow \neg c)$ *et* $\vdash (a \Rightarrow \neg c) \Rightarrow (a \Rightarrow b)$
     …*ou n'importe quel autre couple de séquent de la forme* $\vdash P$ et $\vdash P \Rightarrow (a \Rightarrow b)$

2. En **synthèse** (de haut en bas) : si les antécédents sont prouvés alors la conclusion est prouvée.
   - Sur MP : si les séquents $\vdash P$ et $\vdash (P \Rightarrow Q)$ sont des théorèmes alors le séquent $\vdash Q$ est un théorème.
   - Exemple : *les séquents* $\vdash a \Rightarrow (a \Rightarrow a)$ *et*
     $\vdash (a \Rightarrow (a \Rightarrow a)) \Rightarrow ((a \Rightarrow a) \Rightarrow (a \Rightarrow a))$ *sont des théorèmes donc* $\vdash (a \Rightarrow a) \Rightarrow (a \Rightarrow a)$ *est un théorème*

Application

- Démontrons que $\vdash a \Rightarrow a$ est un théorème
- Recherche d'une preuve :
  1. $\vdash a \Rightarrow a$ *ne correspond pas à un schéma d'axiome*
  2. *Donc la seule possibilité est d'utiliser MP*
  3. *Il faut donc identifier une formule* ***P*** *et démontrer :*
     4. *D'une part :* $\vdash \boldsymbol{P}$
     5. *Et d'autre part :* $\vdash \boldsymbol{P} \Rightarrow (a \Rightarrow a)$

Une démonstration de ⊢ a⇒a

$$\dfrac{\dfrac{}{\vdash a \Rightarrow ((a \Rightarrow a) \Rightarrow a)}\,\text{Ax1}\;[P=a, Q=a\Rightarrow a] \qquad \dfrac{}{\vdash (a \Rightarrow ((a \Rightarrow a) \Rightarrow a)) \Rightarrow ((a \Rightarrow (a \Rightarrow a)) \Rightarrow (a \Rightarrow a))}\,\text{Ax2}\;[P=R=a, Q=a\Rightarrow a]}{\dfrac{\dfrac{}{\vdash a \Rightarrow (a \Rightarrow a)}\,\text{Ax1}\;[P=a, Q=a] \qquad \dfrac{}{\vdash (a \Rightarrow (a \Rightarrow a)) \Rightarrow (a \Rightarrow a)}\,\text{MP}\;[P=a\Rightarrow((a\Rightarrow a)\Rightarrow a),\ Q=(a\Rightarrow(a\Rightarrow a)) \Rightarrow (a\Rightarrow a)}}{\vdash a \Rightarrow a}\,\text{MP}\;[P=a\Rightarrow(a\Rightarrow a),\ Q=a\Rightarrow a]}$$

Propriété du système formel de Hilbert

- **Propriété** : Le système formel de Hilbert produit toutes les formules valides de la logique des propositions :

  pour toute fbf F : $\vdash$ ***F est démontrable ssi F est valide***

  - On dit que ce système formel est adéquat et complet vis à vis de la sémantique formelle de la logique

- Hilbert introduit de plus un système de déduction sous hypothèse et démontre via le théorème de déduction la complétude de son système.
  - Cette notion de déduction sous hypothèse est repris de manière plus simple par Gentzen dans la déduction naturelle, puis dans le calcul des séquents.

La déduction naturelle (G. Gentzen 1934)

1. Permettre la représentation d'énoncé sous hypothèses
   ➔ Les séquents peuvent avoir des hypothèses

2. Rendre ***naturelle*** l'exploitation des connecteurs logiques en donnant pour chaque connecteur des règles d'introduction et d'élimination des connecteurs
   - Exemple du connecteur ⇒

$$\frac{\Gamma, P \vdash Q}{\Gamma \vdash (P \Rightarrow Q)} \Rightarrow_i \qquad \frac{\Gamma \vdash (P \Rightarrow Q) \quad \Gamma \vdash P}{\Gamma \vdash Q} \Rightarrow_e$$

Ici les lettres latines représentent des fbf et les lettres grecques des ensembles de fbf

3. Un unique axiome représentant « une démonstration sous hypothèse triviale »

$$\frac{}{\Gamma, P \vdash P} \text{ ax}$$

4. Pour des raisons techniques, il en propose une version plus symétrique (mais moins naturelle !) : le calcul des séquents. Ce système est très adapté à la démonstration automatique.

Le calcul des séquents ou Système LK (“**k**lassische Prädikaten**l**ogik”)

- *Les séquents peuvent avoir plusieurs conclusions :*

$$H_1, H_2 \ldots H_n \vdash C_1, C_2 \ldots C_k$$

les énoncés hypothèses *les énoncés conclusion*

- ***Attention***
  - *Un même énoncé peut être présent plusieurs fois dans l’hypothèse ou dans la conclusion*
  - *Les énoncés de l’hypothèse sont interprétés comme une **conjonction** de formules ➔ Si n=0 alors cela correspond à une hypothèse toujours vraie*
  - *Les énoncés de la conclusion sont interprétés comme une **disjonction** de formules ➔ Si k=0 alors cela correspond à une conclusion toujours fausse*

Les règles du système LK_0

$$\frac{}{\Gamma, P \vdash \Delta, P}\ ax \qquad \frac{}{\Gamma \vdash \Delta, \top}\ \top_d$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot_g \qquad \frac{\Gamma \vdash P \quad \Gamma, P \vdash Q}{\Gamma \vdash Q}\ cut$$

$$\frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\ cont_g \qquad \frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\ cont_d$$

Les règles du système LK_0

$$\frac{\Gamma \vdash \Delta, P}{\Gamma, \neg P \vdash \Delta}\ \neg_g \qquad \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \Delta, \neg P}\ \neg_d$$

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge_g \qquad \frac{\Gamma \vdash \Delta, P \quad \Gamma \vdash \Delta, Q}{\Gamma \vdash \Delta, P \wedge Q}\ \wedge_d$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}\ \vee_g \qquad \frac{\Gamma \vdash \Delta, P, Q}{\Gamma \vdash \Delta, P \vee Q}\ \vee_d$$

Les règles du système LK_0

$$\frac{\Gamma \vdash \Delta, P \qquad \Gamma, Q \vdash \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta} \Rightarrow_g$$

$$\frac{\Gamma, P \vdash \Delta, Q}{\Gamma \vdash \Delta, P \Rightarrow Q} \Rightarrow_d$$

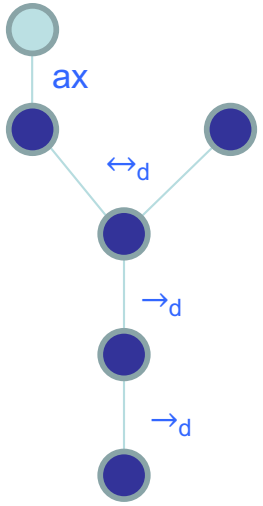
$$\frac{\Gamma \vdash \Delta, P, Q \qquad \Gamma, P, Q \vdash \Delta}{\Gamma, P \Leftrightarrow Q \vdash \Delta} \leftrightarrow_g$$

$$\frac{\Gamma, P \vdash \Delta, Q \qquad \Gamma, Q \vdash \Delta, P}{\Gamma \vdash \Delta, P \Leftrightarrow Q} \leftrightarrow_d$$

Démonstration d'un séquent s dans le système LK_0

- Une démonstration est un **arbre** dont la racine (que l'on met en bas) est le séquent s à prouver et dont chaque nœud est obtenu (en remontant dans l'arbre) par application des règles précédentes.

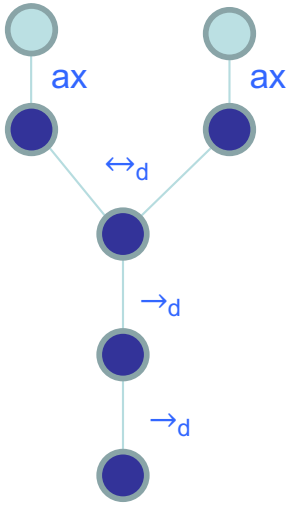
$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash q, p, q}\,\text{ax} \qquad \dfrac{}{p, p, q \vdash q}\,\text{ax}}{p \leftrightarrow q, p \vdash q}\leftrightarrow_{\text{g}}}{p \leftrightarrow q \vdash p \rightarrow q}\rightarrow_{\text{d}}}{\vdash (p \leftrightarrow q) \rightarrow (p \rightarrow q)}\rightarrow_{\text{d}}$$



Théorème = Séquent s démontré

- Si **toutes les feuilles** de l'arbre (en haut) correspondent à des nœuds vides obtenus par une règle axiomatique alors s **le séquent racine est démontré** (et aussi tous les séquents de l'arbre sont démontrés).

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \vdash q, p, q}\,\text{ax} \qquad \dfrac{}{p, p, q \vdash q}\,\text{ax}}{p \leftrightarrow q, p \vdash q}\,\leftrightarrow_{\text{g}}}{p \leftrightarrow q \vdash p \rightarrow q}\,\rightarrow_{\text{d}}}{\vdash (p \leftrightarrow q) \rightarrow (p \rightarrow q)}\,\rightarrow_{\text{d}}$$



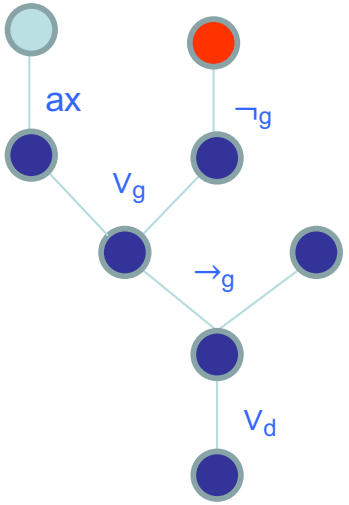
- Un séquent démontré est appelé un **théorème**
  - Ici $\vdash (\boldsymbol{p} \Leftrightarrow \boldsymbol{q}) \Rightarrow (\boldsymbol{p} \Rightarrow \boldsymbol{q})$ est un théorème

Séquent s **réfuté**

- Si (au moins) **une feuille de l'arbre** contient un séquent s_f sur lequel aucune règle de LK_0 ne peut s'appliquer alors le séquent racine s **n'est pas démontrable** (ni le séquent s_f).
  - Un tel séquent s_f ne contient que des symboles propositionnels, n'a aucun symbole commun à gauche et à droite et n'a ni ⊥ à gauche, ni T à droite.
    - si une formule possédait un connecteur alors une règle serait applicable
    - si un symbole était commun aux 2 côtés alors **ax** permettrait de conclure
    - si ⊥ ou T était dans les bonnes positions alors une règle axiomatique permettrait de conclure.

    => Il est de la forme $p_1,p_2\ldots p_m \vdash q_1,q_2\ldots q_m$ où aucun pi n'est égal à un qj

$$\dfrac{\dfrac{\dfrac{\dfrac{}{c \vdash a,b,c}\,\text{ax} \quad \dfrac{\vdash a,b,c,a}{\neg a \vdash a,b,c}\,\neg_g}{\neg a \vee c \vdash a,b,c}\,\vee_g \qquad b, \neg a \vee c \vdash a,b}{c \to b, \neg a \vee c \vdash a,b}\,\to_g}{c \to b, \neg a \vee c \vdash a \vee b}\,\vee_d$$



LK_0 permet donc de décider si un séquent est un théorème ou non

- Les règles du système LK_0 (pour la logique propositionnelle) garantissent que toute démonstration d'un séquent fini est un arbre fini
  - On ne peut pas développer infiniment un arbre de preuve à partir d'un séquent fini.

- Ainsi LK_0 permet de définir un algorithme itératif de démonstration automatique :

répéter
  si toutes les feuilles de l'arbre sont des nœuds vides alors
    retourner démontré
  sinon
    choisir une feuille non vide de l'arbre
    si aucune règle n'est applicable à cette feuille alors
      retourner réfuté
    sinon *// une règle de LK_0 est applicable sur cette feuille*
      Etendre l'arbre en appliquant la règle
fin répéter

Adéquation du système LK_0 à la sémantique de la logique

- **Théorème d'adéquation** : Le système LK_0 est **correct** et **complet** vis à vis de la sémantique de la logique des propositions

Il existe une démonstration de $H_1, H_2 \ldots H_n \vdash C_1, C_2 \ldots C_k$

SSI

$\{ H_1, H_2, \ldots H_n \} \models C_1 \vee C_2 \vee \ldots \vee C_k$

- **Remarque :** Lorsque le séquent est réfuté on peut extraire du séquent feuille sur laquelle aucune règle n'est applicable une interprétation I qui montre que la conséquence logique associée au séquent racine n'est pas établie (c'est-à-dire une interprétation qui rend vrai les hypothèses mais ne rend vrai aucune des conclusions)

  Ex. : pour $p_1,p_2 \ldots p_m \vdash q_1,q_2 \ldots q_m$ on associe $I(p_1)=I(p_2)=I(p_m)=\mathbf{1}$ *et* $I(q_1)=I(q_2)=I(q_m)=\mathbf{0}$

Correction

- **Propriété de correction :**

  Si un séquent est démontré alors ce séquent correspond à une conséquence logique

- **Pour LK_0 :**

  S'il existe une démonstration de $H_1, H_2 \ldots H_n \vdash C_1, C_2 \ldots C_k$ avec les règles de LK_0 alors $\{ H_1, H_2, \ldots H_n \} \models C_1 \vee C_2 \vee \ldots \vee C_k$

- **Preuve:**

  1. Montrons que chaque séquent d'axiome correspond bien à une conséquence logique
  2. Montrons que chaque séquent conséquent d'une règle d'inférence correspond bien à une conséquence logique si ses séquents hypothèses correspondent à des conséquences logiques
  3. Finalement montrons par induction sur la profondeur de l'arbre que si un séquent est démontré alors il correspond bien à une conséquence logique

Complétude

- **Propriété de complétude :**
  Toute conséquence logique correspond à un séquent démontrable
- **Pour LK_0 :**
  Si $\{ H_1, H_2, \ldots H_n \} \models C_1 \vee C_2 \vee \ldots \vee C_k$ ***alors il existe une démonstration de*** $H_1, H_2 \ldots H_n \vdash C_1, C_2 \ldots C_k$ ***avec les règles de*** LK_0

- **Preuve :**
  1. Réversibilité des règles d'inférence : Montrons que chaque séquent hypothèse d'une règle d'inférence correspond bien à une conséquence logique si son séquent conséquent correspond à une conséquence logique.
  2. Finalement montrons par induction sur le nombre de connecteurs des formules de $\{H_1, H_2, \ldots H_n, C_1 \vee C_2 \vee \ldots \vee C_k\}$ qu'il existe une démonstration pour le séquent associé à une conséquence logique.

Utilisation de LK en pratique

F est valide
ssi
$\vdash$ F est démontrable dans LK

F est insatisfiable
ssi
F $\vdash$ est démontrable dans LK

$\{H_1, H_2 \ldots H_n\} \models C$
ssi
$H_1, H_2 \ldots H_n \vdash C$ est démontrable dans LK