

Jean Goubault-Larrecq

λ -calcul

7. Recherche de preuves, autres logiques propositionnelles

$$\begin{array}{c} \frac{}{\Gamma, x : F \vdash x : F} (Var) \\ \frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2} (App) \quad \frac{\Gamma, y : F_1 \vdash u[x := y] : F_2 \quad (y \notin \text{dom } \Gamma, y \notin \text{fv}(u))}{\Gamma \vdash \lambda x \cdot u : F_1 \Rightarrow F_2} (Abs) \\ \frac{\Gamma \vdash u : F_1 \wedge F_2}{\Gamma \vdash \pi_i u : F_i} (\wedge E_i), i = 1, 2 \quad \frac{\Gamma \vdash u : F_1 \quad \Gamma \vdash v : F_2}{\Gamma \vdash \langle u, v \rangle : F_1 \wedge F_2} (\wedge I) \\ \frac{\Gamma \vdash u : F_1 \vee F_2 \quad \Gamma, x_1 : F_1 \vdash v_1 : F \quad \Gamma, x_2 : F_2 \vdash v_2 : F}{\Gamma \vdash \text{case } u \left\{ \begin{array}{l} \iota_1 x_1 \mapsto v_1 \\ \iota_2 x_2 \mapsto v_2 \end{array} \right\} : F} (\vee E) \quad \frac{\Gamma \vdash u : F_i}{\Gamma \vdash \iota_i u : F_1 \vee F_2} (\vee I_i), i = 1, 2 \end{array}$$

Aujourd'hui

- ❖ Suite de notre étude du λ -calcul simplement typé:
recherche de preuve en logique propositionnelle intuitionniste **minimale**
- ❖ Nouveaux connecteurs logiques: $\wedge, \vee, \perp, \neg$
 $\rightarrow$ logique propositionnelle **intuitionniste**
- ❖ Logique propositionnelle **classique**

Recherche de preuve

(en logique propositionnelle)

Recherche de preuve

$$\begin{array}{c}
 \frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2} (\Rightarrow E) \quad \frac{\frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I) \quad \frac{\Gamma, F \vdash F}{\Gamma, F \vdash F} (Ax)}{\Gamma, F \vdash F} \text{« logique minimale en déduction naturelle »}
 \end{array}$$

- ❖ **Problème (prouvabilité).** En entrée, un jugement $\Gamma \vdash F$
Question: est-il dérivable?
- ❖ I.e., y a-t-il une dérivation dont la conclusion est $\Gamma \vdash F$?

Recherche de preuve

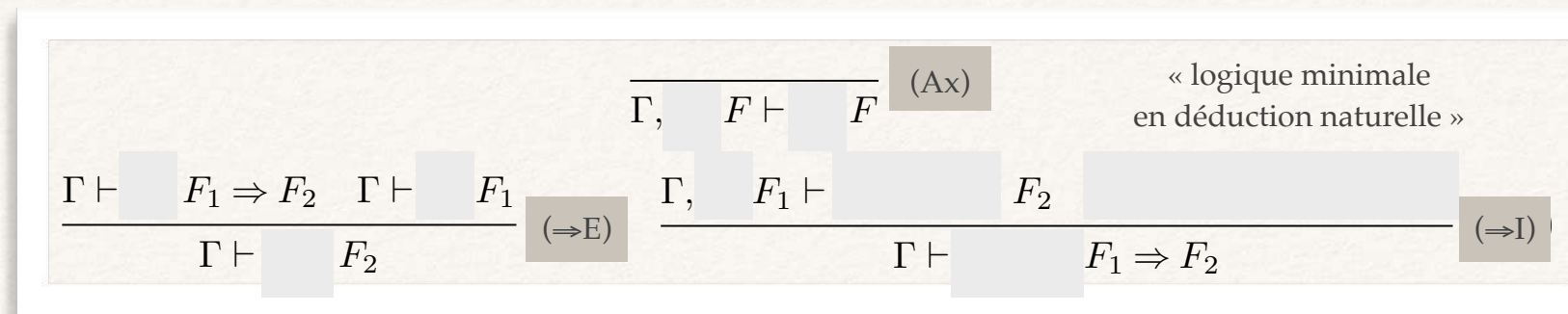
$$\begin{array}{c}
 \frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2} (\Rightarrow E) \quad \frac{\frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I) \quad \frac{\Gamma, F \vdash F}{\Gamma, F \vdash F} (Ax)}{\Gamma, F \vdash F} \text{« logique minimale en déduction naturelle »}
 \end{array}$$

❖ **Problème.** En entrée, un jugement $\Gamma \vdash F$

Question: est-il dérivable?

❖ Idée: chercher en arrière.

Exemple: peut-on montrer $\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F$?



$$\frac{}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F}$$

quelle règle pourrait-on appliquer pour obtenir ce jugement?

$$\begin{array}{c}
 \frac{\Gamma \vdash \boxed{F_1 \Rightarrow F_2} \quad \Gamma \vdash \boxed{F_1}}{\Gamma \vdash \boxed{F_2}} (\Rightarrow E) \quad \frac{\overline{\Gamma, \boxed{F} \vdash \boxed{F}} (Ax) \quad \Gamma, \boxed{F_1} \vdash \boxed{F_2} \quad \boxed{\text{« logique minimale en déduction naturelle »}}}{\Gamma \vdash \boxed{F_1 \Rightarrow F_2}} (\Rightarrow I)
 \end{array}$$

$$\frac{(F \Rightarrow G) \Rightarrow F \vdash F}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow I)$$

oui, bien sûr, c'est la possibilité la plus évidente; continuons

$$\begin{array}{c}
 \frac{\Gamma \vdash \boxed{F_1 \Rightarrow F_2} \quad \Gamma \vdash \boxed{F_1}}{\Gamma \vdash \boxed{F_2}} (\Rightarrow E) \quad \frac{\overline{\Gamma, \boxed{F} \vdash \boxed{F}} (Ax) \quad \Gamma, \boxed{F_1} \vdash \boxed{F_2} \quad \boxed{}}{\Gamma \vdash \boxed{F_1 \Rightarrow F_2}} (\Rightarrow I)
 \end{array}$$

« logique minimale
en déduction naturelle »

$$\frac{\overline{(F \Rightarrow G) \Rightarrow F \vdash F}}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow I)$$

ah, mais que faire
ici?

$$\begin{array}{c}
 \frac{\Gamma \vdash \boxed{F_1 \Rightarrow F_2} \quad \Gamma \vdash \boxed{F_1}}{\Gamma \vdash \boxed{F_2}} (\Rightarrow E) \quad \frac{\overline{\Gamma, \boxed{F} \vdash \boxed{F}} (Ax) \quad \Gamma, \boxed{F_1} \vdash \boxed{F_2} \quad \boxed{}}{\Gamma \vdash \boxed{F_1 \Rightarrow F_2}} (\Rightarrow I)
 \end{array}$$

« logique minimale
en déduction naturelle »

on peut inventer
une nouvelle
formule H

... et espérer
pouvoir la
prouver

$$\frac{(F \Rightarrow G) \Rightarrow F \vdash H \Rightarrow F \quad (F \Rightarrow G) \Rightarrow F \vdash H}{(F \Rightarrow G) \Rightarrow F \vdash F} (\Rightarrow E)$$

$$\frac{(F \Rightarrow G) \Rightarrow F \vdash F}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow I)$$

- ❖ Telle quelle, la recherche de preuve est difficile à automatiser (besoin d'**inventer** des formules, plus grave encore que de devoir backtrack)
- ❖ Notamment, il n'est même pas clair que la prouvabilité soit **décidable**

en fait, on aurait déjà pu vouloir appliquer ($\Rightarrow E$), et inventer une formule ici... comment décider?

$$\frac{}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F}$$

quelle règle pourrait-on appliquer pour obtenir ce jugement?

Preuves en forme normale

- ❖ L'idée de Gerhard Gentzen (1934, 1936):
(qui l'a quand même appliquée directement à l'arithmétique, pas juste notre pauvre logique minimale...)
- ❖ Montrer que si $\Gamma \vdash F$ a une dérivation, alors il en a une en forme normale;
- ❖ et que les preuves en forme normale sont faciles à trouver (**aucune** formule à inventer)
- ❖ Bon, en fait, il n'y est pas arrivé en déduction naturelle, mais Dag Prawitz oui (1965)



<https://opc.mfo.de/photoNormal?id=8540>



https://pp-prod-admin.it.su.se/polopoly_fs/1.208175!/image/image.jpg_gen/derivatives/article_465/image.jpg

Preuves en forme normale

$$\begin{array}{c}
 \frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2} (\Rightarrow E) \quad \frac{\overline{\Gamma, F \vdash F} (Ax) \quad \Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I)
 \end{array}$$

« logique minimale en déduction naturelle »

- ❖ C'est tout simple: une preuve en **forme normale**, c'est une preuve dont le λ -terme est β -normal
- ❖ Mais avant, une petite parenthèse...

Une parenthèse: Curry-Howard

- ❖ On a déjà vu:
 - formule = type
 - preuve = programme
- ❖ Mais que signifie la β -réduction sur les preuves?

	Monde de la logique	Monde des programmes
F	formule	type
u	preuve	λ -terme (programme)
$u \rightarrow^* v$		β -réduction (exécution)



Détours

$$\begin{array}{c}
 \vdots^{\pi_1} \\
 \hline
 \Gamma, x:F \vdash u : G \\
 \hline
 \Gamma \vdash \lambda x.u : F \Rightarrow G \quad (\Rightarrow I)
 \end{array}
 \quad
 \begin{array}{c}
 \vdots^{\pi_2} \\
 \hline
 \Gamma \vdash v : F
 \end{array}
 \quad
 \begin{array}{c}
 \text{(voir preuve d'autoréduction,} \\
 \text{de la dernière fois)} \\
 \hline
 \Gamma \vdash (\lambda x.u)v : G \quad (\Rightarrow E)
 \end{array}
 \longrightarrow
 \begin{array}{c}
 \ll \pi_1[x:=\pi_2] \gg \\
 \text{(voir preuve du lemme 1} \\
 \text{dans le poly types.pdf)} \\
 \hline
 \Gamma \vdash u[x:=v] : G
 \end{array}$$

β -redex = **détour**:

on introduit un $\Rightarrow$,
pour l'éliminer juste après

(~ coupure en calcul des séquents,
voir cours de Gilles Dowek [pour les saclaisiens])

β -réduction =
élimination des détours

Une parenthèse: Curry-Howard

- ❖ On a déjà vu:
 - formule = type
 - preuve = programme
- ❖ Mais que signifie la β -réduction sur les preuves?

	Monde de la logique	Monde des programmes
F	formule	type
u	preuve	λ -terme (programme)
$u \rightarrow^* v$		β -réduction (exécution)



Une parenthèse: Curry-Howard

- ❖ On a déjà vu:
 - formule = type
 - preuve = programme
- ❖ La β -réduction est **l'élimination des détours**
- ❖ Un λ -terme normal est **une preuve sans détour**

	Monde de la logique	Monde des programmes
F	formule	type
u	preuve	λ -terme (programme)
$u \rightarrow^* v$	élimination des détours	β -réduction (exécution)

Revenons à notre problème

- ❖ L'idée de Gerhard Gentzen (1934, 1936):
(qui l'a quand même appliquée directement à l'arithmétique, pas juste notre pauvre logique minimale...)
- ❖ Montrer que si $\Gamma \vdash F$ a une dérivation, alors il en a une en forme normale;
= preuve sans détour
- ❖ et que les preuves en forme normale sont faciles à trouver (aucune formule à inventer)
- ❖ Bon, en fait, il n'y est pas arrivé en déduction naturelle, mais Dag Prawitz oui (1965)



<https://opc.mfo.de/photoNormal?id=8540>



Preuves sans détour

$$\begin{array}{c}
 \lambda\text{-calcul simplement typé} \\
 \text{« logique minimale en déduction naturelle »} \\
 \hline
 \frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2} (\Rightarrow E) \quad \frac{\Gamma, F_1 \vdash F \quad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I)}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I)
 \end{array}$$

- ❖ C'est tout simple: une preuve **sans détour**, c'est une preuve dont le λ -terme est **β -normal**
- ❖ Refaisons apparaître les λ -termes
- ❖ Un terme β -normal est une **forme normale de tête**

$$\lambda x_1, \dots, x_n . x \ u_1 \ \dots \ u_m$$

dont les arguments $u_1, \dots, u_m$ sont eux-mêmes β -normaux

Typage des formes normales

- ❖ Nos règles de typage typent **tous** les λ -termes
- ❖ Nous allons créer de nouvelles règles de typage qui ne typent plus **que** les formes β -normales, en utilisant que ce sont des formes normales de tête itérées

Typage des formes normales

$$\frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I)$$

$$\frac{\Delta \vdash u_1 : F_1 \quad \dots \quad \Delta \vdash u_m : F_m}{\Delta \vdash x u_1 \dots u_m : F} (BC)$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_m \Rightarrow F$

avec le même F , d'accord?

- ❖ Par s Réessayons de démontrer $\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F$
- ❖ une règle $(\Rightarrow^+I)$ qui introduit les abstractions
- ❖ une règle (BC) [« backchain »] pour les applications

$$\begin{array}{c}
 \frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I) \\
 \\
 \frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x \ u_1 \dots u_m : F} (BC)
 \end{array}$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F$

$$\frac{}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F}$$

quelle règle pourrait-on appliquer pour obtenir ce jugement?

$$\begin{array}{c}
\frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I) \\
\\
\frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x \ u_1 \dots u_m : F} (BC)
\end{array}$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F$

$$\frac{(F \Rightarrow G) \Rightarrow F \vdash F}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow^+I)$$

oui: c'est la **seule**
règle applicable

$$\begin{array}{c}
 \frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} \quad (\Rightarrow^+I) \\
 \\
 \frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x \ u_1 \dots u_m : F} \quad (BC)
 \end{array}$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F$

$$\frac{\frac{}{(F \Rightarrow G) \Rightarrow F \vdash F}}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} \quad (\Rightarrow^+I)$$

ah, mais que faire
ici?

$$\begin{array}{c}
 \frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I) \\
 \\
 \frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x \ u_1 \dots u_m : F} (BC)
 \end{array}$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F$

$$\Delta \left\langle \frac{(F \Rightarrow G) \Rightarrow F \vdash F \Rightarrow G}{(F \Rightarrow G) \Rightarrow F \vdash F} (BC) \right\rangle \frac{}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow^+I)$$

oui: c'est la **seule**
règle applicable

$$\begin{array}{c}
 \frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I) \\
 \\
 \frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x u_1 \dots u_m:F} \text{ (BC)} \\
 \text{où } \Delta \text{ contient } x:F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F
 \end{array}$$

aucune règle ne s'applique:
le jugement donné n'est
pas dérivable

et maintenant?

encore une fois,
c'est la **seule**
règle applicable

$$\begin{array}{c}
 \frac{(F \Rightarrow G) \Rightarrow F, F \vdash G}{(F \Rightarrow G) \Rightarrow F \vdash F \Rightarrow G} (\Rightarrow^+I) \\
 \frac{(F \Rightarrow G) \Rightarrow F \vdash F \Rightarrow G}{(F \Rightarrow G) \Rightarrow F \vdash F} \text{ (BC)} \\
 \frac{(F \Rightarrow G) \Rightarrow F \vdash F}{\vdash ((F \Rightarrow G) \Rightarrow F) \Rightarrow F} (\Rightarrow^+I)
 \end{array}$$

La loi de Peirce



Charles Sanders Peirce

Domaine public,

<https://commons.wikimedia.org/w/index.php?curid=128147>

- ❖ La formule $((F \Rightarrow G) \Rightarrow F) \Rightarrow F$ est la **loi de Peirce** (prononcé « peurse », pas « pirce »)
- ❖ Elle est exprimable mais **pas démontrable** en logique intuitionniste minimale
- ❖ Et pourtant elle est valide en logique classique!
- ❖ ... si F est vraie, alors $((F \Rightarrow G) \Rightarrow F) \Rightarrow F$ est vraie
- ❖ ... si F est fausse, $F \Rightarrow G$ est vraie,
donc $(F \Rightarrow G) \Rightarrow F$ est fausse
donc $((F \Rightarrow G) \Rightarrow F) \Rightarrow F$ est vraie

n'importe quoi
implique **vrai**

faux implique
n'importe quoi

La loi de Peirce



- ❖ La formule $((F \Rightarrow G) \Rightarrow F) \Rightarrow F$
est la **loi de Peirce** (prononcé « peurse », pas « pirce »)
- ❖ Elle est exprimable mais **pas démontrable** Charles Sanders Peirce
en logique intuitionniste minimale <https://commons.wikimedia.org/w/index.php?curid=128147> Domaine public,
- ❖ (En fait, logique classique = intuitionniste+Peirce)

Prouvabilité

- ❖ **Thm (R. Statman 1979).** La prouvabilité en logique propositionnelle intuitionniste minimale est décidable, et **PSPACE**-complète.
(en logique classique, c'est **NP**-complet, ce qui est *beaucoup* plus bas; vous verrez **PSPACE** avec S. Haddad à Paris-Saclay: c'est la classe des problèmes décidables en espace polynomial et temps arbitraire.)
- ❖ ... mais la procédure de recherche par $(\Rightarrow^+I)$ et (BC) n'est pas suffisante pour ça (voir suite)

Richard Statman



Le 1er problème: non-déterminisme inutile

$$\begin{array}{c}
 \frac{\Gamma, x_1:F_1, \dots, x_n:F_n \vdash u:F}{\Gamma \vdash \lambda x_1, \dots, x_n. u : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F} (\Rightarrow^+I) \\
 \\
 \frac{\Delta \vdash u_1:F_1 \quad \dots \quad \Delta \vdash u_m:F_m}{\Delta \vdash x u_1 \dots u_m : F} (BC)
 \end{array}$$

où Δ contient $x : F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow F$

- ❖ Essayez de prouver $F \Rightarrow G \Rightarrow F$
 - ❖ Facile, d'accord, mais imaginez comment procédera l'algorithme de recherche de preuve suggéré ici
- voir tester non déterministique $(\Rightarrow^+I)$ avec $n=1$ ou $n=2$

mais celui-là est possible aussi! et si l'essai de droite n'aboutit pas à une preuve, il faudra en principe backtracker et essayer celui-ci

$$\frac{F \vdash G \Rightarrow F}{\vdash F \Rightarrow G \Rightarrow F} (\Rightarrow^+I)_{(n=1)}$$

$$\frac{F, G \vdash F}{\vdash F \Rightarrow G \Rightarrow F} (\Rightarrow^+I)_{(n=2)}$$

oui, celui-ci, c'est celui auquel vous avez certainement pensé...

... et c'est effectivement inutile, voir la suite

La η -expansion

- ❖ (Je reviens temporairement au système de typage usuel)

$$\frac{}{\Gamma, x : F \vdash x : F} (Var) \quad \frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2} (App) \quad \frac{\Gamma, y : F_1 \vdash u[x := y] : F_2 \quad (y \notin \text{dom } \Gamma, y \notin \text{fv}(u))}{\Gamma \vdash \lambda x . u : F_1 \Rightarrow F_2} (Abs)$$

- ❖ De même que la β -réduction est l'élimination des détours,
- ❖ la **η -expansion** élimine les cas d'axiomes sur des formules non atomiques:

$$\frac{}{\Gamma, x:F \Rightarrow G \vdash x:F \Rightarrow G} (Ax) \longrightarrow$$

(cas particulier de (BC) avec $n=0$)

$$\frac{\frac{}{\Gamma, x:F \Rightarrow G, y:F \vdash y:F} (Ax)}{\Gamma, x:F \Rightarrow G, y:F \vdash xy:G} (BC) \quad \frac{}{\Gamma, x:F \Rightarrow G \vdash \lambda y.xy:F \Rightarrow G} (\Rightarrow^+I)$$

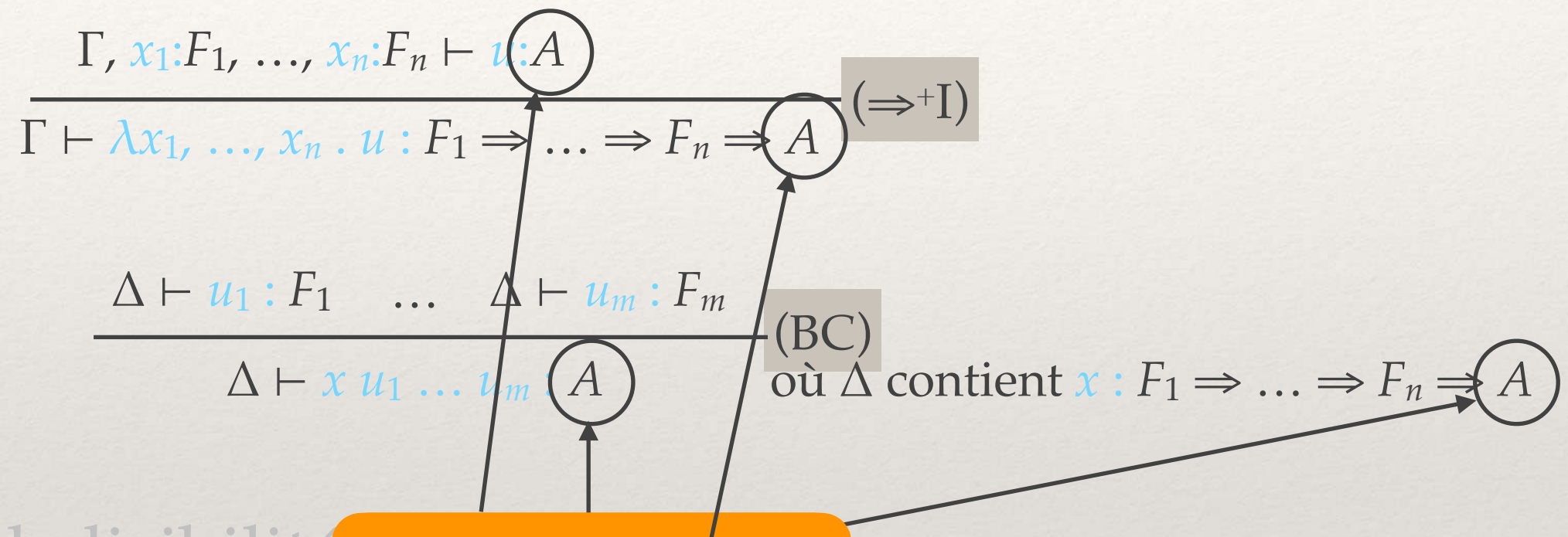
(oui, c'est la η -réduction à l'envers)

La η -expansion

- ❖ Je ne vais pas rentrer dans les détails, mais:
- ❖ sur les formes β -normales bien typées, la η -expansion termine, sur une forme β -normale dite **η -longue** (voir `poly types.pdf`, exercice 12 p.12)
- ❖ on peut former un système de typage qui ne type plus que les formes **β -normales η -longues**

The diagram illustrates the η -expansion rule. It shows a typing derivation starting from $\Gamma, x:F \Rightarrow G \vdash x:F \Rightarrow G$ with a label (Ax) . An arrow points to a more complex derivation. This derivation has two main branches. The left branch is $\Gamma, x:F \Rightarrow G, y:F \vdash x:F \Rightarrow G$ with a label (Ax) . The right branch is $\Gamma, x:F \Rightarrow G, y:F \vdash y:F$ with a label $(\Rightarrow)$. These two branches are combined under a single line, which then leads to $\Gamma, x:F \Rightarrow G, y:F \vdash xy:G$ with a label $(\Rightarrow I)$. Finally, this leads to the conclusion $\Gamma, x:F \Rightarrow G \vdash \lambda y.xy:F \Rightarrow G$ with a label $(\Rightarrow I)$.

Typage des formes β -normales η -longues



- ❖ Par souci de lisibilité
- ❖ une règle $(\Rightarrow^+I)$ qui introduit les abstractions
- ❖ une règle (BC) [« back »] pour les applications

Seule nouveauté:
 A est une **formule atomique**
 (un type de base)

1er problème: résolu

Réessayons de démontrer $F \Rightarrow G \Rightarrow F$
(je suppose F atomique)

Nous avons deux possibilités:

$$\frac{F \vdash G \Rightarrow F}{\vdash F \Rightarrow G \Rightarrow F} \begin{array}{l} (\Rightarrow^+I) \\ (n=1) \end{array}$$

$$\frac{F, G \vdash F}{\vdash F \Rightarrow G \Rightarrow F} \begin{array}{l} (\Rightarrow^+I) \\ (n=2) \end{array}$$

1er problème: résolu

Réessayons de démontrer $F \Rightarrow G \Rightarrow F$
(je suppose F atomique)

Nous avons deux possibilités... plus maintenant:

impossible:
 $G \Rightarrow F$ pas atomique

$$\frac{F \vdash G \Rightarrow F}{\vdash F \Rightarrow G \Rightarrow F} \begin{matrix} (\Rightarrow^+I) \\ (n=1) \end{matrix}$$

c'est maintenant la
seule règle applicable

$$\frac{F, G \vdash F}{\vdash F \Rightarrow G \Rightarrow F} \begin{matrix} (\Rightarrow^+I) \\ (n=2) \end{matrix}$$

1er problème: résolu

Réessayons de démontrer $F \Rightarrow G \Rightarrow F$
(je suppose F atomique)

Nous avons deux possibilités... plus maintenant:

impossible:
 $G \Rightarrow F$ pas atomique

$$\frac{F \vdash G \Rightarrow F}{\vdash F \Rightarrow G \Rightarrow F} \begin{matrix} (\Rightarrow^+I) \\ (n=1) \end{matrix}$$

fini!

$$\frac{\frac{}{F, G \vdash F} (Ax)}{\vdash F \Rightarrow G \Rightarrow F} \begin{matrix} (\Rightarrow^+I) \\ (n=2) \end{matrix}$$

2ème problème: bouclage

$$\begin{array}{c}
 \vdots \\
 \hline
 A \Rightarrow A \vdash A \quad (\text{BC}) \\
 \hline
 A \Rightarrow A \vdash A \quad (\text{BC}) \\
 \hline
 A \Rightarrow A \vdash A \quad (\text{BC}) \\
 \hline
 \vdash (A \Rightarrow A) \Rightarrow A \quad (\Rightarrow^+ \text{I})
 \end{array}$$

c'est ballot, hein?

- ❖ Solution: **tests de bouclage**: si on retombe sur un jugement déjà vu plus bas, backtracker
- ❖ Les seuls cas de backtracking sont le choix de la formule $F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow A$ dans (BC)

$$\frac{\Delta \vdash F_1 \quad \dots \quad \Delta \vdash F_m}{\Delta \vdash A} (\text{BC})$$

où Δ contient $F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow A$

3ème problème: bouclage

$$\begin{array}{c}
 \vdots \\
 \frac{(A \Rightarrow B) \Rightarrow B, A, A \vdash B}{(A \Rightarrow B) \Rightarrow B, A \vdash A \Rightarrow B} (\Rightarrow^+I) \\
 \frac{(A \Rightarrow B) \Rightarrow B, A \vdash A \Rightarrow B}{(A \Rightarrow B) \Rightarrow B, A \vdash B} (BC) \\
 \frac{(A \Rightarrow B) \Rightarrow B, A \vdash B}{(A \Rightarrow B) \Rightarrow B \vdash A \Rightarrow B} (\Rightarrow^+I) \\
 \frac{(A \Rightarrow B) \Rightarrow B \vdash A \Rightarrow B}{(A \Rightarrow B) \Rightarrow B \vdash B} (BC) \\
 \frac{(A \Rightarrow B) \Rightarrow B \vdash B}{\vdash ((A \Rightarrow B) \Rightarrow B) \Rightarrow B} (\Rightarrow^+I)
 \end{array}$$

- ❖ On doit raffiner les tests de bouclage:
backtracker si on retrouver le même jugement
en ignorant les duplications de formules (je ne justifierai pas cela formellement)

$$\frac{\Delta \vdash F_1 \quad \dots \quad \Delta \vdash F_m}{\Delta \vdash A} (BC)$$

où Δ contient $F_1 \Rightarrow \dots \Rightarrow F_n \Rightarrow A$

Recherche de preuve

- ❖ Tout ceci permet de démontrer:
- ❖ **Thm.** Le problème de prouvabilité en logique intuitionniste minimale est **décidable**.
- ❖ (Prouver que c'est **PSPACE**-complet est une autre paire de manches. La procédure que nous avons donnée est dans la classe encore plus grande **coNEXPTIME**.)

Cohérence

Cohérence

- ❖ « consistant » en anglais; certains disent « consistante » en français, mais ce sont les **soupes** qui sont consistantes... si elle sont bien denses.
- ❖ ordinairement, une logique est cohérente si on ne peut pas y démontrer le **faux**; mais ici, nous n'avons pas de formule « faux »... et dans une logique avec « faux », on peut tout démontrer: donc une logique est cohérente si on ne peut pas en démontrer toutes les formules!
- ❖ **Th. n.** La logique prop. intuitionniste minimale est **cohérente**: il existe une formule F qu'on ne peut pas démontrer (i.e., on ne peut pas dériver $\vdash F$).
- ❖ *Preuve*: tous les exemples qu'on a vus (Peirce, $(A \Rightarrow A) \Rightarrow A$, $((A \Rightarrow B) \Rightarrow B) \Rightarrow B$), mais aussi juste A , où A est une formule atomique. $\square$

Cohérence

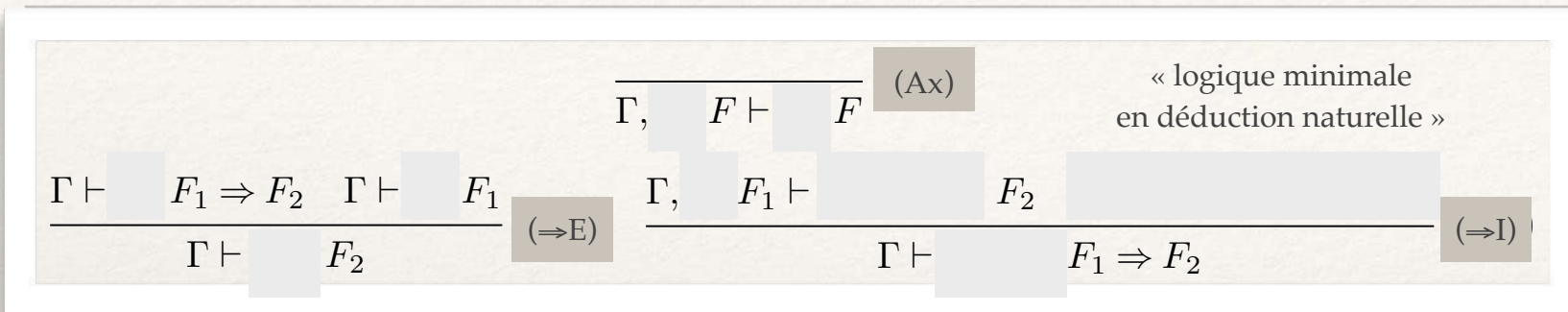
- ❖ Notre stratégie pour montrer la cohérence:
 - il n'y a pas de λ -terme normal u tel que $\vdash u : A$
 - si A avait une preuve, il aurait une preuve normale (théorème de **normalisation forte**)

Cohérence

- ❖ Notre stratégie pour montrer la cohérence:
 - il n'y a pas de λ -terme normal u tel que $\vdash u : A$
 - si A avait une preuve, il aurait une preuve normale (théorème de **normalisation forte**)

C'est quand même un marteau-pilon
pour écraser une mouche!

Cohérence: une preuve plus simple



❖ On définit une **sémantique**...

à 2 valeurs de vérité (0=faux, 1=vrai)

$\llbracket F \Rightarrow G \rrbracket \rho = \llbracket F \rrbracket \rho \Rightarrow \llbracket G \rrbracket \rho$, voir:

(c'est quand même plus simple que les candidats de réductibilité!)

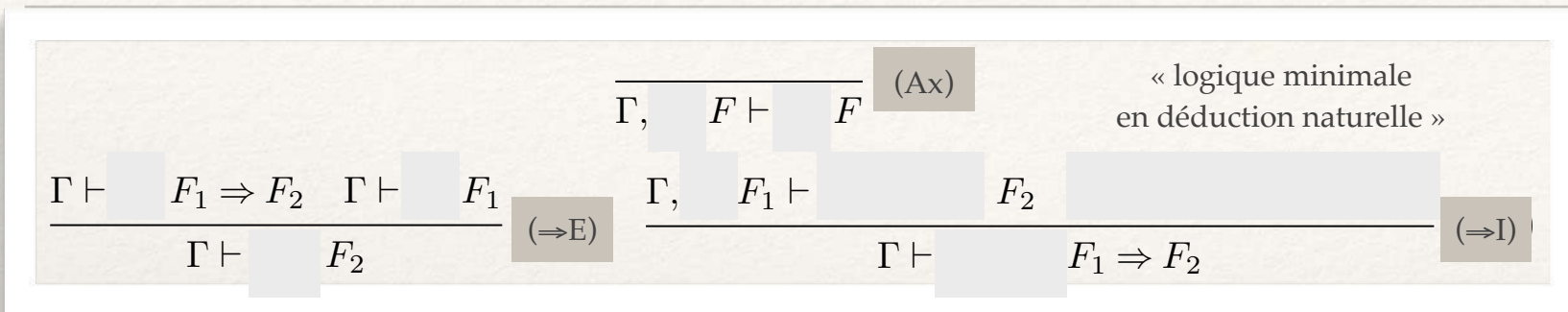
n'importe quoi
implique vrai

$\Rightarrow$	0	1
0	1	1
1	0	1

faux
implique
n'importe
quoi

❖ $\llbracket A \rrbracket \rho = \rho(A)$ — ρ est un **environnement**
qui à chaque formule atomique
associe sa valeur de vérité

Cohérence: une preuve plus simple



n'importe quoi
implique vrai

- ❖ On vérifie que tout jugement dérivable $F_1, \dots, F_n \vdash F$ est **valide**: pour tout ρ tel que $\llbracket F_1 \rrbracket \rho = \dots = \llbracket F_n \rrbracket \rho = 1$, on a $\llbracket F \rrbracket \rho = 1$ (récurrence sur la dérivation)

$\Rightarrow$	0	1
0	1	1
1	0	1

faux
implique
n'importe
quoi

- ❖ Donc un jugement non valide
(par exemple $\vdash A$: prendre $\rho(A)=0$)
n'est pas dérivable.

Incomplétude

$$\begin{array}{c}
 \frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2} (\Rightarrow E) \quad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2} (\Rightarrow I) \quad \frac{}{\Gamma, F \vdash F} (Ax) \\
 \text{« logique minimale en déduction naturelle »}
 \end{array}$$

- ❖ Tout jugement dérivable est valide, mais la réciproque est **fausse**:
- ❖ la formule de Peirce

$$((F \Rightarrow G) \Rightarrow F) \Rightarrow F$$

est valide, mais pas dérivable en logique **intuitionniste**
 (... minimale, mais ça n'est pas très important)

- ❖ normalement, Stéphane devrait vous parler de la sémantique de **Kripke** — qui, elle, est complète.

n'importe quoi
implique vrai

$\Rightarrow$	0	1
0	1	1
1	0	1

faux
implique
n'importe
quoi

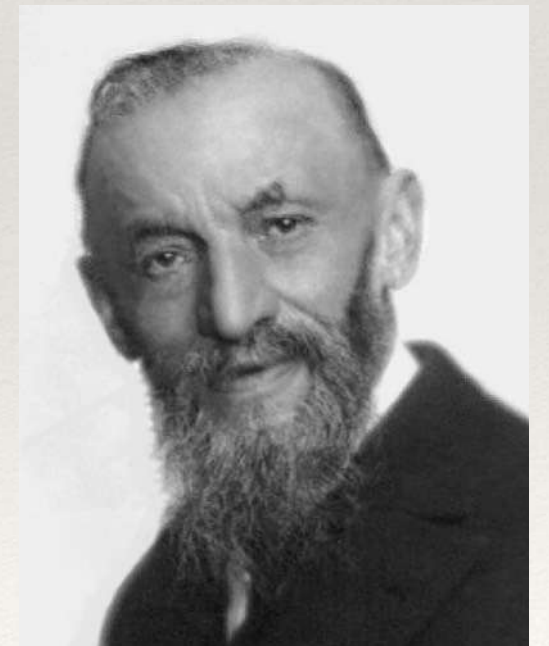
Saul Aaron Kripke



Cohérence

- ❖ En résumé, on a fait une preuve de cohérence de la logique prop. intuitionniste minimale **extraordinairement compliquée.**
- ❖ A quoi ça sert?
- ❖ Pour la cohérence de cette logique, à rien.
- ❖ Mais plus tard, on fera l'arithmétique de Peano, et ça sera une autre histoire!

Giuseppe Peano



Autres connecteurs logiques

(à commencer par le faux)

Le faux

- ❖ J'ai donné une définition tordue de la cohérence, au motif qu'on n'avait pas de **faux**
- ❖ Rajoutons-le!

Voilà ce qu'on ajoute:

❖ Types (formules):

$F, G, \dots ::= A$

| $F \Rightarrow G$

| $\perp$ (« faux »)

du faux on
peut déduire
n'importe quoi

$\frac{\Gamma \vdash u : \perp}{\Gamma \vdash \nabla u : G} (\perp E)$

❖ Termes:

$u, v, \dots ::= x$

| uv

| $\lambda x.u$

| ∇u

❖ Réduction:

$(\beta) (\lambda x.u)v \rightarrow u[x:=v]$

$(\nabla) (\nabla u)v \rightarrow \nabla u$

élimination du faux
(... et pas d'intro du faux!)

$\frac{}{\Gamma, x:F \vdash x : F} (Ax)$

$\frac{\Gamma \vdash u : F \Rightarrow G \quad \Gamma \vdash v : F}{\Gamma \vdash uv : G} (\Rightarrow E)$

$\frac{\Gamma, x:F \vdash u : G}{\Gamma \vdash \lambda x.u : F \Rightarrow G} (\Rightarrow I)$

Autoréduction

- ❖ La règle $(\nabla u)v \rightarrow \nabla u$ correspond à la simplification de preuve:

$$\frac{\frac{\frac{\vdots \pi_1}{\Gamma \vdash u : \perp}}{\Gamma \vdash \nabla u : F_1 \Rightarrow F_2} (\perp E) \quad \frac{\vdots \pi_2}{\Gamma \vdash v : F_1}}{\Gamma \vdash \nabla uv : F_2} (\Rightarrow E) \quad \rightarrow \quad \frac{\frac{\vdots \pi_1}{\Gamma \vdash u : \perp}}{\Gamma \vdash \nabla u : F_2} (\perp E)$$

- ❖ Ce n'est pas une élimination de détour à proprement parler: on n'en a pas besoin pour montrer la cohérence de la logique correspondante; mais c'est une simplification utile quand même.

Curry-Howard de nouveau

- ❖ Un programme de type $\perp$ ne **termine pas normalement** ... pensez-y comme à un programme qui a appelé la primitive `abort ( )` en C ou une exception non capturée en Caml
- ❖ Si $u : \perp$, alors ∇u est un **cast** vers un type arbitraire F « de toute façon, le résultat qu'il (ne) retourne (pas) est de type F »
- ❖ La règle $(\nabla u)v \rightarrow \nabla u$ propage l'exception.

VALEUR RENVOYÉE

La fonction **abort()** ne revient jamais.

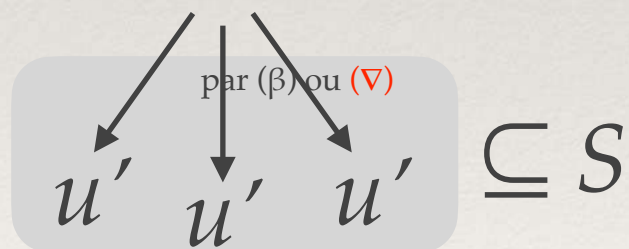
<http://manpagesfr.free.fr/man/man3/abort.3.html>

Normalisation forte

- ❖ **Thm.** Tout terme typable (dans ce nouveau système de types) est fortement normalisable.
- ❖ La démonstration est comme la dernière fois...
je vous montre juste les changements (en rouge).

Candidats de réductibilité

- ❖ Un ensemble de $\lambda \nabla$ -termes S est un **candidat de réductibilité** si et seulement si:
- ❖ (CR1) $S \subseteq SN$ *(SN = les fortement normalisables pour $(\beta) + (\nabla)$)*
- ❖ (CR2) si $u \in S \xrightarrow{\text{par } (\beta) \text{ ou } (\nabla)} u'$ alors $u' \in S$ *(on suit les réductions en avant)*
- ❖ (CR3) si u neutre alors $u \in S$ *(réductions en arrière)*



où u **neutre** ssi ne commence ni par λ **ni par** ∇ .

Candidats de réductibilité

(CR1) $S \subseteq \text{SN}$

(CR2) si $u \in S \rightarrow u'$ alors $u' \in S$

(CR3) si $\begin{array}{c} u \text{ neutre} \\ \swarrow \quad \downarrow \quad \searrow \\ u' \quad u' \quad u' \end{array} \subseteq S$ alors $u \in S$

- ❖ **Lemme A.** Si S et S' sont des candidats de réductibilité, alors $S \Rightarrow S'$ aussi.

$$S \Rightarrow S' = \{u \mid \forall v \in S, uv \in S'\}$$

(Preuve: comme la dernière fois.)

- ❖ On pose $\text{RED}_A = \text{SN}$ pour toute formule atomique A ,
 $\text{RED}_{F \Rightarrow G} = \text{RED}_F \Rightarrow \text{RED}_G$,
 $\text{RED}_\perp = \text{SN}$

- ❖ SN vérifie (CR1)–(CR3) (facile). Donc:

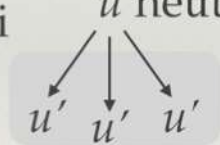
- ❖ **Lemme B.** Pour tout type F , RED_F est un candidat.

(Preuve: par récurrence sur F .)

Un lemme utile

(CR1) $S \subseteq \text{SN}$

(CR2) si $u \in S \rightarrow u'$ alors $u' \in S$

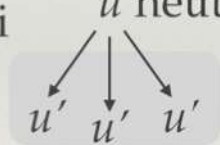
(CR3) si u neutre
 alors $u \in S$

- ❖ **Lemme C.** Si (pour tout $v \in \text{RED}_F$, $s[x:=v] \in \text{RED}_G$)
alors $\lambda x.s \in \text{RED}_{F \Rightarrow G}$
- ❖ Preuve: comme la dernière fois, à coups de (CR3).
- ❖ Permettait de traiter de la règle ($\Rightarrow$ I)
- ❖ Nous avons une nouvelle règle ($\perp$ E), pour laquelle nous démontrons le...

Un autre lemme utile

(CR1) $S \subseteq \text{SN}$

(CR2) si $u \in S \rightarrow u'$ alors $u' \in S$

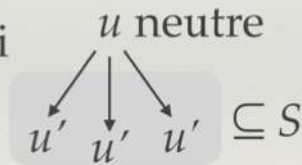
(CR3) si u neutre
 alors $u \in S$

- ❖ **Lemme D.** Si $u \in \text{RED}_\perp$, alors pour tout type F ,
$$\nabla u \in \text{RED}_F$$
- ❖ Preuve: par récurrence sur F
- ❖ Si F atomique ou $\perp$, toutes les réductions de ∇u se passent dans u , donc $\nabla u \in \text{SN} = \text{RED}_F$
- ❖ Dans le cas d'un type flèche...

Un autre lemme utile

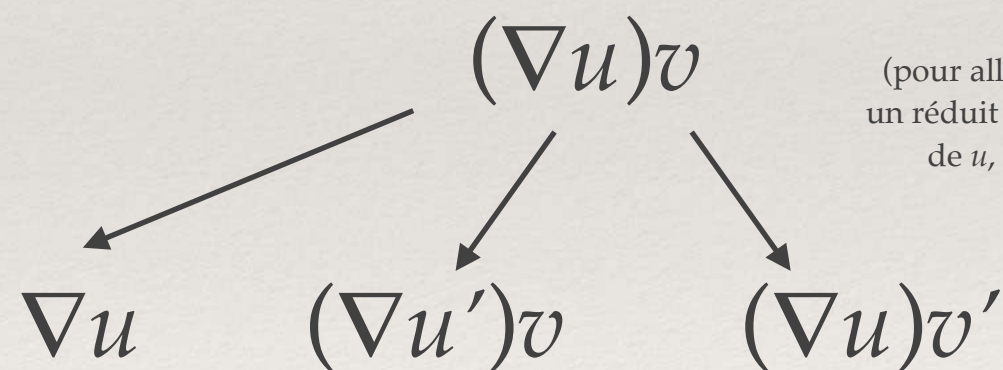
(CR1) $S \subseteq \text{SN}$

(CR2) si $u \in S \rightarrow u'$ alors $u' \in S$

(CR3) si u neutre alors $u \in S$


- ❖ ... il reste à démontrer que $\nabla u \in \text{RED}_{F \Rightarrow G}$, sachant que $\nabla u \in \text{RED}_G$ (hyp. réc.) et $u \in \text{RED}_\perp = \text{SN}$
- ❖ Par définition de $\text{RED}_{F \Rightarrow G}$, il suffit de démontrer que pour tout $v \in \text{RED}_F$, $(\nabla u)v$ est dans RED_G
- ❖ Il y a **trois** cas de réduction possibles:

Dans RED_G , par hypothèse (facile!)



Dans RED_G , pourquoi?
(il semble que ce soit aussi difficile à montrer que $(\nabla u)v \in \text{RED}_G$, non?)

Un autre lemme utile

(CR1) $S \subseteq \text{SN}$

(CR2) si $u \in S \rightarrow u'$ alors $u' \in S$

(CR3) si u neutre alors $u \in S$
 $\begin{array}{c} u \\ \swarrow \downarrow \searrow \\ u' \quad u' \quad u' \end{array} \subseteq S$

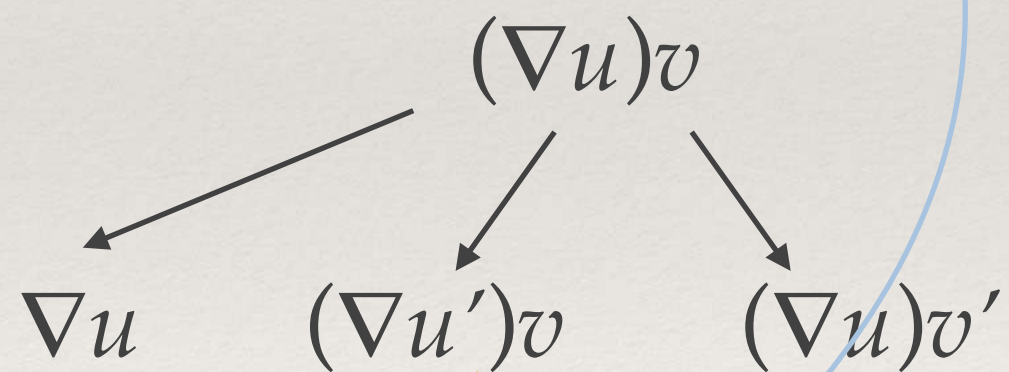
❖ ... il reste à démontrer que $\nabla u \in \text{RED}_G$ que
 $\nabla u \in \text{RED}_G$

par **récurrence** sur (u, v) ordonné par $\rightarrow^* \times_{\text{lexicogr.}} \rightarrow^*$
 (les deux sont dans SN, par (CR1))

Il faut démontrer que
 si tout $v \in \text{RED}_F$, $(\nabla u)v$ est dans RED_G

❖ Il y a **trois** cas
 de réduction possibles:

Dans RED_G , par hypothèse
 (facile!)



Dans RED_G , par hypothèse de
 récurrence

Normalisation forte

- ❖ **Def:** $\theta \in \underline{\text{RED}}_\Gamma$ ssi pour tout $x:F$ dans Γ , $\theta(x) \in \text{RED}_F$
- ❖ **Thm.** si $\Gamma \vdash u : G$ dérivable alors
pour toute $\theta \in \underline{\text{RED}}_\Gamma$, $u\theta \in \text{RED}_G$.
- ❖ Preuve: par récurrence sur la dérivation de $\Gamma \vdash u : G$, comme la dernière fois; on utilise la déf. de $\text{RED}_{F \Rightarrow G}$ dans le cas de $(\Rightarrow E)$, le Lemme C pour $(\Rightarrow I)$
- ❖ **Nouveau cas:** règle $(\perp E)$
par hyp. réc., $u\theta \in \text{RED}_\perp$
donc $(\nabla u)\theta \in \text{RED}_G$ par le **Lemme D**.

$$\frac{\Gamma \vdash u : \perp}{\Gamma \vdash \nabla u : G} (\perp E)$$

Lemme D. Si $u \in \text{RED}_\perp$, alors pour tout type G ,
 $\nabla u \in \text{RED}_G$

Conséquences

- ❖ Eh bien, comme pour le λ -calcul sans le faux:
- ❖ La prouvabilité est décidable
(toujours **PSPACE**-complète)
- ❖ et la logique est cohérente
(et maintenant on peut vraiment montrer que $\vdash \perp$ n'est pas dérivable, voir le corollaire 3 du `poly types.pdf`).

Autres connecteurs logiques:

le « non »

Il n'y a rien à faire!

- ❖ En intuitionniste comme en classique,
on peut définir $\neg F$ (« non F »)
comme $F \Rightarrow \perp$
- ❖ (Faites l'expérience, comparez la table de vérité des deux
en logique classique
—avec juste vrai et faux comme valeurs de vérité)

Autres connecteurs logiques:

le « et »

Voilà ce qu'on ajoute:

❖ Types (formules):

$F, G, \dots ::= A$

| $F \Rightarrow G$

| $F \wedge G$ (« F et G »)

❖ Termes:

$u, v, \dots ::= x$

| uv

| $\lambda x.u$

| $\langle u, v \rangle$ (couples)

| $\pi_1 u$ (première projection)

| $\pi_2 u$ (deuxième projection)

❖ Réductions:

$(\beta) \quad (\lambda x.u)v \rightarrow u[x:=v]$

$(\pi_1) \quad \pi_1 \langle u, v \rangle \rightarrow u$

$(\pi_2) \quad \pi_2 \langle u, v \rangle \rightarrow v$

la 1ère projection d'un couple $\langle u, v \rangle$
se **réduit** en u

(non, ce n'est **pas une égalité**,
syntaxiquement!)

Typage

$$\begin{array}{c} \frac{}{\Gamma, x:F \vdash x : F} \text{ (Ax)} \\[10pt] \frac{\Gamma \vdash u : F \Rightarrow G \quad \Gamma \vdash v : F}{\Gamma \vdash uv : G} \text{ (}\Rightarrow\text{E)} \quad \frac{\Gamma, x:F \vdash u : G}{\Gamma \vdash \lambda x.u : F \Rightarrow G} \text{ (}\Rightarrow\text{I)} \\[10pt] \frac{\Gamma \vdash u : F \wedge G}{\Gamma \vdash \pi_1 u : F} \text{ (}\wedge\text{E}_1\text{)} \quad \frac{\Gamma \vdash u : F \wedge G}{\Gamma \vdash \pi_2 u : G} \text{ (}\wedge\text{E}_2\text{)} \quad \frac{\Gamma \vdash u : F \quad \Gamma \vdash v : G}{\Gamma \vdash \langle u, v \rangle : F \wedge G} \text{ (}\wedge\text{I)} \end{array}$$

oui, il y a **deux** règles d'élimination!
c'est de la **syntaxe**, le $\wedge$ ne **commute pas** en
syntaxe (= juste du texte!)

mais je vous rassure: on peut démontrer
que $F \wedge G$ **implique** $G \wedge F$
(et réciproquement):
exercice, trouvez le terme de preuve!

Brouwer-Heyting-Kolmogorov

- ❖ Rappel de la dernière fois
Une preuve de $F \Rightarrow G$ est une fonction qui prend en entrée des preuves de F et retourne des preuves de G
c'est le type **produit** $F * G$ de Caml
- ❖ Ici, une preuve de $F \wedge G$ est un **couple** formé:
 - d'une preuve de F
 - et d'une preuve de G
- ❖ Mais attention! C'est une intuition **sémantique**...
en **syntaxe**, on a $x : F \wedge G \vdash x : F \wedge G$ dérivable
et pourtant x n'est pas de la forme $\langle u, v \rangle$!

Candidats de réductibilité

- ❖ L'intuition sémantique mène à la définition:

$$\text{RED}_{F \wedge G} = \{u \mid \pi_1 u \in \text{RED}_F \text{ et } \pi_2 u \in \text{RED}_G\}$$

- ❖ On définit les termes **neutres** comme ceux qui ne sont ni de la forme $\lambda x.u$ **ni de la forme** $\langle u,v \rangle$
(ni de la forme ∇u si on ajoute aussi le faux)
- ❖ **Normalisation forte:** comme avant.

Autres connecteurs logiques:

le « ou »

Voilà ce qu'on ajoute:

❖ Types (formules):

$F, G, \dots ::= A$

| $F \Rightarrow G$

| $F \vee G$ (« F ou G »)

❖ Termes:

$u, v, \dots ::= x$

| $\lambda x_1. u$
| $\lambda x_1. \lambda x_2. u$
| $\dots$
| $\text{case } u \text{ of } l_1 x_1 \mapsto v_1 \mid l_2 x_2 \mapsto v_2 \mid \dots$

x_1 est **liée**; sa portée est v_1
similairement pour x_2 et v_2

| $\text{case } u \text{ of } l_1 x_1 \mapsto v_1 \mid l_2 x_2 \mapsto v_2 \mid \dots$ (pattern matching)

$l_1 x_1 \mapsto v_1$

| $l_2 x_2 \mapsto v_2$

u (première injection)

u (deuxième injection)

❖ Réductions:

(β) $(\lambda x. u) v \rightarrow u[x := v]$

Comparez:
les règles (l_1) et (l_2)
ne se déclenchent
que si **case** est suivi
de l_1 ou de l_2

(l_1) $\text{case } l_1 u \text{ of } l_1 x_1 \mapsto v_1 \mid l_2 x_2 \mapsto v_2 \mid \dots \rightarrow v_1[x_1 := u]$

(l_2) $\text{case } l_2 u \text{ of } l_1 x_1 \mapsto v_1 \mid l_2 x_2 \mapsto v_2 \mid \dots \rightarrow v_2[x_2 := u]$

Nota bene

case u of est la notation Standard ML

**$\quad \quad \quad \iota_1 x_1 \mapsto v_1$
 $\quad \quad \quad | \quad \iota_2 x_2 \mapsto v_2$**

Dans le poly, j'ai écrit **case u $\left\{ \begin{array}{l} \iota_1 x_1 \mapsto v_1 \\ \iota_1 x_2 \mapsto v_2 \end{array} \right\}$**

(parce que sinon, j'avais des débordements infernaux dans les marges...
mais c'est trop difficile à reproduire dans ces transparents)

En Caml, on écrirait **match u with**
 $\quad \quad \quad | \quad \iota_1 x_1 \mapsto v_1$
 $\quad \quad \quad | \quad \iota_2 x_2 \mapsto v_2$

Typage

oui, il y a **deux** règles d'introduction

logiquement, ceci est une règle d'**analyse de cas**:
pour démontrer H sachant que $F \vee G$ est vrai,
on démontre H sous l'hypothèse F ,
et on démontre H sous l'hypothèse G

$$\frac{}{\Gamma, x:F \vdash x : F} \text{ (Ax)}$$

$$\frac{x:F \vdash u : G}{x.u : F \Rightarrow G} \text{ (}\Rightarrow\text{I)}$$

$$\frac{\Gamma \vdash u : G}{\Gamma \vdash \iota_2 u : F \vee G} \text{ (}\vee\text{I}_2\text{)}$$
$$\frac{}{\Gamma \vdash \iota_1 u : F \vee G} \text{ (}\vee\text{I}_1\text{)}$$

$$\frac{\Gamma \vdash u : F \vee G \quad \Gamma, x_1:F \vdash v_1 : H \quad \Gamma, x_2:G \vdash v_2 : H}{\Gamma \vdash \text{case } u \text{ of } \iota_1 x_1 \mapsto v_1 \mid \iota_2 x_2 \mapsto v_2 : H} \text{ (}\vee\text{E)}$$

Brouwer-Heyting-Kolmogorov

- ❖ Rappel de la dernière fois : en Caml, on écrirait
Une preuve de $F \Rightarrow G$ est un lambda-term qui prend en entrée des preuves de F et retourne des preuves de G

```
type FvG = iota1 of F  
         | iota2 of G
```
- ❖ Ici, une preuve de $F \vee G$ est un couple (tag, π) :
 - où $\text{tag} = \text{« gauche »}$ et π est une preuve de F
 - ou bien $\text{tag} = \text{« droite »}$ et π est une preuve de G
- ❖ Encore une fois c'est une intuition **sémantique...**
fausse en **syntaxe**.

Normalisation forte

- ❖ **Normalisation forte:** mais c'est plus compliqué qu'avant, et je ne le ferai pas
- ❖ (pas plus que dans le poly...)

La logique propositionnelle intuitionniste

- ❖ On peut tout mettre ensemble...
la logique propositionnelle intuitionniste est:

- ❖ **cohérente**

- ❖ **de prouvabilité décidable**
(toujours PSPACE-complète)

(β) $(\lambda x.u)v \rightarrow u[x:=v]$

(∇) $(\nabla u)v \rightarrow \nabla u$

(π_1) $\pi_1 \langle u, v \rangle \rightarrow u$

(π_2) $\pi_2 \langle u, v \rangle \rightarrow v$

(ι_1) $\text{case } \iota_1 u \text{ of } \iota_1 x_1 \mapsto v_1 \mid \iota_2 x_2 \mapsto v_2 \rightarrow v_1[x_1:=u]$

(ι_2) $\text{case } \iota_2 u \text{ of } \iota_1 x_1 \mapsto v_1 \mid \iota_2 x_2 \mapsto v_2 \rightarrow v_2[x_2:=u]$

$$\begin{array}{c}
 \frac{\Gamma \vdash u : \perp}{\Gamma \vdash \nabla u : G} (\perp E) \qquad \frac{}{\Gamma, x:F \vdash x : F} (Ax) \\
 \\
 \frac{\Gamma \vdash u : F \Rightarrow G \quad \Gamma \vdash v : F}{\Gamma \vdash uv : G} (\Rightarrow E) \qquad \frac{\Gamma, x:F \vdash u : G}{\Gamma \vdash \lambda x.u : F \Rightarrow G} (\Rightarrow I) \\
 \\
 \frac{\Gamma \vdash u : F \wedge G}{\Gamma \vdash \pi_1 u : F} (\wedge E_1) \quad \frac{\Gamma \vdash u : F \wedge G}{\Gamma \vdash \pi_2 u : G} (\wedge E_2) \quad \frac{\Gamma \vdash u : F \quad \Gamma \vdash v : G}{\Gamma \vdash \langle u, v \rangle : F \wedge G} (\wedge I) \\
 \\
 \frac{\Gamma \vdash u : F}{\Gamma \vdash \iota_1 u : F \vee G} (\vee I_1) \quad \frac{\Gamma \vdash u : G}{\Gamma \vdash \iota_2 u : F \vee G} (\vee I_2) \\
 \\
 \frac{\Gamma \vdash u : F \vee G \quad \Gamma, x_1:F \vdash v_1 : H \quad \Gamma, x_2:G \vdash v_2 : H}{\Gamma \vdash \text{case } u \text{ of } \iota_1 x_1 \mapsto v_1 \mid \iota_2 x_2 \mapsto v_2 : H} (\vee E)
 \end{array}$$

La logique classique

Logique classique

- ❖ La logique définie par une sémantique avec juste 2 valeurs de vérité (faux, vrai)...
- ❖ a causé quelques soucis aux théoriciens de la preuve et aux lambda-calculistes...
- ❖ mais j'en parlerai la **prochaine fois**, on en a fait suffisamment pour aujourd'hui, non?