GdT Logique 2012/2013, 1ère séance introductive:

Déduction naturelle et calcul des séquents

Marc Bagnol

1er décembre 2012

L'objectif de cette séance est de présenter deux outils fondamentaux de la théorie de la démonstration, la déduction naturelle (DN) et le calcul des séquents (CS).

Ces outils ont été introduits par G. Gentzen (voir [3, 2, 4]) pour prouver des résultats de cohérence relative.

On commencera pour s'échauffer un peu par voir comment on écrit des preuves en déduction naturelle, car le système est plus facile au premier abord.
Dans un deuxième temps on regardera plus en détails le calcul des séquents, qui est l'outil dont on se servira le plus souvent dans les séances du GdT. On commencera par étudier son fonctionnement *statique*, *i.e.* comment on y écrit des preuves, puis on se penchera sur ses aspects *dynamiques*, *i.e.* comment on réécrit les preuves vers une "forme normale".

Pour aller plus loin

Cet exposé est largement inspiré des chapitres 3 et 4 du tome I du *"Point Aveugle"* [5] de J.-Y. Girard. disponible librement en anglais à l'adresse :
http://iml.univ-mrs.fr/~girard/coursang/coursang.html

Les cours d'olivier Laurent [6] (parties I, II.1, II.2) et de DiCosmo-Danos [1] (parties 1.3 à 1.5) dévraient également aider.

On pourra jeter un œil aux papiers originaux de G. Gentzen [3, 2, 4] (et même les autres du volume, après tout pourquoi pas).

Références

[1] Roberto Di Cosmo ; Vincent Danos, *The linear logic primer*, (1996), notes de cours, disponibles à l'adresse www.dicosmo.org/CourseNotes/LinLog/CorsoPisa.pdf.

[2] Gerhard Gentzen, *The consistency of elementary number theory*, The collected works of Gerhard Gentzen (Szabo, ed.), North-Holland, 1969, pp. 132 – 213.

[3] _____, *Investigations into logical déduction*, The collected works of Gerhard Gentzen (Szabo, ed.), North-Holland, 1969, pp. 68 – 131.

[4] _____, *New version of the consistency proof for elementary number theory*, The collected works of Gerhard Gentzen (Szabo, ed.), North-Holland, 1969, pp. 252 – 286.

[5] Jean-Yves Girard, *« Le Point Aveugle » – Tome I*, Hermann, 2006.

[6] Olivier Laurent, *Théorie de la démonstration*, (2008), notes de cours, disponibles à l'adresse perso.ens-lyon.fr/olivier.laurent/thdem.pdf.

1 Prélude : systèmes “à la Hilbert”

S’appuyant sur le travail du logicien G. Frege, D. Hilbert a proposé un formalisme pour les preuves mathématique qu’on appelle aujourd’hui formalisme “à la Hilbert”.

Une définition formelle de la notion de preuve mathématique était un ingrédient indispensable du programme de preuve de cohérence de Hilbert. L’idée est la suivante : on dispose d’un ensemble d’axiomes qui donne les propriétés logiques des formules qu’on manipule, et d’une règle générale, appelée *modus ponens* qui dit essentiellement que si on a prouvé A et qu’on à prouvé $A \Rightarrow B$, alors on peut en déduire B. Plus précisément :

Définition : Système de preuve à la Hilbert

> Soit $\mathscr{A}$ un ensemble de formules (les **axiomes** du système). Une **preuve** dans le système à la Hilbert muni des axiomes $\mathscr{A}$ est une suite finie de formules (F_i) telle que pour tout n l’une des deux propriétés suivantes est vérifiée :
> - $F_k \in \mathscr{A}$ (F_k est un axiome)
> - il existe $i, j < k$ tels que $F_j = (F_i \Rightarrow F_k)$ (F_k est justifiée par un *modus ponens*)

Par exemple un ensemble d’axiomes possible pour la conjonction ($\wedge$ “et”) et pour la disjonction ($\vee$ “ou”) serait :

$$A \Rightarrow (B \Rightarrow A \wedge B) \quad , \quad A \wedge B \Rightarrow A \quad , \quad A \wedge B \Rightarrow B$$

$$A \Rightarrow A \vee B \quad , \quad B \Rightarrow A \vee B \quad , \quad A \vee B \Rightarrow \big((A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow C\big)$$

Cette approche est la traduction mathématique de la méthode “axiomatique” préconisée par Hilbert. Bien que cette formalisation ouvre la possibilité de manipuler les preuves comme n’importe quel autre objet mathématique (et, par exemple, de prouver les théorèmes d’(in)complétude de Gödel), elle n’est pas sans défauts :

- si les preuves formalisées sont des objets mathématiques, se sont des objets mathématiques très peu structurés : ce sont des suites de formules avec une relation de dépendance (*modus ponens*). On aura donc du mal à travailler dessus, par exemple les preuves par récurrence buterons typiquement sur le cas *modus ponens* : on remplace la prouvabilité d’une formule B par la prouvabilité de deux formules A et $A \Rightarrow B$, dont l’une ($A \Rightarrow B$) est “plus complexe” que la formule de départ.
- les ensembles d’axiomes décrivant les propriétés d’un connecteur logique, d’une notion (être un groupe...), d’un symbole mathématique, n’ont également aucune structure. Plusieurs ensemble d’axiomes peuvent décrire de manière équivalente la même notion, sans que cette équivalence soit évidente[1]. Par conséquent, il n’est pas facile en général de voir si l’on a bien “axiomatisé” la notion que l’on cherche à formaliser. On remarquera aussi que les ensembles d’axiomes peuvent rapidement devenir assez illisibles (*c.f.* le troisième axiome pour le connecteur $\vee$).

Vous avez déjà entendu parler de G. Gentzen. Son projet en logique se place dans la continuité du programme de Hilbert, revu à la baisse suite aux résultats d’incomplétude de K. Gödel. Pour résumer : il s’agit pour lui de prouver que le principe d’induction ordinale plus ou moins fort (selon jusqu’à quel ordinal l’induction peut être faite) suffit à prouver la cohérence.

Pour réaliser ce programme, il va mettre en place deux outils qui auront une grande postérité en logique (surtout le deuxième) : la déduction naturelle et le calcul des séquents. On va voir que ces systèmes répondent en partie aux deux critiques des systèmes à la Hilbert posées plus haut.

2 La déduction naturelle, survol

Commençons par un rapide tour d’horizon du premier de ces deux systèmes : la déduction naturelle. Pour certaines logiques (en particulier la logique intuitionniste, avec les seuls connecteurs $\Rightarrow$ et $\wedge$)

1. Exercice : prouver que si A est muni d’une loi de composition associative $\bullet$ telle que $\forall x \exists! y \,.\, x \bullet y \bullet x = x$, alors $(A, \bullet)$ est un groupe. La formule logique ci-dessus (plus l’associativité) est donc une axiomatisation des groupes.

ce système est d'une grande facilité d'utilisation. Il sera donc un bon premier contact avec un système de preuve formel pour celles et ceux qui n'en n'ont jamais manipulé.

Ceci dit, on passera relativement rapidement dessus pour plusieurs raisons :
- le traitement de la logique classique dans ce système est délicat, pour dire le moins
- dès qu'on sort du fragment $(\Rightarrow, \wedge)$ intuitionniste, le système perd une bonne partie de sa simplicité
- le calcul des séquents sera un outil central dans une grande partie des exposés du GdT, et permettra d'introduire plus naturellement la logique linéaire, qui en est un des thèmes importants

Voyons tout de même comment ça marche.

On tacklait dans la partie précédent le manque de structure des systèmes de preuve à la Hilbert. Dans ces systèmes, le seul élément qui imposait un peu de contraintes (dans ce monde d'axiomes) était la *règle* de déduction, le *modus ponens*. On pourrait formuler un slogan anachronique de Hilbert : *« beaucoup d'axiomes, peu de règles »*.

Pour mettre un peu d'ordre là dedans, l'idée va être de renverser ce slogan, *« beaucoup de règles, peu d'axiomes »*. On va représenter les preuves par des arbres

$$\begin{array}{c} H_1\ [H_2]\ H_3\ \dots\ H_n \\ \ddots\ \ \vdots\ \ \iddots \\ C \end{array}$$

dont les feuilles sont des formules (les *hypothèses*), la racine est une formule (la *conclusion*) et les nœuds sont des application de règles de déduction (comme le *modus ponens*, mais on va en ajouter d'autres).

De plus les hypothèses peuvent être *actives* ou *inactives*, dans le deuxième cas on notera l'hypothèse entre crochets $[H]$.

L'idée derrière cette présentation est qu'un arbre avec hypothèses $H_1, [H_2], H_3, \dots, H_n$ et conclusion C est moralement une preuve de « $H_1 \wedge H_3 \cdots \wedge H_n \Rightarrow C$ », *i.e.* la conjonction des hypothèses *actives* implique la conclusion.

Il y a un cas de base : on *pose une hypothèse* H, qui est à la fois racine (conclusion) et feuille (hypothèse) de l'arbre de preuve (qui n'a pas de nœuds, on n'a appliqué aucune règle logique).

Voyons quelques exemples de règles pour des connecteurs logiques, cela nous permettra de manipuler un peu le système sur quelques exemples.
Pour un connecteur logique donné, on distingue deux types de règles : les règles d'*introduction* qui font apparaître le connecteur en question et les règles d'*élimination* qui le font disparaître.

Pour les connecteurs $\wedge$ et $\Rightarrow$, ça donne

$$\frac{\begin{array}{cc} \vdots & \vdots \\ A & B \end{array}}{A \wedge B}\ (\wedge\text{-i}) \qquad \frac{\begin{array}{c} \vdots \\ A \wedge B \end{array}}{A}\ (\wedge\text{-e}) \qquad \frac{\begin{array}{cc} \vdots & \vdots \\ A & A \Rightarrow B \end{array}}{B}\ (\Rightarrow\text{-e}) \qquad \frac{\begin{array}{c} [A]\ A\ \dots\ [A]\ [A] \\ \ddots\ \ \vdots\ \ \iddots \\ B \end{array}}{A \Rightarrow B}\ (\Rightarrow\text{-i})$$

Dans la dernière règle, en même temps qu'on introduit le connecteur $\Rightarrow$ on *désactive* un nombre arbitraire d'hypotèses correspondant à la formule à gauche de la flèche : toutes les hypothèses, une partie d'entre elles, ou bien... aucune (voir les exemples).
Un point dont l'importance apparaîtrait si on s'intéressait aussi aux aspects dynamiques de la déduction naturelle : il faut, pour une introduction de $\Rightarrow$ donnée, se rappeler quelles hypothèses elle désactive, on en garde une trace par un coloriage (ou autre astuce syntaxique, comme l'utilisation d'indice ; ce qu'on retient ici).

On va mettre tout ça en pratique sur quelques exemples, en prouvant des formules mettant en jeu les deux connecteurs pour lesquels on a donné des règles :

$$\dfrac{[A]}{A \Rightarrow A}\ (\Rightarrow\text{-i})$$

$$\dfrac{\dfrac{[A \wedge B]}{B}\ (\wedge\text{-e})}{A \wedge B \Rightarrow B}\ (\Rightarrow\text{-i})$$

$$\dfrac{\dfrac{[A]_1}{A \Rightarrow A}\ (\Rightarrow\text{-i})_1}{B \Rightarrow (A \Rightarrow A)}\ (\Rightarrow\text{-i})_2$$

$$\dfrac{\dfrac{[A] \qquad [A]}{A \wedge A}\ (\wedge\text{-i})}{A \Rightarrow A \wedge A}\ (\Rightarrow\text{-i})$$

$$\dfrac{\dfrac{\dfrac{[A]_1 \qquad [A]_2}{A \wedge A}\ (\wedge\text{-i})}{A \Rightarrow A \wedge A}\ (\Rightarrow\text{-i})_1}{A \Rightarrow (A \Rightarrow A \wedge A)}\ (\Rightarrow\text{-i})_2$$

$$\dfrac{\dfrac{\dfrac{[A \wedge B]_2}{B}\ (\wedge\text{-e}) \qquad [C]_1}{B \wedge C}\ (\wedge\text{-i})}{C \Rightarrow B \wedge C}\ (\Rightarrow\text{-i})_1}{(A \wedge B) \Rightarrow (C \Rightarrow B \wedge C)}\ (\Rightarrow\text{-i})_2$$

3 Calcul des séquents

La structure d'arbre des preuves en déduction naturelle va largement faciliter le travail mathématique sur ces objets. À la place d'une récurrence avec un cas trivial (axiome) et un cas infernal (*modus ponens*) on peut désormais raisonner par induction sur la dernière règle appliquée, ce qui simplifie considérablement le travail.

Le problème, c'est que personne n'est parfait [2]. La déduction naturelle corrige certains défauts des systèmes à la Hilbert mais introduit des difficultés dont on a déjà un peu parlé.

On va se pencher un peu plus attentivement sur le premier problème évoqué : la difficulté à représenter la logique classique. C'est probablement un des points qui a pu motiver G. Gentzen à introduire un nouveau système, car il cherchait à prouver des résultats de cohérence, en particulier pour l'arithmétique de Peano qui utilise la logique classique.

Il y a en fait un problème de symmétrie : en déduction naturelle, on a *des* hypothèses et *une* conclusion. Il y a un déséquilibre dans le système, assez naturel [3] d'ailleurs si l'objectif est de modéliser le raisonnement mathématique.
Mais la logique classique est, vis-à-vis de l'implication $\Rightarrow$, parfaitement symmétrique : une hypothèse peut se retrouvér niée en conclusion et *vice versa* :

$$A \Rightarrow B \quad \simeq \quad \neg A \vee B \quad \simeq \quad \neg B \Rightarrow \neg A$$

La solution de G. Gentzen à été de proposer un nouveau formalisme qui permet d'avoir plusieurs hypothèses *et* plusieurs conclusions (ce qui rétablit la symmétrie entre "entrées" et "sorties" d'une preuve) tout en conservant l'idée d'organiser les preuves en arbres dont les nœuds sont les application de règles logiques.

3.1 Statique : écrire des preuves

L'objet de base qu'on va maintenant manipuler jusqu'à la fin de l'exposé est le séquent.

Définition : Séquent

> On suppose fixé un ensemble de formules logiques. Un **séquent** est une expression de la forme suivante
>
> $$H_1, \ldots, H_m \vdash C_1, \ldots, C_n$$
>
> C'est à dire (formellement) deux suites finies de formules, les **hypothèses** et les **conclusions** du séquent.
> ***Notation :*** *on notera habituellement des suites de formules par des lettres grecques majuscules,* $\Gamma, \Delta, \Theta \ldots$ *des formules simples par des lettres romaines majuscules,* $A, B, C, \ldots$ *Le symbole* $\vdash$ *se "dit" traditionellement « thèse ».*

2. No pun intended. (vous pourrez comprendre cette blague à partir de la 3ème séance introductive)
3. No pun intended, again.

Le sens intuitif d'un séquent

$$H_1, \dots, H_m \vdash C_1, \dots, C_n$$

est $(H_1 \wedge \cdots \wedge H_m) \Rightarrow (C_1 \vee \cdots \vee C_n)$, c'est à dire que sous les hypothèses $H_1, \dots, H_m$ au moins une des formules $C_1, \dots, C_n$ est vraie. Cette intuition va être utile pour comprendre les règles du calcul.

Définition : Règle

On peut définir de manière très (trop) générale ce qu'est une règle de calcul des séquents, ou plutôt décrire ce à quoi ressemble une règle de calcul des séquents, "vue de loin".

$$\frac{\mathfrak{H}_1 \quad \mathfrak{H}_2 \quad \dots \quad \mathfrak{H}_n}{\mathfrak{C}} \ (\mathtt{R})$$

où $\mathfrak{H}_1$, $\mathfrak{H}_2, \dots,$ $\mathfrak{H}_n$ et $\mathfrak{C}$ sont des séquents. On appelle $\mathfrak{H}_1$, $\mathfrak{H}_2, \dots,$ $\mathfrak{H}_n$ les **prémisses** de la règle, et $\mathfrak{C}$ sa **conclusion**.

Une preuve dans un système de calcul des séquents sera finalement un arbre dont les nœuds sont des application de règles du système en question. Avec la condition que les feuilles de l'arbre doivent être règles dont l'ensemble de prémisses est vide, *i.e.* de la forme

$$\frac{}{\mathfrak{C}} \ (\mathtt{R})$$

La racine de l'arbre de preuve est donc un séquent, la *conclusion* de la preuve, le *séquent établi* par la preuve.

On peut formaliser facilement la logique classique dans le calcul des séquents (c'était l'objectif), cela donne le système connu sous le nom de **LK**. On va passer en revue les règles de **LK** dans sa variante *multiplicative*[4].

On répartit souvent les règles en trois groupes : le groupe identité, le groupe logique et le groupe structurel.

Groupe identité : ce sont les règles qui font apparaître `(Ax)` ou disparaître `(Cut)` une formule A.

$$\frac{}{A \vdash A} \ (\mathtt{Ax}) \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \ (\mathtt{Cut})$$

L'axiome `(Ax)` est le cas de base. Dans le cas d'un système logique "pur", il sera la seule feuille possible pour un arbre de preuve (on se souvient qu'on a imposé que les feuilles sont des règles sans prémisses). Il correspond au fait de poser une hypothèse en déduction naturelle.

La coupure `(Cut)` permet de "brancher" une conclusion d'un séquent avec une hypothèse correspondante d'un autre séquent.
C'est une version généralisée, ou plutôt symmétrisée pour être compatible avec l'approche "séquents", du *modus ponens*. Dans le cas particulier suivant, c'est assez clair

$$\frac{\vdash A \qquad A \vdash B}{\vdash B} \ (\mathtt{Cut})$$

Le groupe logique donne les règles d'introduction des connecteurs logiques. Pour le $\vee$ et le $\wedge$:

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \ (\wedge\vdash) \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \ (\vdash\wedge)$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'} \ (\vee\vdash) \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \ (\vdash\vee)$$

4. Une dernière fois, rendez-vous dans deux séances pour l'explication de cette terminologie.

la négation permet de faire transiter des formules entre la gauche et la droite d'un séquent :

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

Le groupe structurel : avec la définition de séquents qu'on a choisie[5], il va falloir un ensemble de règles pour réorganiser les formules, gérer des copies et des effacements.

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ (\mathtt{W}\vdash) \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ (\mathtt{C}\vdash) \qquad \frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \Delta}\ (\mathtt{E}\vdash)$$

où $\sigma(.)$ *est une permutation quelconque de la liste de formules*

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ (\vdash\mathtt{W}) \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ (\vdash\mathtt{C}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \sigma(\Delta)}\ (\vdash\mathtt{E})$$

Les règles (⊢E)-(E⊢), (⊢C)-(C⊢) et (⊢W)-(W⊢) sont respectivement appelées règles d'*échange*, de *contraction* et d'*affaiblissement* (à gauche et à droite).

Quelques exemples de preuves dans **LK** :

Remarque : *Comme on parle ici de logique classique, on* définit *le connecteur* $\Rightarrow$ *comme*

$$A \Rightarrow B \ := \ \neg A \vee B$$

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\mathtt{Ax})}{\vdash \neg A, A}\,(\vdash\neg)}{\vdash \neg A \vee A}\,(\vdash\vee) \qquad \dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\mathtt{Ax})}{A, B \vdash A}\,(\mathtt{W}\vdash)}{A \wedge B \vdash A}\,(\wedge\vdash) \qquad \dfrac{\dfrac{}{A \vdash A}\,(\mathtt{Ax}) \quad \dfrac{}{A \vdash A}\,(\mathtt{Ax})}{A, A \vdash A \wedge A}\,(\vdash\wedge)}{A \vdash A \wedge A}\,(\mathtt{C}\vdash) \qquad \dfrac{\dfrac{\dfrac{}{B \vdash B}\,(\mathtt{Ax}) \quad \dfrac{}{A \vdash A}\,(\mathtt{Ax})}{B, A \vdash B \wedge A}\,(\vdash\wedge)}{A, B \vdash B \wedge A}\,(\mathtt{E}\vdash)}{A \wedge B \vdash B \wedge A}\,(\wedge\vdash)$$

Exercice : *prouver les autres formules des exemples de la partie 2, c'est à dire établir les séquents* $\vdash A \wedge B \Rightarrow (C \Rightarrow (B \wedge C))$, $\vdash A \Rightarrow (A \Rightarrow A \wedge A)$, ...
Prouver $\neg\neg A \Leftrightarrow A$ *, c'est à dire* $(A \Rightarrow \neg\neg A) \wedge (\neg\neg A \Rightarrow A)$.

Déduction naturelle *vs.* calcul des séquents

Quelques éléments de comparaison des deux systèmes qu'on a introduit.

Les règles structurelles du calcul des séquents sont plus ou moins implicites en déduction naturelle. Les règles d'échange (⊢E)-(E⊢) n'apparait pas du tout, les règles de contraction (⊢C)-(C⊢) et d'affaiblissement (⊢W)-(W⊢) sont cachées par le fait qu'on peut désactiver un nombre arbitraire d'hypothèses lors d'une introduction de $\Rightarrow$.

D'autre part, supposont qu'on ait une traduction des preuves du calcul des séquents pour la logique intuitionniste avec les connecteurs $\wedge$ et $\Rightarrow$ vers la déduction naturelle pour cette même logique (je ne détaille pas ces notions, faites un effort d'imagination).

Considérons une preuve $\dfrac{\ddots \ \vdots \ \iddots}{A, B, C, D \vdash E}$

qui se traduirait en déduction naturelle par un arbre de la forme $\begin{array}{c} A \ B \ C \ D \\ \ddots \ \vdots \ \iddots \\ E \end{array}$

5. Il existe des variantes, où les deux côtés du séquents sont des ensembles, multi-ensembles, etc. de formuls au lieu d'être des suites.

On peut poursuivre la preuve de calcul des séquents de deux façons différentes (du point de vue séquents) : l'arbre de preuve change puisque les deux règles $(\wedge\vdash)$ sont interverties.

$$\dfrac{\dfrac{\dfrac{\vdots}{A,B,C,D\vdash E}}{A\wedge B,C,D\vdash E}\,(\wedge\vdash)}{A\wedge B,C\wedge D\vdash E}\,(\wedge\vdash) \qquad \dfrac{\dfrac{\dfrac{\vdots}{A,B,C,D\vdash E}}{A,B,C\wedge D\vdash E}\,(\wedge\vdash)}{A\wedge B,C\wedge D\vdash E}\,(\wedge\vdash)$$

Pourtant elles sont toutes les deux traduites par le même arbre de déduction naturelle, sur lequel l'ordre des éliminations du $\wedge$ n'apparait pas.

$$\dfrac{\dfrac{\dfrac{\dfrac{A\wedge B}{A}\quad\dfrac{A\wedge B}{B}}{\vdots}\quad\dfrac{C\wedge D}{C}}{\vdots}\quad\dfrac{C\wedge D}{D}}{E}$$

Ces deux points de comparaison peuvent se résumer ainsi : la déduction naturelle est un mode d'écriture des preuves plus compact, synthétique, abstrait ; alors que le calcul des séquents est plus verbeux, analytique, concret. On pourrait dire aussi que la déduction naturelle est un *quotient* du calcul des séquents.
Ainsi une preuve en calcul des séquents contient plus de détails sur sa construction, mais ces détails sont potentiellement "inessentiels". La définition de ce qui est essentiel comme information pour décrire une preuve est un débat méthodologique qui est loin d'être fermé.
On retrouvera ce thème lors de la 4ème séance introductive avec les *réseaux de preuve*.

3.2 Dynamique : réécrire des preuves

S'il s'agissait simplement d'un système formel commode et bien structuré pour écrire des preuves, le calcul des séquents (la déduction naturelle aussi, mais on se concentre ici sur le calcul des séquent) n'aurait probablement pas connu une telle postérité. La preuve de cohérence de G. Gentzen dans [4] repose sur un résultat qui deviendra un des piliers de la théorie de la démonstration moderne : le *Hauptsatz* [6] ou théorème d'*élimination des coupures*.

Théorème : Hauptsatz

> Pour toute preuve de calcul des séquents (disons dans le système **LK**) il existe une preuve de même conclusion *sans coupure*, c'est à dire qui n'utilise pas la règle `(Cut)`.

Il s'agit en fait d'une version considérablement affaiblie, méthodologiquement parlant, du résultat. On verra pourquoi un peu plus loin, mais qui à les mêmes conséquences en termes de cohérence du système logique.

C'est un résultat plutôt surprenant au premier abord : dans les systèmes à la Hilbert, la coupure (*modus ponens*) était la *seule* règle déductive, alors qu'ici on dit qu'on peut finalement s'en passer !

Élimination des coupures, sous-formule et preuves cohérence

Le théorème d'élimination des coupures va apporter encore plus de structure aux preuves en calcul des séquents : quand on doit prouver un résultat sur la logique qui nous intéresse, on pourra se contenter de le prouver pour les preuves sans coupures, dont la forme est considérablement plus simple que les preuves générales.

Un premier résultat dont vous avez déjà entendu parler si vous êtiez là la semaine dernière est la propriété de la sous-formule

6. Ce qui signifie « théorème principal », si j'ai bien compris. On peut difficilement trouver un nom moins évocateur pour un résultat. Folklore, quand tu nous tiens...

Théorème : Propriété de la sous-formule

> Dans une preuve sans coupure d'un séquent $\Gamma \vdash \Delta$ tous les séquents qui apparaissent dans l'arbre de preuve sont formés de sous-formules des éléments de la liste Γ, Δ.

Cette propriété donne une idée de la simplification apportée par le fait d'être sans coupure : contrairement au cas des systèmes à la Hilbert, où l'induction sur un *modus ponens* pouvait mettre en jeu une formule plus complexe que celle sur laquelle on travaillait, on manipule des règles qui ne font que recombiner des formules, sans jamais en faire disparaître.

Concernant la cohérence, remarquons d'abord que

Lemme : Séquent vide

> Un système logique (disons **LK**, à nouveau) en calcul des séquents est cohérent (il ne peut pas prouver à la fois A et $\neg A$ pour un certain A) si et seulement si il ne prouve pas le séquent vide.

Exercice : *prouver ce lemme.*

Il devient alors très simple de prouver des résultats de cohérence, comme corollaire du *Hauptsatz* : le système **LK**, par exemple, est cohérent si et seulement si il ne prouve pas le séquent vide, mais on voit rapidement qu'aucune des règles logiques ne peut avoir pour conséquence le séquent vide, excepté éventuellement la règle de coupure, qu'on a éliminée.

Procédure d'élimination

On termine par l'aspect le plus important du calcul des séquent pour les exposés suivants du GdT : la procédure d'élimination des coupures du calcul des séquents. On continue à prendre l'exemple de **LK**, mais la plupart de ce qui est dit dans cette partie s'applique aux autres systèmes écrits en calcul des séquents.

Remarque : *il faudrait plus de temps pour voir en détails comment la notion d'élimination des coupures, d'abord peu mise en avant par G. Gentzen dont l'objectif principal était sa preuve de cohérence est devenue centrale, et comment on a pu réinterpréter le travail de Gentzen avec ce point de vue. Mais on se contentera pour cette fois d'un résumé un peu simplificateur afin d'être plus pédagogique.*

La preuve du *Hauptsatz* par Gentzen est une preuve d'existence (« il existe une preuve sans coupure… ») *constructive*, *procédurale*. Il donne une "méthode de réduction" (un *algorithme*), qui transforme progressivement une preuve quelconque en une preuve sans coupure.

Dans le cas de l'arithmétique de Péano, la terminaison de cette procédure est le point de la preuve qui nécessite une induction ordinale. D'une manière générale, la procédure d'élimination est un algorithme qui peut mettre beaucoup de temps à terminer.

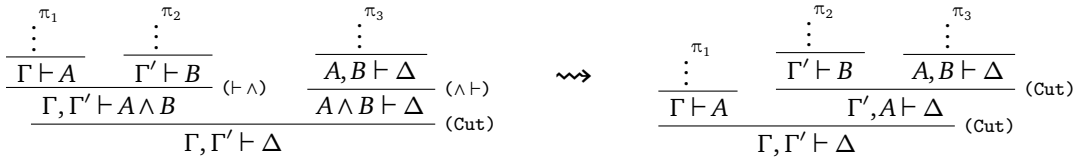
On ne va pas refaire la preuve de Gentzen (les curieuses et curieux peuvent aller regarder [4]) mais plutôt regarder comment elle fonctionne sur des exemples.

Le principe général est de "faire remonter" les coupures dans l'arbre de preuve, jusqu'à atteindre les feuilles (qui sont des règles `(Ax)`), car dans ce cas on peut faire disparaître la coupure :

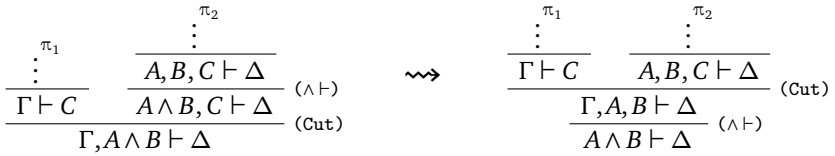
$$\dfrac{\dfrac{}{A \vdash A}\,(\mathtt{Ax}) \qquad \dfrac{\overset{\pi}{\vdots}}{\Gamma, A \vdash \Delta}}{\Gamma, A \vdash \Delta}\,(\mathtt{Cut}) \quad \rightsquigarrow \quad \dfrac{\overset{\pi}{\vdots}}{\Gamma, A \vdash \Delta}$$

On distingue plusieurs cas :

Les cas-clefs : la coupure qu'on veut faire remonter oppose deux règles duales, introduisant le même connecteur à gauche et à droite du symbole $\vdash$, par exemple



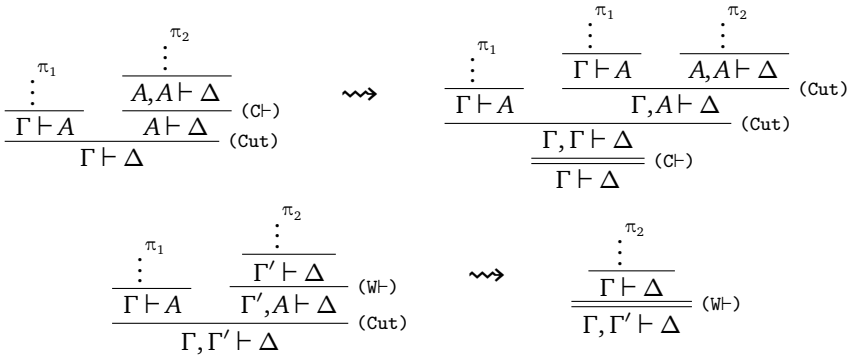
Les commutations : une coupure peut également opposer deux formules dont le dernier connecteur a été introduit plus haut dans l'arbre de preuve. Pour essayer de se ramener au cas précédent, on fait remonter la coupure jusqu'au point où le connecteur en question a été introduit.



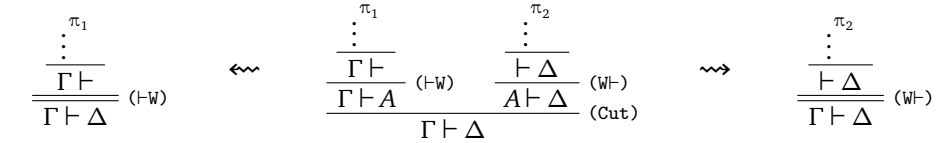
L'existence de ces étapes de réduction, où moralement "il ne se passe rien", est liée au format séquent : comme on se souvient de l'ordre dans lequel on a pu appliquer les règles logiques, il va falloir souvent permuter l'ordre d'application de ces règles avant de pouvoir appliquer un cas-clef. Là encore, voir l'exposé sur les réseaux de preuve.

Les coupures structurelles : il se peut qu'une des règles immédiatement au dessus de la coupure qu'on veut réduire soit une règle structurelle. C'est ici que les vrais ennuis commencent.

une ligne double indique une série d'applications de la même règle

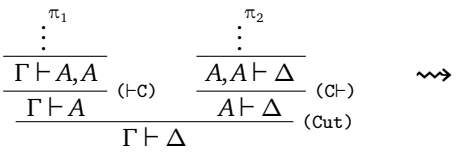


Dans le cas de la contraction, on voit tout de suite que la taille de la preuve augmente lorsqu'on effectue une "réduction". C'est en grande partie ce qui va rendre la preuve de terminaison difficile et l'algorithme long à terminer.
De plus, pour ces deux réductions, il y a un cas particulier problématique : quand une coupure oppose une règle structurelle à sa règle duale (*i.e.* agissant de l'autre côté du symbole $\vdash$). Dans ce cas, pour l'affaiblissement, on a deux possibilités de réduction



Cette situation est connue sous le nom de *paire critique de Lafont* et fait que la procédure de réécriture de Gentzen est un algorithme non-déterministe.

Pour la contraction, c'est encore pire



Pour ce cas, la solution de Gentzen, les “coupures croisées”, est très complexe. Une autre solution viendra plus tard de la logique linéaire et de la polarisation, on en reparlera certainement de tout ça au GdT.

On peut maintenant donner la “vraie” version du théorème de Gentzen,

Théorème : Hauptsatz

> La procédure de réécriture des preuves décrite ci dessus, appliquée à une preuve quelconque, termine et produit une preuve sans coupure.

Annexe : le système LK

Axiome, coupure, négation

$$\frac{}{A \vdash A}\ (\mathtt{Ax})$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ (\mathtt{Cut})$$

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

Règles structurelles

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ (\mathtt{W}\vdash) \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ (\mathtt{C}\vdash) \qquad \frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \Delta}\ (\mathtt{E}\vdash)$$

où $\sigma(.)$ est une permutation quelconque de la liste de formules

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ (\vdash\mathtt{W}) \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ (\vdash\mathtt{C}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \sigma(\Delta)}\ (\vdash\mathtt{E})$$

Règles des connecteurs logiques (variante multiplicative, LK$^{\mathrm{m}}$)

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ (\wedge\vdash) \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'}\ (\vdash\wedge)$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'}\ (\vee\vdash) \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ (\vdash\vee)$$

Règles des connecteurs logiques (variante additive, LK$^{\mathrm{a}}$)

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ (\wedge_g\vdash) \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ (\wedge_d\vdash)$$

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

$$\frac{\vdash A, \Gamma}{\vdash A \vee B, \Gamma}\ (\vdash\vee_g) \qquad \frac{\vdash B, \Gamma}{\vdash A \vee B, \Gamma}\ (\vdash\vee_d)$$

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