# ÉLIMINATION DU CUT

Patrick Bellot

Télécom Paris
Institut Polytechnique de Paris
bellot@telecom-paris.fr

MITRO 202

# Citons :

PROOFS AND TYPES
J.Y. Girard & Y. Lafont & P. Taylor
Cambridge Tracts in T.C.S., Cambridge, Angleterre, 1989

# Introduction

On rappelle la règle de *coupure* qui est une règle du calcul des séquents intuitionniste :

$$\frac{\Gamma \vdash A \quad \Gamma', A \vdash B}{\Gamma, \Gamma' \vdash B}$$

Son analogue en calcul des séquents classique est :

$$\frac{\Gamma \vdash \Delta, A \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

# Introduction

Cette règle peut sembler essentielle dans un calcul des séquents puisqu'elle dit *grosso modo* que si une formule $A$ est une conséquence dans un séquent et que la même formule $A$ est hypothèse dans un autre séquent, il est possible de combiner ces deux séquents pour n'en faire qu'un dans lequel $A$ a disparu !

Cependant, cette règle est redondante au sens de la section sur les extensions dérivables. En effet, toute preuve utilisant des coupures peut être remplacée par une preuve n'utilisant pas de coupures. C'est l'objet du résultat suivant dont nous ébaucherons la démonstration un peu plus loin.

# Hauptsatz de Gentzen

Le résultat suivant est valable dans le calcul des séquents classique, dans le calcul des séquents intuitionniste et dans la plupart des calculs des séquents. J-Y. Girard affirme même qu'un système formel de logique qui n'a pas cette propriété ne peut être qualifié de *logique*.

**Théorème d'élimination des coupures (Hauptsatz de Gentzen, 1934).** Si un séquent est prouvable alors il existe une preuve de ce séquent qui n'utilise pas la règle de coupure.

**N.B.** A présent, on se place en Logique Intuitionniste.

# Hauptsatz de Gentzen

Ce résultat est **LE** résultat de la théorie des preuves. J-Y. Girard affirme même que c'est le seul résultat d'importance mais, comme nous le verrons, ses conséquences sont importantes.

Par ailleurs, et nous allons le voir, il est obtenu par des moyens purement formels, i.e. syntaxiques.

Nous allons examiner les conséquences de ce théorème qui sont très importantes. En effet, une preuve n'utilisant pas la règle de coupure possède des propriétés particulières, spécialement en logique intuitionniste.

# La dernière règle en logique intuitionniste

Lorsque l'on considère une preuve sous forme d'arbre, on peut s'intéresser à la *dernière règle* utilisée, c'est-à-dire à celle utilisée pour produire la racine de l'arbre. Nous avons le résultat suivant :

**Propriété.** Si un séquent $\vdash A$ est prouvable en logique intuitionniste alors il existe une preuve de $\vdash A$ où la dernière règle est une règle logique à droite.

**Démonstration.** Si le séquent $\vdash A$ est prouvable, d'après le *Hauptsatz*, il existe une preuve sans coupures de ce séquent. On remarque que la conclusion de la dernière règle est un séquent qui n'a pas d'hypothèses dans sa partie gauche.

Puis...

# La dernière règle en logique intuitionniste

Si l'on examine les règles structurelles du calcul des séquents intuitionniste, on remarque que toutes les règles sauf la règle d'affaiblissement à droite ($aff_d$) ont des hypothèses dans le séquent conclusion. Aucune d'entre elles ne peut donc être la dernière règle utilisée dans la preuve.

Si l'on examine ($aff_d$), la seule application de cette règle fournissant un séquent conclusion sans hypothèse à gauche serait :

$$\frac{\vdash}{\vdash A}\,(aff_d)$$

Cela voudrait dire que l'on a prouvé le séquent *vide* mais le séquent *vide* $\vdash$ n'est pas prouvable.

Donc, la dernière règle n'est pas une règle structurelle.

# La dernière règle en logique intuitionniste

Maintenant, si l'on examine les règles logiques à gauche, par construction elles ont toutes des hypothèses dans leur séquent conclusion. La dernière règle ne peut donc pas être une règle logique à gauche.

Ayant éliminé les règles structurelles et les règles logiques à gauche, la dernière règle utilisée ne peut être qu'une règle logique à droite.

QED

# Propriété de consistance

**Propriété de consistance.** Le séquent $\vdash \bot$ n'est pas démontrable en logique intuitionniste.

**Démonstration.** Si le séquent est prouvable, il existe une preuve de ce séquent dont la dernière règle est une règle logique à droite. Il n'existe pas de règle à droite ayant $\bot$ comme conclusion.

**N.B.** Cette démonstration était inutile puisque les règles du calcul des séquents intuitionniste sont un cas particulier des règles du calcul des séquents classique où l'on restreint la partie droite d'un séquent à contenir au plus une formule. Donc tout théorème intuitionniste est aussi un théorème classique. La consistance de la logique classique entraîne donc celle de la logique intuitionniste.

# Propriété de disjonction (DP)

**Propriété de disjonction.** Si un séquent $\vdash A \vee B$ est prouvable en logique intuitionniste alors soit le séquent $\vdash A$, soit le séquent $\vdash B$ soit les deux sont prouvables.

**Démonstration.** Si le séquent est prouvable, il existe une preuve de ce séquent dont la dernière règle est une règle logique à droite. Or les seules règles logiques à droite ayant une formule de la forme $A \vee B$ dans la partie droite de leur séquent conclusion sont les règles $\vee_{d_1}$ et $\vee_{d_2}$ et la dernière étape de la démonstration est donc l'une des deux suivantes :

$$\frac{\vdash A}{\vdash A \vee B} \vee_{d_1} \qquad \frac{\vdash B}{\vdash A \vee B} \vee_{d_2}$$

et donc, soit $\vdash A$ dans le premier cas, soit $\vdash B$ dans le deuxième cas, sont prouvables.

# Propriété d'existence (EP)

**Propriété d'existence.** Si un séquent $\vdash \exists x \cdot A$ est prouvable en logique intuitionniste, alors il existe au moins un terme $t$ tel que le séquent $\vdash [t/x]A$ soit prouvable.

**Démonstration.** Si le séquent est prouvable, il existe une preuve de ce séquent dont la dernière règle est une règle logique à droite. Or le seule règle logique à droite ayant une formule de la forme $\vdash \exists x \cdot A$ est la règle $\exists_d$. La dernière étape de la démonstration est donc :

$$\frac{\vdash [t/x]A}{\vdash \exists x \cdot A}\ \exists_d$$

on y voit un terme $t$ tel que $\vdash [t/x]A$ est prouvable.

# Caractérisation d'une logique intuitionniste

Les propriétés de disjonction (DP) et d'existence (EP) sont considérées comme caractéristiques d'un système de logique intuitionniste.

**Rappel : sémantique intuitionniste des preuves**

La preuve d'un disjonction $A \vee B$, i.e. $A$ *ou* $B$, est formée d'une preuve de $A$ ou bien d'une preuve de $B$ plus une indication permettant de savoir lequel a été prouvé.

La preuve d'une quantification existentielle, $\forall x \cdot A(x)$, est la donnée d'un processus effectivement calculable qui transforme tout élément $t$ du domaine de quantification en une preuve de $A(t)$.

# Propriété de la sous-formule

**Définition.** On définit la notion de *sous-formule* d'une formule $A$ par induction sur la structure de la formule $A$. Plus précisément, on définit $SF(A)$ l'ensemble des sous-formules de $A$. Attention ! Sous-formule est pris au sens large, ce n'est pas la définition naturelle d'une sous-formule d'une formule $A$.

- Si $A$ est une formule atomique, $SF(A) = \{A\}$.
- Si $A \equiv \neg B$, $SF(A) = \{A\} \cup SF(B)$.
- Si $A \equiv B \vee C$ ou si $A \equiv B \wedge C$ ou si $A \equiv B \Rightarrow C$ alors : $SF(A) = \{A\} \cup SF(B) \cup SF(C)$.
- Si $A \equiv \forall x \cdot B$ ou si $A \equiv \exists x \cdot B$ alors : $SF(A) = \{A\} \cup SF(B) \cup \bigcup_{t \ terme} SF([t/x]B)$.

# Propriété de la sous-formule

**Remarque.** Si l'on cherche à démontrer un séquent $\Gamma \vdash A$, on possède la conclusion, i.e. le futur théorème, et l'on recherche la dernière règle de la preuve. Dans tous les cas, cette dernière règle pourrait être la règle de coupure :

$$\frac{\Gamma \vdash A \quad \Gamma', A \vdash B}{\Gamma, \Gamma' \vdash B}$$

mais cette règle pose un problème : pour déterminer ses prémisses, il faut déterminer la formule $A$ qui a servi à faire la coupure et cela n'est pas évident même pour un humain censé être intelligent.

Mais si l'on sait qu'il existe une preuve sans coupure...

# Propriété de la sous-formule

**Propriété.** Si un séquent $\Gamma \vdash A$ est prouvable en logique intuitionniste alors il existe une preuve de ce séquent dont la dernière règle n'est pas une règle de coupure et dont les prémisses ne contiennent que des sous-formules de $A$ et des formules dans $\Gamma$.

**Démonstration.** On sait qu'il existe une preuve sans utilisation de la règle de coupure.

Puis on examine chacune des autres règles du calcul des séquents intuitionniste et on vérifie aisément que chacune de ces règles possède la propriété annoncée.

# Propriété de la sous-formule

**Propriété de la sous-formule.** Si un séquent $\Gamma \vdash A$ est prouvable en logique intuitionniste alors il existe une preuve de ce séquent qui ne contient aucune utilisation de la règle de coupure et telle que toutes les formules apparaissant dans cette preuve soient des sous-formules de $A$ ou des formules dans $\Gamma$.

**Démonstration.** La démonstration ne pose pas de problème et se fait par récurrence sur la hauteur de l'arbre de preuve. Si l'arbre de preuve est de hauteur 0, le séquent démontré est l'identité $A \vdash A$. Si la preuve est de hauteur $n+1$, sa dernière règle vérifie la propriété précédente et on applique l'hypothèse de récurrence à chacune des prémisses de la règle pour conclure.

# Démonstration automatique

En appliquant le résultat précédent, on automatise la recherche de preuve puisque pour chaque résultat à démontrer, il y a un nombre fini de règles applicables et que la manière de les appliquer est déterminée par la propriété de la sous-formule.

Seul le cas des quantificateurs peut amener à faire des choix *intelligents* si l'ensemble des termes est infini, ce qui est le cas dès qu'il y a au moins un symbole de fonction.

D'où le discours enthousiaste de certains selon lequel la propriété de la sous-formule est la clé de la démonstration automatique. Mais ce discours idéaliste est bien loin des réalités.

# Démonstration automatique

Comme nous allons le voir, la preuve sans coupure est obtenue par transformations successives de la preuve originale et sa *hauteur au pire* est hyper-exponentielle :

$$4^{4^{4^{\cdot^{\cdot^{\cdot^{4^{4^n}}}}}}}$$

en fonction $n$, la hauteur de la preuve avec coupures. Le nombre de niveaux de 4 est le **degré de la preuve** qui sera défini plus tard.

Pour une preuve de degré 3, la hauteur de la preuve sans coupure pourrait dépasser les capacités de l'univers puisqu'elle serait de l'ordre de $10^{150}$ alors que le nombre de protons pouvant être contenus dans l'univers est estimé inférieur à $10^{130}$.

# Démonstration automatique

La recherche de preuves sans coupures est donc surtout destinée aux démonstrateurs jouets pour la démonstration de quelques identités remarquables de l'algèbre des connecteurs.

Cependant, elle peut être utilisée de manière non-exclusive, avec des **heuristiques**.

# La démonstration du Hauptsatz de Gentzen

La transformation procède par transformations successives qui réduisent strictement une certaine mesure de la preuve.

Lorsque cette mesure devient nulle, c'est que la preuve ne contient plus de coupures.

Pour définir cette mesure, on introduit la notion de degré d'une formule, d'une coupure et d'une preuve.

# Degré d'une formule

**Définition.** Le *degré d'une formule* $A$, noté $\delta(A)$, est défini inductivement par :

- si $A$ est atomique, $\delta(A) = 1$ ;
- $\delta(A \wedge B) = \delta(A \vee B) = \delta(A \Rightarrow B) = max(\delta(A), \delta(B)) + 1$ ;
- $\delta(\neg A) = \delta(\forall x \cdot A) = \delta(\exists x \cdot A) = \delta(A) + 1$ ;

où $A$ et $B$ sont des formules.

**Propriété.** Si $A$ est une formule, $t$ un terme et $x$ une variable, on a :

$$\delta([t/x]A) = \delta(A)$$

**Démonstration.** Induction évidente. À faire.

# Degré d'une coupure

**Définition.** Le *degré d'une coupure* intuitionniste (cas où $\Delta$ est une séquence vide de formule et $\Delta'$ est une séquence à 0 ou 1 formule) ou classique :

$$\frac{\Gamma \vdash \Delta, A \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

est le degré de la formule $A$qui a servi à faire la coupure.

# Degré d'une preuve

**Définition.** Le *degré d'une preuve* est le maximum des degrés des coupures utilisées dans la preuve.

**Remarque.** Le degré d'une formule n'est jamais nul. Donc le degré d'une coupure n'est jamais nul. Donc une preuve est de degré zéro si et seulement si elle est sans coupure.

# La proposition principale

**Lemme.** Soit $d \geq 0$, soit $A$ une formule de degré $d$, soit $\Gamma \vdash \Delta, A$ un séquent dont la preuve est de degré strictement inférieur à $d$, soit $\Gamma', A \vdash \Delta'$ un autre séquent dont la preuve est aussi de degré strictement inférieur à $d$, on peut construire une preuve de $\Gamma, \Gamma' \vdash \Delta, \Delta'$ de degré strictement inférieur à $d$.

**Démonstration.** La preuve en est très longue et procède par examen des dernières règles des preuves de chacun des deux séquents. Il y a de nombreux cas. On se reportera à *PROOFS AND TYPES*, chapitre 13, cité en tête de ce chapitre.

# Démonstration

On distingue plusieurs cas :

- le cas où la dernière règle de la preuve du séquent $\Gamma \vdash \Delta, A$ est une règle à droite créant $A$ et la dernière règle du séquent $\Gamma', A \vdash \Delta'$ est unes règles à gauche correspondante ;
- le cas où l'un des deux séquents est un axiome, i.e. $A \vdash A$ ;
- les autres cas où la dernière règle de l'un des deux séquents est une règle structurelle ;
- les cas non principaux où l'on se contente d'effectuer une permutation pour obtenir l'un des deux séquents.

# Exemple

Supposons que $A \equiv B \wedge C$, que $A$ dans le séquent de gauche est créé par $\wedge_d$, que $A$ dans le séquent de droite est construits à gauche par $\wedge_{g_1}$, on remplace alors la preuve :

$$\dfrac{\dfrac{\Gamma_1 \vdash \Delta_1, B \quad \Gamma_2 \vdash \Delta_2, C}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, B \wedge C}\wedge_d \qquad \dfrac{\Gamma_3, B \vdash \Delta_3}{\Gamma_3, B \wedge C \vdash \Delta_3}\wedge_{g_1}}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_2, \Delta_3}(cut)$$

par la preuve :

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma_1 \vdash \Delta_1, B \quad \Gamma_3, B \vdash \Delta_3}{\Gamma_1, \Gamma_3 \vdash \Delta_1, \Delta 3}(cut)}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_3}(aff_g^*, ch_g^*)}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_2, \Delta_3}(aff_d^*, ch_d^*)}$$

où $(aff_d^*, ch_d^*)$ signifie une suite d'affaiblissements à droite pour introduire $\Delta_2$ et une suite d'échanges à droite pour le placer. Smilairement pour $(aff_g^*, ch_g^*)$ avec $\Delta_2$. On a remplacé une coupure de degré $d = \delta(B \wedge C)$ par une coupure de degré $\delta(B) < d$ mais la hauteur de l'arbre a augmenté.

# Proposition

**Proposition.** Si $\pi$ est la preuve d'un séquent de degré $d > 0$, on peut construire une preuve $\omega(\pi)$ du même séquent mais de degré strictement inférieur à $d$.

**Démonstration.** La démonstration se fait par induction sur la hauteur de la preuve $\pi$. On considère la dernière règle $r$ de la preuve $\pi$. Si ce n'est pas une coupure, on applique l'hypothèse d'induction aux preuves de ses prémisses et le résultat est immédiat.

Si c'est une coupure de degré strictement inférieur à $d$, ici aussi on applique l'hypothèse d'induction aux preuves de ses prémisses et le résultat est immédiat.

*(suite ->)*

# Proposition

Si $r$ est une coupure de degré $d$, l'hypothèse d'induction nous assure qu'on peut trouver des preuves de ses prémisses de degré strictement inférieur à $d$ de sorte que $r$ est la seule coupure de degré au moins $d$. On a donc une coupure :

$$\frac{\Gamma \vdash \Delta, A \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

avec $A$ de degré $d$. Le lemme ci-dessus permet immédiatement de conclure.

# Le théorème

**Théorème.** Si un séquent est prouvable alors il est prouvable avec une preuve sans coupure.

**Démonstration.** Par application du lemme précédent.

# Conclusion

Le théorème d'élimination des coupures de Gentzen est long et fastidieux à démontrer.

Mais il permet de prouver bien des choses...