Logique et Preuve

Philippe Duchon – duchon@labri.fr

Année 2019-20 – 3 octobre 2019

Logique minimale

- Assez “pauvre” en termes de ce qu’elle peut exprimer (un seul connecteur, l’implication)

Logique minimale

- Assez “pauvre” en termes de ce qu’elle peut exprimer (un seul connecteur, l’implication)
- On a vu la propriété essentielle de **cohérence**: *tout séquent prouvable est nécessairement un séquent valide*.

Logique minimale

- Assez “pauvre” en termes de ce qu’elle peut exprimer (un seul connecteur, l’implication)
- On a vu la propriété essentielle de **cohérence**: *tout séquent prouvable est nécessairement un séquent valide*.
- Ce qu’on n’a pas énoncé en cours, c’est la réciproque: est-ce qu’un séquent valide est forcément prouvable? (c’est la question, à peine moins essentielle, de la **complétude**).

Logique minimale

- Assez “pauvre” en termes de ce qu’elle peut exprimer (un seul connecteur, l’implication)
- On a vu la propriété essentielle de **cohérence**: *tout séquent prouvable est nécessairement un séquent valide*.
- Ce qu’on n’a pas énoncé en cours, c’est la réciproque: est-ce qu’un séquent valide est forcément prouvable? (c’est la question, à peine moins essentielle, de la **complétude**).
- Ce qu’on va voir aujourd’hui: *non*, la logique minimale n’est pas complète, avec un exemple de *séquent valide qui n’admet aucune preuve*.

Logique minimale

- Assez “pauvre” en termes de ce qu’elle peut exprimer (un seul connecteur, l’implication)
- On a vu la propriété essentielle de **cohérence**: *tout séquent prouvable est nécessairement un séquent valide*.
- Ce qu’on n’a pas énoncé en cours, c’est la réciproque: est-ce qu’un séquent valide est forcément prouvable? (c’est la question, à peine moins essentielle, de la **complétude**).
- Ce qu’on va voir aujourd’hui: *non*, la logique minimale n’est pas complète, avec un exemple de *séquent valide qui n’admet aucune preuve*.
- Et surtout: exemple complexe de raisonnement **sur** les preuves (les preuves sont des objets bien définis, on peut raisonner dessus).

Les arbres de preuves

- Les preuves qu'on considère sont systématiquement sous forme d'arbres; on n'utilise aucune règle dérivée.
- Chaque noeud de l'arbre correspond à l'utilisation d'une règle de la logique formelle:
  - les feuilles sont forcément des "règles d'hypothèse"
  - les noeuds unaires sont forcément des "introduction de l'implication"
  - les noeuds binaires sont des "modus ponens"
- Chaque noeud porte un séquent; le sous-arbre enraciné en ce noeud est un arbre de preuve correct de ce même séquent.
- Les raisonnements sur les preuves, vont souvent être des raisonnements *par récurrence* sur (la taille de) l'arbre de preuve.

La formule de Peirce

$$((P \to Q) \to P) \to P$$

- C'est une tautologie (vu en exercice)
- Donc le séquent $\vdash ((P \to Q) \to P) \to P$ est valide

Théorème

Le séquent (valide) $\vdash ((P \to Q) \to P) \to P$ n'admet pas de preuve en logique minimale.

Lemme des hypothèses

Dans tout arbre de preuve de la logique minimale, l'ensemble des hypothèses est *croissant le long des branches* : toute hypothèse présente dans le séquent d'un noeud, est présente dans chaque noeud du sous-arbre enraciné en ce noeud.

Preuve: par récurrence sur l'arbre de preuve; on se ramène à remarquer que la propriété est vraie, localement, pour chacune des trois règles de déduction.

Note: ce ne serait pas vrai si on utilisait la règle dérivée d'"affaiblissement"

La propriété de récurrence

On note H_n la propriété: "dans tout arbre de preuve (correct) de taille au plus n, dans le séquent de chaque noeud autre que la racine, on trouve au moins toutes les hypothèse du séquent du père de ce noeud".

- H_1 est vraie: si un arbre de preuve n'a qu'un seul noeud (preuve par la règle d'hypothèse, donc), il n'y a pas de noeud qui ne soit pas la racine.
- Soit $n \geq 1$ tel que H_n soit vraie: il nous faut prouver H_{n+1}, pour pouvoir conclure par récurrence sur n.
- On se donne donc un arbre de preuve de taille $n+1$; il nous faut montrer qu'il a la propriété cherchée (chaque noeud autre que la racine, a au moins les hypothèse de son père).

La preuve d'hérédité

- Considérons donc notre arbre de preuve T, de taille $n+1$. La racine de cet arbre est donc un noeud soit unaire (règle d'introduction) soit binaire (règle du modus ponens). Notons T_1 et, éventuellement, T_2, les sous-arbres enracinés au(x) fils de la racine.

La preuve d'hérédité

- Considérons donc notre arbre de preuve T, de taille $n+1$. La racine de cet arbre est donc un noeud soit unaire (règle d'introduction) soit binaire (règle du modus ponens). Notons T_1 et, éventuellement, T_2, les sous-arbres enracinés au(x) fils de la racine.
- Chaqe T_i est donc un arbre de preuve, et il est de taille au plus n; donc, par H_n, chacun de ses noeuds autre que sa racine, a au moins les hypothèses de son père.

La preuve d'hérédité

- Considérons donc notre arbre de preuve T, de taille $n+1$. La racine de cet arbre est donc un noeud soit unaire (règle d'introduction) soit binaire (règle du modus ponens). Notons T_1 et, éventuellement, T_2, les sous-arbres enracinés au(x) fils de la racine.
- Chaqe T_i est donc un arbre de preuve, et il est de taille au plus n; donc, par H_n, chacun de ses noeuds autre que sa racine, a au moins les hypothèses de son père.
- Il ne reste qu'un ou deux noeuds à vérifier, à savoir le(s) racine(s) de T_1 et éventuellement T_2.

La preuve d'hérédité

- Considérons donc notre arbre de preuve T, de taille $n+1$. La racine de cet arbre est donc un noeud soit unaire (règle d'introduction) soit binaire (règle du modus ponens). Notons T_1 et, éventuellement, T_2, les sous-arbres enracinés au(x) fils de la racine.
- Chaqe T_i est donc un arbre de preuve, et il est de taille au plus n; donc, par H_n, chacun de ses noeuds autre que sa racine, a au moins les hypothèses de son père.
- Il ne reste qu'un ou deux noeuds à vérifier, à savoir le(s) racine(s) de T_1 et éventuellement T_2.
- Il suffit de constater que, lors de l'application d'une des deux règles possibles (introduction ou modus ponens), les sous-buts engendrés contiennent toujours au moins les hypothèses du séquent racine.

La preuve d'hérédité

- Considérons donc notre arbre de preuve T, de taille $n+1$. La racine de cet arbre est donc un noeud soit unaire (règle d'introduction) soit binaire (règle du modus ponens). Notons T_1 et, éventuellement, T_2, les sous-arbres enracinés au(x) fils de la racine.
- Chaqe T_i est donc un arbre de preuve, et il est de taille au plus n; donc, par H_n, chacun de ses noeuds autre que sa racine, a au moins les hypothèses de son père.
- Il ne reste qu'un ou deux noeuds à vérifier, à savoir le(s) racine(s) de T_1 et éventuellement T_2.
- Il suffit de constater que, lors de l'application d'une des deux règles possibles (introduction ou modus ponens), les sous-buts engendrés contiennent toujours au moins les hypothèses du séquent racine.
- Donc on a bien H_{n+1} et, par récurrence sur n, tout arbre de preuve a bien la propriété.

Notion de coupure

Définition

Dans un arbre de preuve, on appelle *coupure* la configuration de deux noeuds suivante:

- un noeud $s : \Gamma \vdash B$ utilisant la règle du *modus ponens* (élimination de l'implication)
- le noeud $t : \Gamma \vdash A \to B$, fils gauche de s, utilisant la règle d'introduction de l'implication

Note: le nom évoque l'utilisation de la règle dérivée de coupure, et ça ressemble, mais ce n'est pas exactement la même chose (on n'utilise pas de règle dérivée)

Note bis: en logique propositionnelle (avec d'autres connecteurs), on parlera aussi de coupure pour une preuve utilisant (dans le "sens de la preuve", vers la racine) une élimination immédiatement après une introduction.

Élimination des coupures

On a un *algorithme* pour faire disparaître les coupures d'une preuve: **tant qu'il reste des coupures dans l'arbre**, on trouve un couple (s, t) qui constitue une coupure, puis...

- L'arbre enraciné en s constitue une preuve de $\Gamma \vdash B$
- L'arbre enraciné au fils droit de s constitue une preuve de $\Gamma \vdash A$; notons T_A cet arbre.
- En t, on a le séquent $\Gamma \vdash A \to B$, prouvé par introduction; donc le fils t' de t contient le séquent $\Gamma, A \vdash B$, et le sous-arbre enraciné en t' constitue une preuve T_B de ce séquent.
- Construction d'un nouvel arbre de preuve pour $\Gamma \vdash B$: on prend l'arbre T_B, et on enlève A des hypothèses de tous les séquents; et, **chaque fois que dans T_B on utilise la règle d'hypothèse pour prouver A**, on greffe à la place une copie de l'arbre T_A.

Élimination des coupures(2)

Précisions sur l'algorithme d'élimination des coupures:

- Dans T_B, on supprime normalement l'hypothèse A dans tous les noeuds; mais si, dans un noeud de T_B, on fait une autre introduction sous la forme $A \rightarrow C$, on laisse bien la "nouvelle" hypothèse A dans le sous-arbre.
- Quand on "greffe" T_A en remplacement de l'utilisation, dans T_B, de la règle d'hypothèse sur $\Gamma, \Delta \vdash A$ (les hypothèses contiennent Γ d'après le lemme 1), il faut ajouter, dans chaque noeud de l'arbre greffé, toutes les hypothèses qui sont dans Δ; ajouter des hypothèses ne peut pas remettre en cause la validité de l'arbre de preuve.

Élimination des coupures (3)

Théorème (admis)

L'algorithme d'élimination des coupures **termine**: on finit **toujours** par atteindre un arbre sans aucune coupure.

Note: pendant l'algorithme, il est possible que le nombre de coupures augmente (si par exemple l'arbre T_A contient des coupures, et qu'on greffe plusieurs fois cet arbre)

Note bis: une preuve complète et propre du théorème d'élimination des coupures est au-delà du niveau Licence...

Propriété de la sous-formule

Corollaire (Lemme de la sous-formule)

Dans une preuve sans coupures de la logique minimale, toutes les formules qui apparaissent (dans les hypothèses ou dans la conclusion de n'importe quel noeud de l'arbre) sont des sous-formules de formules qui apparaissent à la racine de l'arbre (comme hypothèse ou comme conclusion).

Note: Comme les sous-arbres d'un arbre de preuve sont aussi des arbres de preuve, le lemme de la sous-formule s'appliquera également à n'importe quel noeud d'un tel arbre, pas seulement à la racine.

Preuve de la sous-formule

- Même schéma de preuve que pour le premier lemme: par récurrence sur la taille de l'arbre, se ramène à une vérification locale pour les règles.
- La règle du modus ponens est la seule qui risque de faire échouer la propriété de la sous-formule (les autres ont directement la propriété, localement)
- On procède par récurrence sur la taille de l'arbre, avec comme propriété de récurrence $\mathbf{H}_n$: "dans tout arbre de preuve sans coupure de taille au plus n, chaque formule qui apparaît est une sous-formule d'une des formules du séquent racine"
- $\mathbf{H}_1$ est vraie: les arbres de taille 1 utilisent la seule règle d'hypothèse.
- Montrons $\mathbf{H}_n \implies \mathbf{H}_{n+1}$: prenons donc un arbre T de taille $n+1$ (en supposant $\mathbf{H}_n$ vraie).

On discute selon la règle utilisée à la racine de T:

- Si c'est la règle d'introduction: le sous-arbre T' porte un séquent dont les formules sont des sous-formules de celles de T; en appliquant $\mathbf{H}_n$ à T', ce sont des sous-formules de la racine de T.
- Si c'est la règle du *modus ponens*: il faut regarder de plus près (au tableau)
- Au total, dans tous les cas la propriété de sous-formule s'applique à T; donc on a bien $\mathbf{H}_n \implies \mathbf{H}_{n+1}$, donc $\mathbf{H}_n$ pour tout n.

Dernière règle

Corollaire (Lemme de la dernière règle)

Dans une preuve sans coupures (en logique minimale) d'un séquent **sans hypothèses**, la règle utilisée à la racine est forcément la règle d'introduction.

Preuve:

- Ça ne peut pas être la règle d'hypothèse (il n'y a pas d'hypothèses)
- Ça ne peut pas être un *modus ponens* (ce serait incompatible avec le lemme de la sous-formule: aucune formule $A \to B$ n'est une sous-formule de B)

Formule de Peirce

Théorème

Le séquent (valide) $\vdash ((P \to Q) \to P) \to P$ n'est pas prouvable en logique minimale.

Preuve: Par l'absurde; on suppose une preuve et on montre que ça ne colle pas avec les lemmes précédents.

Non-prouvabilité de Peirce

- On suppose que le séquent est prouvable, et on en considère une preuve sans coupure.
- Par le lemme de la dernière règle, la racine est une introduction, et le reste de l'arbre prouve $(P \to Q) \to P \vdash P$.
- Ce séquent ne peut pas être prouvé par hypothèse ni par introduction, donc il faut faire un *modus ponens* avec une implication $A \to P$, pour un A approprié.
- $A \to P$ doit être une sous-formule de $(P \to Q) \to P$; la seule possibilité est $A = (P \to Q)$.
- Mais on constate que le séquent $(P \to Q) \to P \vdash P \to Q$ n'est pas valide (il suffit de prendre $v(P) = V$ et $v(Q) = F$), donc il n'est pas prouvable.
- On a exploré l'unique piste possible, il n'existe donc pas de preuve.

Et au-delà?

- La logique minimale est donc incomplète: il existe des séquents valides, mais non prouvables.
- Vous avez vu (ou allez voir) qu'il en est de même de la logique propositionnelle intuitionniste (le séquent $\sim\sim P \vdash P$ n'est pas prouvable non plus).
- C'est (beaucoup) plus pénible à prouver, mais l'élimination des coupures et le lemme de la sous-formule restent valides en logique propositionnelle intuitionniste.
- En ajoutant **une** règle à la logique intuitionniste (le "tiers exclus"), on obtient une nouvelle logique dite "classique", qui est enfin complète.