L1MD – Notes de cours[1] sur le calcul des séquents **31 mars 2014**

1. Un séquent se présente sous la forme $\Gamma \vdash B$ où Γ est une liste d'énoncés et de déclaration de variables libres avec leur type et où B est un énoncé, toute les variables libres étant déclarées à gauche de $\vdash$. On écrira aussi $[\Gamma \vdash B]$ pour distinguer le séquent du reste du texte. Le séquent $\Gamma \vdash B$ se lit "dans le contexte Γ, B est vrai" ou " Sous les hypothèses données par Γ, B est vrai". Le séquent $\vdash B$ (Γ est vide) se lit "On a B". Le séquent $\Gamma \vdash$ (B est absent) se lit "la liste des énoncés de Γ est contradictoire"

L'écriture

$$\frac{\Gamma_1 \vdash B_1 \quad \Gamma_2 \vdash B_2 \quad \dots}{\Gamma'_1 \vdash B'_1 \quad \dots}$$

signifie qu'on peut passer de la liste de séquents en haut à la liste de séquents en bas par application d'une ou plusieurs règles du calcul des séquents (voir plus bas). L'application successive des règles constitue le calcul des séquents. Une fois le calcul établi on obtient une nouvelle règle.

On déclare des axiomes ou on rappelle des théorèmes sans leurs preuves par les séquents $\Gamma \vdash B$ correspondants. Ils induisent des règles de la forme $\frac{}{\Gamma \vdash B}$. Un calcul partant des axiomes et théorèmes et aboutissant à $\Gamma' \vdash B'$ établit $\Gamma' \vdash B'$ comme nouveau théorème. Un calcul abouttisant à $\vdash B$ est une preuve de B : il établit la valeur de vérité $B \equiv$ Vrai. Un calcul aboutissant à $\Gamma \vdash$ est une preuve par l'absurde : il établit que Γ est contradictoire. Si Γ est la liste des énoncés $A_1, A_2, \dots, A_n$ le calcul établit la valeur de vérité (A_1 et A_2 et $\dots$ et A_n) $\equiv$ Faux.

Les règles du calcul des séquents ont deux roles : elles précisent ce que sont les règles de déduction donc ce qu'on admet comme preuve (il y a d'ailleurs plusieurs jeux de règles présentes dans la littérature correspondant à des logiques différentes : logique classique pour ce cours, logique intuisionniste,...) ; elles permettent d'établir la valeur de vérité d'un énoncé commençant par un quantificateur $\forall, \exists$ ce que ne permettent pas les tables de vérité.

2. Lien avec les tables de vérité

Les connecteurs logiques $\neg$, et , ou , $\Rightarrow, \Leftrightarrow$ ont leur table de vérité et relations habituelles. Par exemple $A \equiv \neg\neg A$ (A et $\neg\neg A$ ont même valeurs de vérité d'après la table de vérité de $\neg$, quel que soit le contenu de A), $(A \Rightarrow B) \equiv (\neg A$ ou $B)$, $(A$ et $A \Rightarrow B) \equiv (A$ et $B)$.

On ajoute le lien entre les quantificateurs et la négation : $\neg\big(\forall x : \mathcal{T},\ P(x)\big) \equiv \big(\exists x : \mathcal{T},\ \neg P(x)\big)$ où $\mathcal{T}$ est un type (le type ensemble par exemple) et $P(x)$ est un énoncé dépendant de $x : \mathcal{T}$.

La première règle ci-dessous avec à gauche son nom ($\vdash V$) dit qu'on a $\Gamma \vdash A$ si on sait $A \equiv$ Vrai ; la deuxième (id) dit qu'on a toujours $\Gamma, A \vdash A$:

$$(\vdash V)\ \frac{}{\Gamma \vdash A} \qquad (\text{id})\ \frac{}{\Gamma, A \vdash A}$$

(Γ peut être vide).

3. Quelques règles avec à gauche leur nom.

La liste que nous donnons n'est pas minimale : certaines règles se déduisent des autres. Les premières règles sont réversibles : l'écriture obtenue en échangeant le haut et le bas est aussi une règle.

Lorsqu'un énoncé d'un séquent fait intervenir une variable liée (par un quantificateur ou une construction), celle-ci ne doit pas être une variable libre dans le reste du séquent. On évite le conflit de notation en renommant au besoin les variables liées.

$$(\vdash \text{ et })\ \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \text{ et } B} \qquad (\vdash\Rightarrow)\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad (\vdash \text{ ou })\ \frac{\Gamma, \neg A \vdash B}{\Gamma \vdash A \text{ ou } B}$$

$$(\vdash \neg)\ \frac{\Gamma, A, B \vdash}{\Gamma, A \vdash \neg B} \qquad (\text{ et } \vdash)\ \frac{\Gamma, A, B \vdash C}{\Gamma, A \text{ et } B \vdash C} \qquad (\text{ ou } \vdash)\ \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \text{ ou } B \vdash C}$$

$(\exists \vdash)\ \dfrac{\Gamma, \big(\exists x : \mathcal{T},\ P(x)\big) \vdash B}{\Gamma, x : \mathcal{T}, P(x) \vdash B}$ où x est une variable (de type $\mathcal{T}$) n'apparaissant pas dans Γ et B et où $P(x)$ est un énoncé dépendant de x.

[1] F-X. Dehon, Université de Nice — dehon@unice.fr

$(\vdash \forall)$ $\dfrac{\Gamma, x : \mathcal{T} \vdash P(x)}{\Gamma \vdash \big(\forall x, P(x)\big)}$ où x est une variable (de type $\mathcal{T}$) n'apparaissant pas dans Γ et où $P(x)$ est un énoncé dépendant de x.

Voici maintenant quelques règles non réversibles :

Affaiblissement à droite (ad) $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \text{ ou } B}$.

Affaiblissement à gauche (ag) $\dfrac{\Gamma \vdash B}{\Gamma, A \vdash B}$

Réécritures $(\Leftrightarrow\vdash)$ $\dfrac{\Gamma \vdash A \Leftrightarrow B \qquad \Gamma, A \vdash C}{\Gamma, B \vdash C}$ $(\vdash\Leftrightarrow)$ $\dfrac{\Gamma \vdash A \Leftrightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$

$(\Leftrightarrow \forall)$ $\dfrac{\Gamma \vdash \forall x : \mathcal{T}, (P(x) \Leftrightarrow Q(x))}{\Gamma \vdash (\forall x : \mathcal{T}, P(x)) \Leftrightarrow (\forall x : \mathcal{T}, Q(x))}$ $(\Leftrightarrow \exists)$ $\dfrac{\Gamma \vdash \forall x : \mathcal{T}, (P(x) \Leftrightarrow Q(x))}{\Gamma \vdash (\exists x : \mathcal{T}, P(x)) \Leftrightarrow (\exists x : \mathcal{T}, Q(x))}$

Cas particulier à gauche $(\forall \vdash)$ $\dfrac{\Gamma, P(t) \vdash B}{\Gamma, \big(\forall x : \mathcal{T}, P(x)\big) \vdash B}$ où x est une variable (de type $\mathcal{T}$) n'apparaissant pas dans Γ et B, P est un énoncé dépendant de x et t est un objet de type $\mathcal{T}$ donné par une formule faisant intervenir les variables libres de Γ ou les constantes. On peut préciser la valeur prise pour x en nommant la règle $(\forall \vdash)[x := t]$.

Exhiber à droite $(\vdash \exists)$ $\dfrac{\Gamma \vdash P(t)}{\Gamma \vdash \big(\exists x : \mathcal{T}, P(x)\big)}$ où x est une variable (de type $\mathcal{T}$) n'apparaissant pas dans Γ, P est un énoncé dépendant de x et t est un objet de type $\mathcal{T}$ donné par une formule faisant intervenir les variables libres de Γ ou les constantes. On peut préciser la valeur prise pour x en nommant la règle $(\vdash \exists)[x := t]$.

4. Premiers objets : ensembles, entiers et les règles associées.

Règle associée à la relation d'égalité : $(=)$ $\dfrac{}{x, y : \mathcal{T}, x = y, P(x) \vdash P(y)}$ où $P(x)$ est un énoncé dépendant d'une variable libre x de type $\mathcal{T}$. Cette règle semble aller de soi mais il vaut mieux l'expliciter.

Quelques axiomes de la théorie des ensembles (axiomatique de Zermelo). On écrit ici chaque axiome par le séquent $\Gamma \vdash B$ correspondant plutôt que par l'écriture $\dfrac{}{\Gamma \vdash B}$.

$(\in)$ $\big[A, B : \mathcal{E}\text{ns}, \big(\forall x : \mathcal{E}\text{ns},\ (x \in A \Leftrightarrow x \in B)\big) \vdash A = B\big]$. Le séquent $\big[A, B : \mathcal{E}\text{ns}, A = B \vdash \forall x,\ (x \in A \Leftrightarrow x \in B)\big]$ se déduit de la règle $(=)$.

$(\{a, b\})$ $\big[a, b : \mathcal{E}\text{ns} \vdash \exists X : \mathcal{E}\text{ns}, \forall x : \mathcal{E}\text{ns}, \big(x \in X \Leftrightarrow (x = a \text{ ou } x = b)\big)\big]$

...

$(\{x \in X, P(x)\})$ $\big[X : \mathcal{E}\text{ns} \vdash \exists E : \mathcal{E}\text{ns}, \forall x : \mathcal{E}\text{ns}, x \in E \Leftrightarrow (x \in X \text{ et } P(x))\big]$ où $P(x)$ est un énoncé dépendant de x dont E n'est pas une variable.

Pour X un ensemble d'objets de type $\mathcal{T}$ et $P(x)$ un énoncé dépendant de $x : \mathcal{T}$, on écrit $\big(\exists x \in X,\ P(x)\big)$ pour $\big(\exists x : \mathcal{T},\ \big(x \in X \text{ et } P(x)\big)\big)$. On écrit $\big(\forall x \in X,\ P(x)\big)$ pour $\big(\forall x : \mathcal{T},\ \big(x \in X \Rightarrow P(x)\big)\big)$.

On dispose des deux "théorèmes" suivants, où $X \setminus \{x_0\}$ désigne l'ensemble $\{x \in X, x \neq x_0\}$ et où $P(x)$ est un énoncé dépendant de la variable x :

$(x_0\exists)$ $\big[X : \mathcal{E}\text{ns}, x_0 : X \ \vdash\ \big(\exists x \in X, P(x)\big) \Leftrightarrow \big(P(x_0) \text{ ou } \exists x \in X \setminus \{x_0\}, P(x)\big)\big]$

$(x_0\forall)$ $\big[X : \mathcal{E}\text{ns}, x_0 : X \ \vdash\ \big(\forall x \in X, P(x)\big) \Leftrightarrow \big(P(x_0) \text{ et } \forall x \in X \setminus \{x_0\}, P(x)\big)\big]$

Type entier et récurrence. On a la règle :

(rec) $\dfrac{\Gamma \vdash P(0) \qquad \Gamma, n : \mathbb{N}, P(n) \vdash P(n+1)}{\Gamma \vdash \forall n : \mathbb{N}, P(n)}$, où $P(n)$ est un énoncé dépendant de l'entier n.

Exercice : Déduire de (rec) et de la théorie des ensembles une preuve du séquent

$$\big[E : \mathcal{P}(N), 0 \in E, \big(\forall n : \mathbb{N}, (n \in E \Rightarrow n+1 \in E)\big) \vdash E = \mathbb{N}\big]$$

5. Preuves

5.1. Stratégies de Preuve

Ce sont des règles qu'on utilise habituellement pour établir le séquent en bas à partir du ou des séquent en haut. Ces règles se déduisent des règles de la section précédente. Voici les plus usuelles :

– Réécritures ($\Leftrightarrow\vdash$), ($\vdash\Leftrightarrow$), ($\Leftrightarrow \forall$), ($\Leftrightarrow \exists$). Ce sont ces règles qu'on utilise pour traduire un énoncé informel en un énoncé formalisé, pour faire apparaitre la définition d'un terme, pour remplacer une définition par une définition équivalente.

– Réduction du séquent à prouver à un ou des séquents plus lisible par application des règles réversibles ($\vdash \forall$), ($\vdash\Rightarrow$), etc.

– Modus Ponens (mp) $\dfrac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}$

Lorsque l'énoncé A n'est pas issu directement de Γ mais est issu de l'imagination de celui qui prouve, on appelera cette stratégie "Observer A"

– Distinguer suivant H ($H \vee \neg H \vdash$) $\dfrac{\Gamma, H \vdash B \qquad \Gamma, \neg H \vdash B}{\Gamma \vdash B}$. Plus généralement on peut distinguer suivant $H_1, H_2, \ldots, H_n$ si (H_1 ou $\ldots$ ou H_n) $\equiv V$:

$$(H_i \vdash) \quad \frac{\Gamma \vdash (H_1 \text{ ou } \ldots \text{ ou } H_n) \qquad \Gamma, H_1 \vdash B \quad \cdots \quad \Gamma, H_n \vdash B}{\Gamma \vdash B}$$

– Séquent plus fort : remplacer le séquent à prouver $\Gamma \vdash B$ par un séquent $\Gamma' \vdash B'$ lorsqu'on sait établir la règle $\dfrac{\Gamma' \vdash B'}{\Gamma \vdash B}$. C'est ce qu'on fait notamment avec les règles (ad), (ag), ($\forall \vdash$), ($\vdash \exists$).

– Preuve par l'absurde de $\Gamma \vdash B$ en prouvant que $\Gamma, \neg B$ est contradictoire : $\dfrac{\Gamma, \neg B \vdash}{\Gamma \vdash B}$.

– Preuve par récurrence d'un séquent $\big[\Gamma \vdash \forall n : \mathbb{N}, P(n)\big]$.

La plupart de ces stratégies (réécritures, observer A, distinguer suivant H, séquent plus fort) font intervenir un (ou des) énoncé auxiliaire ad hoc qui n'est pas issu du séquent à prouver ; c'est ce qui rend les preuves difficiles. Le choix d'une stratégie n'a rien d'automatique.

Voici pour l'exemple l'établissement de la règle (mp) puis de la règle "Distinguer suivant H" :

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash A \quad \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\vdash\Rightarrow)}{\Gamma \vdash A \text{ et } (A \Rightarrow B)}\ (\vdash \text{ et })}{\Gamma \vdash A \text{ et } B}\ (\vdash\Leftrightarrow)}{\Gamma \vdash A \quad \Gamma \vdash B}\ (\vdash \text{ et })}{\Gamma \vdash B}\ \text{(oubli)}$$

$$\dfrac{\dfrac{}{\Gamma \vdash H \text{ ou } \neg H}\ (\vdash V) \quad \dfrac{\Gamma, H \vdash B \quad \Gamma, \neg H \vdash B}{\Gamma, H \text{ ou } \neg H \vdash B}\ (\text{ ou } \vdash)}{\Gamma \vdash B}\ \text{(mp)}$$

5.2. Organisation d'une preuve

on écrit le plus souvent une preuve en partant du séquent à prouver et en écrivant les règles (les stratégies de preuve) à l'envers : le séquent du haut se déduit du ou des séquents du bas. L'application successive des stratégies ramène le séquent à prouver à une liste de séquents qu'on sait vrai (les axiomes, les séquents déjà prouvés, le séquent vide).

La preuve d'un séquent n'est pas unique et peut être plus ou moins fastidieuse suivant le choix plus ou moins heureux des stratégies. Il n'est par exemple pas toujours heureux de remplacer un terme par sa définition, etc.

5.3. Un exemple : preuve de l'énoncé "Toute partie non vide de $\mathbb{N}$ admet un plus petit élément" suivant les indications de l'exercice 1 de la feuille de TD 5.

Soit S un partie non vide de $\mathbb{N}$. On note $\mathrm{Hyp}(n)$ l'énoncé "S contient un entier inférieur ou égal à n" ; $\mathrm{Hyp}(n)$ se formalise comme $\big(\exists k : \mathbb{N},\ k \in S \text{ et } k \leq n\big)$

On note Concl l'énoncé "S admet un plus petit élément". Concl se formalise partiellement comme $\big(\exists n : \mathbb{N},\ n \in S \text{ et } n \text{ minore } S\big)$

On a les équivalences

$$\neg\mathrm{Hyp}(n) \Leftrightarrow \big(\forall k : \mathbb{N},\ k \in S \Rightarrow k > n\big) \Leftrightarrow \big(\forall k : \mathbb{N},\ k \in S \Rightarrow k \geq n+1\big) \Leftrightarrow \big(n+1 \text{ minore } S\big)$$

L'exercice 1 suggère de montrer par récurrence sur n l'implication $\mathrm{Hyp}(n) \Rightarrow \mathrm{Concl}$.

$$\dfrac{\dfrac{S : \mathcal{P}(\mathbb{N}) \vdash \forall n : \mathbb{N},\ \mathrm{Hyp}(n) \Rightarrow \mathrm{Concl}}{\dfrac{S : \mathcal{P}(\mathbb{N}) \vdash \mathrm{Hyp}(0) \Rightarrow \mathrm{Concl}}{S : \mathcal{P}(\mathbb{N}), \mathrm{Hyp}(0) \vdash \mathrm{Concl}}} \quad \dfrac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \mathrm{Hyp}(n) \Rightarrow \mathrm{Concl} \vdash \mathrm{Hyp}(n+1) \Rightarrow \mathrm{Concl}}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n) \text{ ou } \mathrm{Concl}, \mathrm{Hyp}(n+1) \vdash \mathrm{Concl}}\ (\Leftrightarrow\vdash)}\ (rec)$$
$$S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash \mathrm{Concl} \qquad S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \mathrm{Concl}, \mathrm{Hyp}(n+1) \vdash \mathrm{Concl}$$

On continue par

$$\dfrac{\dfrac{\dfrac{S : \mathcal{P}(\mathbb{N}), \mathrm{Hyp}(0) \vdash \mathrm{Concl}}{S : \mathcal{P}(\mathbb{N}), \mathrm{Hyp}(0) \vdash 0 \in S \text{ et } 0 \text{ minore } S}}{\dfrac{S : \mathcal{P}(\mathbb{N}), \mathrm{Hyp}(0) \vdash 0 \in S}{S : \mathcal{P}(\mathbb{N}), k : \mathbb{N}, k \in S, k \leq 0 \vdash 0 \in S}\ (\exists\vdash)}\ \dfrac{S : \mathcal{P}(\mathbb{N}), \mathrm{Hyp}(0) \vdash 0 \text{ minore } S}{}\ (\vdash V)}{S : \mathcal{P}(\mathbb{N}), k : \mathbb{N}, k \in S, k = 0 \vdash 0 \in S}$$

et

$$\dfrac{\dfrac{\dfrac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash \mathrm{Concl}}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash n+1 \in S \text{ et } n+1 \text{ minore } S}}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash n+1 \in S} \quad \dfrac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash n+1 \text{ minore } S}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash \neg\mathrm{Hyp}(n)}}$$

Reste à prouver $\big[S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg\mathrm{Hyp}(n), \mathrm{Hyp}(n+1) \vdash n+1 \in S\big]$.

...