La démonstration à l'interface entre mathématiques, logique et informatique: Comprendre le comment du pourquoi

Alexis Saurin
IRIF, Université Paris Cité, CNRS & INRIA
27 janvier 2025

Introduction

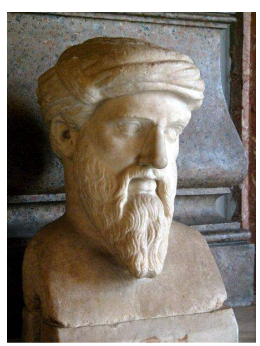
- Retour aux sources : l'origine de la démonstration en mathématiques et la constitution de la logique
- Évolution des sytèmes de déduction : enrichir la structure des démonstrations
- Quelques propriétés des déductions formelles
- Logiques réalistes et déréalistes
- Curry-Howard : entre preuves et programmes

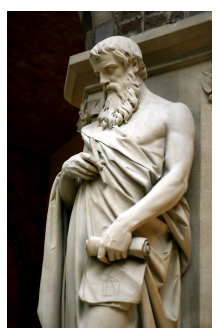
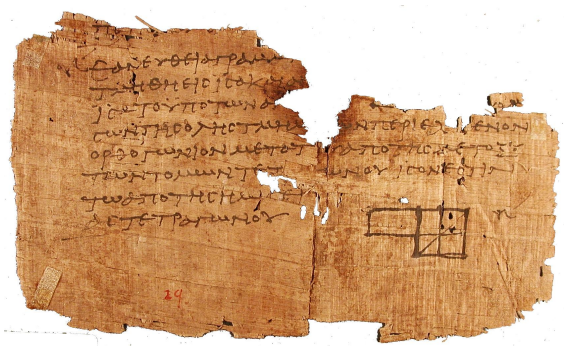
Retour aux sources

Quelques repères historiques mathématico-logiques

Histoire ancienne des mathématiques

- Pré-histoire mathématique avec le développement du calcul et de notations numériques permettant de calculer efficacement : Babyloniens, Mésopotamien, Inde
- Débuts de l'histoire mathématique : l'émergence de la démonstration mathématique et le développement de la méthode axiomatique : Grèce antique (Thalès ($\approx$ 625-546), Anaximandre ($\approx$610-546) , Pythagore ($\approx$ 580-490) aux VIème et Vème siècles, Euclide ($\approx$ 325-265) et ses *Éléments* au IIIème siècle)
- Début de la logique en tant que discipline indépendante avec Aristote (384-322) et les stoïciens
- Al-Khwarizmi ($\approx$ 780-850) : traité d'algèbre, introduction de la numération indienne dans le monde arabe, puis en Europe



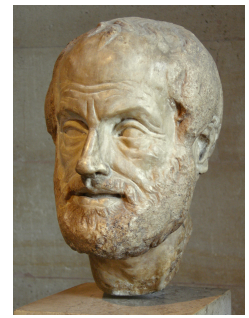
Quelques repères historiques mathématico-logiques

Autonomisation de la logique

- Antiquité : Naissance de la logique en tant que discipline indépendante avec Aristote (384-322) et la logique des stoïciens.
- Moyen-Âge et temps modernes : La logique, une science née et achevée avec Aristote ? Les scholastiques.
- Fin du XIXème siècle : crise des fondements des mathématiques (Cantor, Frege, Peano, Russel).
- Première moitié du XXème siècle :
  - programme de Hilbert ;
  - années 30 : théorème d'incomplétude de Gödel, résultats d'indécidabilité de Church ;
  - émergence des systèmes de déduction modernes avec Gentzen ;
  - mathématiques intuitionistes (Brouwer, Heyting, Kolmogorov).
- 1950-... :
  - Émergence de la programmation informatique ;
  - Correspondance de Curry-Howard entre preuves et programmes ;
  - Débuts des assistants à la preuve.

À l'origine : Aristote et les stoïciens

Aristote :



- Conçoit une logique dont l'énoncé de base est une forme prédicative, qui attribue une propriété à un sujet ;
- Fonde la syllogistique : définit et classe des formes de raisonnements valides, les syllogismes.
- Les énoncés artistotéliciens sont purement prédicatifs et monadiques :
  - Tous les P sont Q ; $\forall x, P(x) \Rightarrow Q(x)$
  - Certains R ne sont pas S. $\exists x, R(x) \wedge \neg S(x)$
- Développe la première logique modale, où les énoncés sont des affirmations modalisées : nécessité / possibilité / contingence.

Les stoïciens formulent une logique des propositions (avec négation, implication, conjonction et disjonction exclusive) et étudient des formes de raisonnement, notamment le *modus ponens* et le *modus tollens* :

Si le premier, le second, or le premier donc le second.
Si le premier, le second, or pas le second donc pas le premier.

Modus Ponens : $\dfrac{P \Rightarrow S \quad P}{S}$ *MP*

Évolution des systèmes de déduction

Le syllogisme aristotélicien

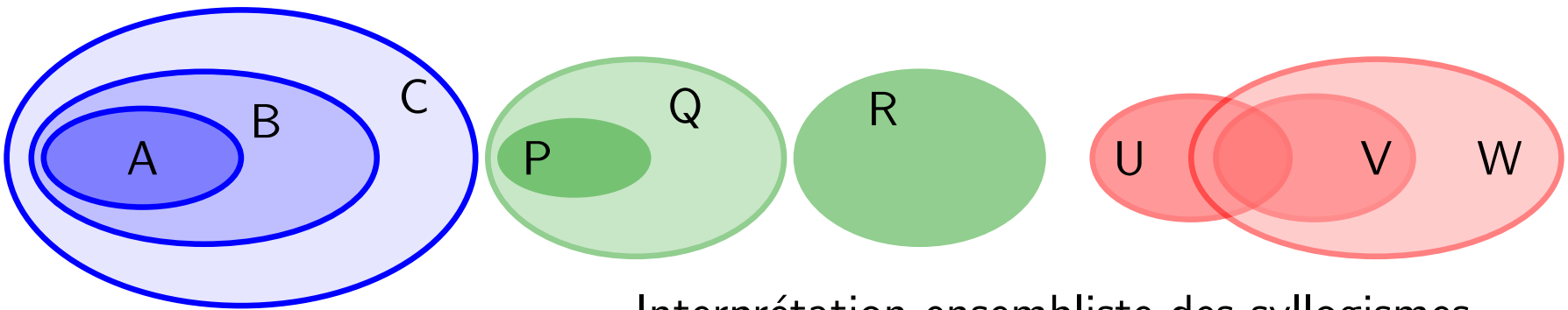
Les syllogismes comme première forme de raisonnement formel :

Tous les A sont des B tous les B sont des C,	Tous les P sont des Q aucun Q n'est R,	Certains U sont des V tous les V sont des W,
donc tous les A sont des C.	donc aucun P n'est R.	donc certains U sont des W.

Le syllogisme aristotélicien

Les syllogismes comme première forme de raisonnement formel :

Tous les A sont des B tous les B sont des C,	Tous les P sont des Q aucun Q n'est R,	Certains U sont des V tous les V sont des W,
donc tous les A sont des C.	donc aucun P n'est R.	donc certains U sont des W.

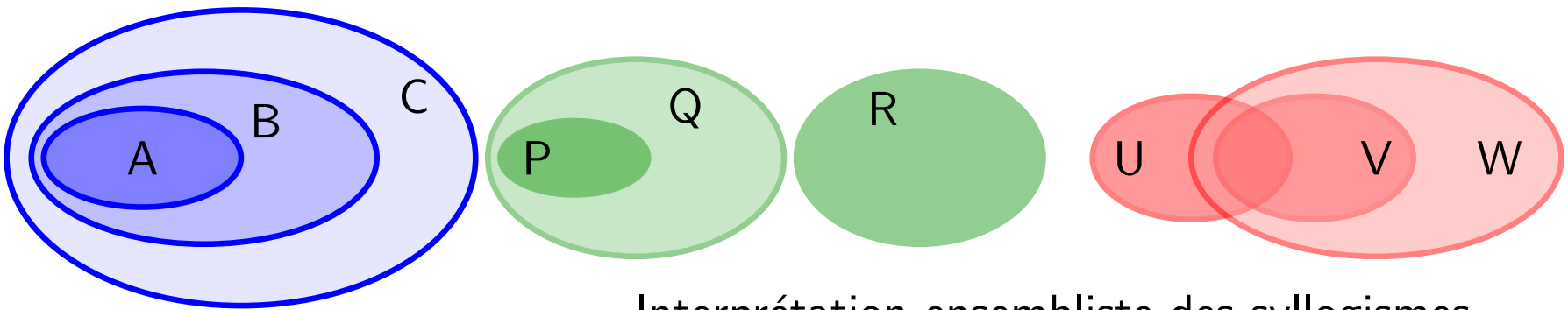


Interprétation ensembliste des syllogismes.

Le syllogisme aristotélicien

Les syllogismes comme première forme de raisonnement formel :

Tous les A sont des B tous les B sont des C,	Tous les P sont des Q aucun Q n'est R,	Certains U sont des V tous les V sont des W,
donc tous les A sont des C.	donc aucun P n'est R.	donc certains U sont des W.



Interprétation ensembliste des syllogismes.

À propos de notations logiques :

A **et** B	$A \cap B$	$A \wedge B$
A **ou** B	$A \cup B$	$A \vee B$

Les systèmes de preuves à la Hilbert : cas propositionel

Idée : De nombreux axiomes logiques et une unique règle de déduction.

H1	$A \Rightarrow B \Rightarrow A$	H2	$(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$
H3	$A \wedge B \Rightarrow A$	H4	$A \wedge B \Rightarrow B$
H5	$A \Rightarrow B \Rightarrow A \wedge B$	H6	$A \Rightarrow A \vee B$
H7	$B \Rightarrow A \vee B$	H8	$(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow (A \vee B) \Rightarrow C$
H9	$\neg A \Rightarrow (A \Rightarrow \bot)$	H10	$(A \Rightarrow \bot) \Rightarrow \neg A$
H11	$\bot \Rightarrow A$	H12	$A \vee \neg A$

Définition

Étant donné un ensemble de formules, Γ, la théorie et une formule T, une Γ-déduction de T est une suite finie de formules $(F_1, \ldots, F_n)$ telle que $F_n = T$ et que pour tout $1 \leq i \leq n$, F_i est :

- *soit un axiome logique : $F_i \in \{H1, \ldots, H12\}$;*
- *soit un axiome de la théorie : $F_i \in \Gamma$;*
- *soit obtenue par modus ponens à partir de formules établies précédemment : il existe $j, k < i$ tels que $F_j = F_k \Rightarrow F_i$.*

On notera $\vdash_\Gamma T$ lorsqu'il existe une Γ-déduction de T.

Les systèmes de preuves à la Hilbert : cas propositionel

Idée : De nombreux axiomes logiques et une unique règle de déduction.

H1	$A \Rightarrow B \Rightarrow A$	H2	$(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$
H3	$A \wedge B \Rightarrow A$	H4	$A \wedge B \Rightarrow B$
H5	$A \Rightarrow B \Rightarrow A \wedge B$	H6	$A \Rightarrow A \vee B$
H7	$B \Rightarrow A \vee B$	H8	$(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow (A \vee B) \Rightarrow C$
H9	$\neg A \Rightarrow (A \Rightarrow \bot)$	H10	$(A \Rightarrow \bot) \Rightarrow \neg A$
H11	$\bot \Rightarrow A$	H12	$A \vee \neg A$

Exemple

Prouvons le théorème suivant (dans la théorie vide) : $\vdash_\emptyset A \Rightarrow A$.

1. $(A \Rightarrow (A \Rightarrow A) \Rightarrow A) \Rightarrow (A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ $H2$
2. $A \Rightarrow (A \Rightarrow A) \Rightarrow A$ $H1$
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ $MP(1,2)$
4. $A \Rightarrow (A \Rightarrow A)$ $H1$
5. $A \Rightarrow A$ $MP(3,4)$

Les systèmes de preuves à la Hilbert : cas propositionel

Idée : De nombreux axiomes logiques et une unique règle de déduction.

H1	$A \Rightarrow B \Rightarrow A$	H2	$(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)$
H3	$A \wedge B \Rightarrow A$	H4	$A \wedge B \Rightarrow B$
H5	$A \Rightarrow B \Rightarrow A \wedge B$	H6	$A \Rightarrow A \vee B$
H7	$B \Rightarrow A \vee B$	H8	$(A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow (A \vee B) \Rightarrow C$
H9	$\neg A \Rightarrow (A \Rightarrow \bot)$	H10	$(A \Rightarrow \bot) \Rightarrow \neg A$
H11	$\bot \Rightarrow A$	H12	$A \vee \neg A$

Théorème de déduction

Si $\vdash_{\Gamma,A} B$ *alors* $\vdash_{\Gamma} A \Rightarrow B$.

Preuve

Par récurrence sur la longueur de la déduction $\delta = (F_i)_{1 \leq i \leq n}$, *en construisant une* Γ*-déduction* $\delta' = (F'_i)_{1 \leq i \leq p}$ *telle que pour tout* $1 \leq i \leq n$, *il existe* $1 \leq j \leq p$ *tel que* $F'_j = A \Rightarrow F_i$, *en utilisant :*
(i) la preuve du transparent précédent pour $F_i = A$,
(ii) H1 *si* $F_i \in \{H_1, \ldots, H_{12}\} \cup \Gamma$ *ou*
(iii) H2 *si c'est par une utilisation du modus ponens (entre* $B \Rightarrow C$ *et* B*).*

Les systèmes de preuves à la Hilbert : la quantification

Pour traiter le calcul des prédicats (logique du premier ordre) dans son ensemble, on ajoute simplement deux axiomes et deux règles d'inférence au cas propositionnel :

- axiomes du premier-ordre :

$$\begin{array}{ll} H_{13} & A[t/x] \Rightarrow \exists x.A[x] \\ H_{14} & \forall x.A[x] \Rightarrow A[t/x] \end{array}$$

- règles d'inférence du premier-ordre :
  - de $C \Rightarrow A[x]$, on peut déduire $C \Rightarrow \forall x.A[x]$ à condition que $x \notin FV(C)$
  - de $A[x] \Rightarrow C$, on peut déduire $\exists x.A[x] \Rightarrow C$ à condition que $x \notin FV(C)$

Limites des sytèmes à la Hilbert

Les sytèmes de preuve à la Hilbert permettent de définir une notion précise de prouvabilité mais :

- les dérivations y sont éloignées du raisonnement mathématique habituel, et
- elles ne sont pas pratiques pour étudier, comparer, analyser les preuves elles-mêmes.

En mathématiques, on a plus souvent deux types de raisonnement :

- Le raisonnement en avant : on déduit un nouvel énoncé de ce qu'on connaît déjà, c'est-à-dire qu'on utilise un énoncé déjà connu.
- Le raisonnement en arrière : on analyse l'énoncé qu'on souhaite établir et on se ramène à de nouveaux énoncés à démontrer qui sont suffisants pour établir l'énoncé qui nous intéresse.
- Ces deux dynamiques de raisonnement sont entremêlées.

Vers la déduction naturelle

Exemples de raisonnement en avant :

- Si l'énoncé $\mathbf{A_1}$ **et** $\mathbf{A_2}$ est démontré, on peut en déduire $\mathbf{A_i}$ pour $i \in \{1, 2\}$.
- Si les énoncés **A implique B** d'une part et **A** d'autre part sont démontré, alors on peut en déduire **B** (Modus Ponens).
- Si l'énoncé disjonctif **A ou B** est démontré et si de plus, on peut d'une part démontrer **C** en supposant **A** et d'autre part démontrer **C** en supposant **B**, alors on peut déduire **C** de cette disjonction de cas.
- Si l'énoncé universel **pour tout x**, $\mathbf{A(x)}$ est démontré, alors on peut en déduire n'importe quelle instance $\mathbf{A(a)}$ pour un objet **a** quelconque.

Exemples de raisonnement en arrière :

- Si on veut démontrer l'énoncé conjonctif **A et B**, il suffit de démontrer **A**, d'une part, et de démontrer **B**, d'autre part
- Si on veut démontrer l'énoncé implicatif **A implique B**, alors il suffit de (sup)poser l'hypothèse **A** et de démontrer **B** sous cette hypothèse, dont on pourra conclure l'implication souhaitée.
- Si on veut démontrer l'énoncé universel **pour tout x**, $\mathbf{A(x)}$, il suffit de poser un élément générique *a* (sur lequel on ne fait aucune hypothèse), et de démontrer $\mathbf{A(a)}$: on peut alors déduire **pour tout x** , $\mathbf{A(x)}$.

Déduction naturelle 1 : Règles d'inférence $(\Rightarrow, \wedge, \forall)$

$$\frac{}{\Gamma, A \vdash A}\ Ax$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge I \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow I \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}\ \forall I\ (\star)$$

$$\frac{\Gamma \vdash A_1 \wedge A_2}{\Gamma \vdash A_j}\ \wedge Ej\ j \in \{1,2\} \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow E \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]}\ \forall E$$

$(\star)$ Pour $\forall I$, x n'est pas libre dans Γ.

Exemple (avec $\Gamma = A \wedge B \Rightarrow C, A, B$)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A \wedge B \Rightarrow C}\ Ax \quad \dfrac{\dfrac{}{\Gamma \vdash A}\ Ax \quad \dfrac{}{\Gamma \vdash B}\ Ax}{\Gamma \vdash A \wedge B}\ \wedge I}{A \wedge B \Rightarrow C, A, B \vdash C}\ \Rightarrow E}{A \wedge B \Rightarrow C, A \vdash B \Rightarrow C}\ \Rightarrow I}{A \wedge B \Rightarrow C \vdash A \Rightarrow (B \Rightarrow C)}\ \Rightarrow I}{\vdash (A \wedge B \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))}\ \Rightarrow I$$

Déduction naturelle 2 : Dynamique des preuves

Certaines déductions font des détours,
ce ne sont pas des arguments directs :

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_A}{\Gamma \vdash A} \quad \dfrac{\mathcal{D}_B}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge I}{\Gamma \vdash B}\ \wedge E2$$

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_1}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow I \quad \dfrac{\mathcal{D}_2}{\Gamma \vdash A}}{\Gamma \vdash B}\ \Rightarrow E$$

($\tilde{\mathcal{D}}$ can be described as $\mathcal{D}_1 \left\{ \mathcal{D}_2 / \dfrac{}{\Gamma, A, \Delta \vdash A}\ Ax \right\}$)

Déduction naturelle 2 : Dynamique des preuves

Certaines déductions font des détours,
ce ne sont pas des arguments directs :

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_A}{\Gamma \vdash A} \quad \dfrac{\mathcal{D}_B}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,\wedge I}{\Gamma \vdash B}\,\wedge E2 \quad \longrightarrow \quad \dfrac{\mathcal{D}_B}{\Gamma \vdash B}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathcal{D}_1}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,\Rightarrow I \quad \dfrac{\mathcal{D}_2}{\Gamma \vdash A}}{\Gamma \vdash B}\,\Rightarrow E \quad \longrightarrow \quad \dfrac{\tilde{\mathcal{D}}}{\Gamma \vdash B}$$

($\tilde{\mathcal{D}}$ can be described as $\mathcal{D}_1 \left\{ \mathcal{D}_2 / \dfrac{}{\Gamma, A, \Delta \vdash A}\,Ax \right\}$)

On peut considérer une *transformation ou simplification de preuves* par le biais d'une notion de coupure, c'est-à-dire une règle d'introduction immédiatement suivie d'une règle d'élimination *du même connecteur*.

Ce système a de très bonnes propriétés : confluence, terminaison, ...
Ce qui assure que toute déduction peut être transformée de manière systématique et algorithmique, en une déduction sans coupure.

Déduction naturelle 3 ($\vee, \neg, \bot, \exists$)

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee I1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee I2$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee E$$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A}\ \exists I \qquad \frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists E \quad (\star)$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg I \qquad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot}\ \neg E \qquad \boxed{\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot\ C}$$

($\star$) x n'est pas libre dans Γ, C

Défauts de la déduction naturelle

- La notion de coupure est implicite, il n'y a pas de règle d'inférence en tant que tel pour la coupure ;
- ND est satisfaisante, mais essentiellement pour un fragment de la logique intuitioniste ($\Rightarrow$, $\wedge$, $\forall$).
  Paradoxalement, les connecteurs qui sont les plus intéressants en logique intuitioniste sont $\vee$ et $\exists$...

La déduction naturelle est proche du raisonnement mathématique réel mais elle manque de structure pour y réaliser une analyse des preuves vraiment intéressante.

Vers le calcul des séquents

- Coupure explicite : elle devient une règle d'inférence,
- Règles d'inférences dédiées à la gestion des formules (règles dites structurelles),
- Grande symétrie gauche-droite du système (qui est le pendant de la symétrie intro / élim de la déduction naturelle ; les règles d'élimination à droite devenant des règles di'ntroduction à gauche),
- Un séquent a la forme :

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

- Il s'agit d'un jugement logique qui affirme que la conjonction des H_i a pour conséquence logique la disjonction des C_j, c'est-à-dire qu'il a la même signification que la formule :

$$\forall \vec{x_k} \left(\bigwedge_{1 \leq i \leq m} H_i \right) \Rightarrow \left(\bigvee_{1 \leq j \leq n} C_j \right)$$

Règles d'inférence de LK (1)

Fragment Identité (*Axiome et Coupure*)

$$\frac{}{A \vdash A}\ Ax \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ Cut$$

Règles Structurelles (*Échange, Affaiblissement et Contraction*)

$$\frac{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}\ LEx \qquad \frac{\Gamma \vdash \Delta_1, B, A, \Delta_2}{\Gamma \vdash \Delta_1, A, B, \Delta_2}\ REx$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ LW \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ RW$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ LC \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ RC$$

Règles d'inférence de LK (2)

Fragment Logique ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\forall$, $\exists$)

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ L\neg \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ R\neg$$

$$\frac{\Gamma, A_j \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta}\ L\wedge j \quad (j \in \{1,2\}) \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ R\wedge$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ L\vee \qquad \frac{\Gamma \vdash A_j, \Delta}{\Gamma \vdash A_1 \vee A_2, \Delta}\ R\vee j \quad (j \in \{1,2\})$$

$$\frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \Rightarrow B \vdash \Delta_1, \Delta_2}\ L\Rightarrow \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}\ R\Rightarrow$$

$$\frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ L\forall \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x A, \Delta}\ R\forall \quad (*)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x A \vdash \Delta}\ L\exists \quad (*) \qquad \frac{\Gamma \vdash A[t/x], \Delta}{\Gamma \vdash \exists x A, \Delta}\ R\exists$$

(*) Pour ces règles, $x \notin FV(\Gamma, \Delta)$.

Quelques théorèmes formels

- $A \vee B \vdash B \vee A$ — Commutativité de la disjonction
- $\vdash A \vee \neg A$ — *Tertium non datur*
- $\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ — Loi de Peirce
- $\vdash (\neg\neg A) \Rightarrow A$ — Élimination de la Double Négation
- $\vdash \exists x \forall y (P(x) \Rightarrow P(y))$ — Propriété du Buveur
- $A \vee B \vdash \neg(\neg A \wedge \neg B)$ — Une instance des lois de de Morgan
- $\vdash (A \Rightarrow B) \vee (B \Rightarrow A)$
- $\vdash \neg\neg(A \vee \neg A)$ — *Tertium non datur* "intuitioniste"
- $(p \Rightarrow q) \vdash (\neg q \Rightarrow \neg p)$
- $(\neg q \Rightarrow \neg p) \vdash (p \Rightarrow q)$

Prouvez-les !

Quelques propriétés des démonstrations formelles

Théorème d'élimination des coupures de Gentzen

Hauptsatz de Gentzen

La règle de coupure est admissible dans LK.

En fait, le résultat de Gentzen nous donne plus qu'une simple preuve d'*admissibilité de la coupure* puisqu'il fournit également *une procédure explicite pour éliminer les coupures d'une preuve* : en commençant avec une preuve contenant des coupures, on peut la transormer étape par étape en une preuve sans coupure, et cette procédure est *algorithmique*.

La preuve se fait par une généralisation du principe de raisonnement par récurrence, la récurrence bien fondée ou noethérienne. En particulier le principe de récurrence usuel de l'arithmétique de Péano ne suffit pas car la structure de l'ordre de bonne fondation est plus compliqué que ce qui est capturé par la récurrence de Péano. Il s'agit d'une forme de récurrence noethérienne.

Conséquences de l'élimination des coupures

Propriété de la sous-formule, Consistance et Interpolation

Propriété de la sous-formule

Un séquent prouvable peut être prouvé en utilisant uniquement des sous-formules des formules apparaissant dans la conclusion du séquent.

Cette propriété réduit énormément l'espace de recherche d'une preuve et nous garantit même, dans certains cas, la décidabilité de la prouvabilité !

Theorem (Consistance de LK)

Le séquent vide n'est pas dérivable dans LK.
En particulier, il n'y a pas de preuve de $\vdash \bot$ dans LK et donc on ne peut, pour aucune formule A, prouver à la fois $\vdash A$ et $\vdash \neg A$.

Theorem (Théorème d'interpolation de Craig)

Si $\vdash_{LK} A \Rightarrow B$, alors il existe une formule I qui n'utilise que les propositions atomiques que A et B ont en commun et telle que $\vdash_{LK} A \Rightarrow I$ et $\vdash_{LK} I \Rightarrow B$.

Symétrie de LK (1)

Les séquents sont maintenant de la forme : $\vdash' \Gamma$.

L'implication est un connecteur défini : $A \Rightarrow B \equiv \neg A \vee B$

La négation n'apparaît que sur les formules atomiques, en utilisant les lois de de Morgan :

$$\begin{array}{ll} \neg(A \vee B) \equiv (\neg A \wedge \neg B) & \neg\forall x A \equiv \exists x \neg A \\ \neg(A \wedge B) \equiv (\neg A \vee \neg B) & \neg\exists x A \equiv \forall x \neg A \end{array}$$

Plus précisément, quand on écrit $\neg A$, on voudra toujours parler de la *forme normale négative* de cette formule pour le système de réécriture clairement terminant et confluent :

$$\begin{array}{l|l} \neg(A \vee B) \to (\neg A \wedge \neg B) & \neg\forall x A \to \exists x \neg A \\ \neg(A \wedge B) \to (\neg A \vee \neg B) & \neg\exists x A \to \forall x \neg A \\ \neg\neg A \to A & \end{array}$$

Symétrie de LK (2)

Règles Identité

$$\frac{}{\vdash' A, \neg A}\ Ax \qquad \frac{\vdash' A, \Gamma \quad \vdash' \neg A, \Delta}{\vdash' \Gamma, \Delta}\ Cut$$

Règles Structurelles

$$\frac{\vdash' \Gamma, B, A, \Delta}{\vdash' \Gamma, A, B, \Delta}\ Ex \qquad \frac{\vdash' \Gamma}{\vdash' A, \Gamma}\ W \qquad \frac{\vdash' A, A, \Gamma}{\vdash' A, \Gamma}\ C$$

Règles Logiques

$$\frac{\vdash' A, \Gamma \quad \vdash' B, \Gamma}{\vdash' A \wedge B, \Gamma}\ \wedge \qquad \frac{\vdash' A, \Gamma}{\vdash' A \vee B, \Gamma}\ \vee 1 \qquad \frac{\vdash' B, \Gamma}{\vdash' A \vee B, \Gamma}\ \vee 2$$

$$\frac{\vdash' A, \Gamma}{\vdash' \forall x A, \Gamma}\ \forall \quad (*) \qquad \frac{\vdash' A[t/x], \Gamma}{\vdash' \exists x A, \Gamma}\ \exists$$

Approches logiques réalistes

Approches logiques réalistes

Idée : Raffiner la logique classique pour lui permettre d'exprimer plus facilement certaines propriétés.
Par exemple des propriétés d'un type particulier, qui exprime selon quelles modalités un énoncé prend une valeur de vérité, ou bien en modifiant les objets sur lequels porte la quantification.

Par exemple, on peut modaliser un énoncé vis-à-vis de :

- la nécessité de sa vérité (logique modale)
- la temporalité de sa vérité (logique temporelle)
- la connaissance que l'on a de sa vérité (logique de la connaissance)
- le caractère obligatoire ou interdit d'un énoncé (logique déontique)
- la valeur de vérité prise après l'occurrence d'une action,

Logiques modales, quelques exemples

La vérité peut être contingente "*il fait beau*", "*par un point extérieur à une droite, il passe une droite et une seule parallèle à la droite donnée*" peuvent être vrais aujourd'hui, ou bien en géométrie euclidienne, mais peuvent s'avérer faux demain, ou en géométrie hyperbolique.
À l'inverse, d'autres énoncés sont nécessairement vrais :

$$A \Rightarrow A \qquad A \wedge B \Rightarrow A \qquad A \Rightarrow B \Rightarrow A \wedge B \qquad A \Rightarrow A \vee B$$

On ajoute deux connecteurs qui modalisent une formule, $\Box, \Diamond$:

- $\Box A$ signifie que A **est nécessairement vraie** ;
- $\Diamond A$ signifie que A **est possiblement vraie**.

Il vient certains principes nouveaux :

- $A \Rightarrow \Diamond A, \quad \Box A \Rightarrow A, \quad \Box A \Rightarrow \Box\Box A, \quad \Box(A \Rightarrow B) \Rightarrow \Box A \Rightarrow \Box B$;
- Si on a prouvé A (sans hypothèse), on peut en déduire $\Box A$

MAIS on n'a pas $A \Rightarrow \Box A$ en général.

Élargir le champ des quantificateurs

Parmi les élargissements du champ de la quantification, on trouve :

- Logiques à plusieurs sortes d'objets. La possibilité de définir plusieurs sortes d'objets du discours (par exemple des personnes, des nombres, des dates, des lieux, etc.), de construire les termes en utilisant des prédicats qui attendent une sorte particulière d'objets, et des quantificateurs qui sont relatifs à chaque sorte d'objets.
- Logiques d'ordre supérieur. Permettre de quantifier non seulement sur les objets du discours, mais possiblement sur des ensembles d'objets (quantification monadique), sur des relations ou sur des fonctions.

Les approches déréalistes et le calcul

Non-Constructivité de *LK*

Certaines preuves sont constructives, d'autres non. Pour donner une idée de ce que cela signifie, donner une preuve non-constructive de la proprosition suivante :

Proposition

Il existe deux nombres irrationnels a, b tels que a^b est rationnel.

Preuve

Considérons le nombre irrationnel $\sqrt{2}$. De deux choses l'une, soit $\sqrt{2}^{\sqrt{2}}$ est rationnet ; soit il ne l'est pas.
Dans le premier cas, il suffit de poser $a = b = \sqrt{2}$ pour avoir le résultat tandis que dans le second, en posant $a = sqrt2^{\sqrt{2}}$ et $b = \sqrt{2}$ on obtient $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$.

□

Non-Constructivité de *LK*

Certaines preuves sont constructives, d'autres non. Pour donner une idée de ce que cela signifie, donner une preuve non-constructive de la proprosition suivante :

Proposition

Il existe deux nombres irrationnels a, b tels que a^b est rationnel.

Preuve

Considérons le nombre irrationnel $\sqrt{2}$. De deux choses l'une, soit $\sqrt{2}^{\sqrt{2}}$ est rationnet ; soit il ne l'est pas.
Dans le premier cas, il suffit de poser $a = b = \sqrt{2}$ pour avoir le résultat tandis que dans le second, en posant $a = sqrt2^{\sqrt{2}}$ et $b = \sqrt{2}$ on obtient $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$.

□

$\sqrt{2}^{\sqrt{2}}$ est-il irrationnel ?

***LK* est donc symétrique mais non-constructif.**

Intuitionisme

Tout commence avec Brouwer qui rejette l'usage du principe du tiers-exclus.

Pourquoi ?
Une vision des mathématiques *centrée sur l'activité mathématique et l'idée de construction* de sortie de la formule A prend le sens de "Je sais que A" ou plus précisément "j'ai une preuve de A". Avec cette interprétation en tête, les connecteurs logiques et les règles de raisonnement doivent être reconsidérées.

En particulier, la disjonction $A \vee B$ signifie "J'ai une preuve de A ou j'ai une preuve de B" ... et le tiers-exclus n'est alors plus un pincipe logique satisfaisant pour établir une telle assertion puisque $A \vee \neg A$ signifierait que l'on a toujours une preuve d'une formule ou de sa négation...
... ce qui n'a rien d'évident.

Constructivisme : une preuve fournit une manière de construire un objet qui représente la propriété prouvée.

Interprétation des preuves dite de *Brouwer-Heyting-Kolmogorov*

- Une preuve de $A \vee B$ est une paire (i, π) avec $i \in \{1; 2\}$ et si $i = 1$ alors π est une preuve de A, sinon c'est une preuve de B ;
- Une preuve de $A \wedge B$ est une paire (π, π') d'une preuve de A et d'une preuve de B ;
- Une preuve de $A \Rightarrow B$ est une *fonction* qui associe à toute preuve de A une preuve de B (c'est donc une transformation de preuves) ;
- Une preuve de $\exists x A$ est une paire (t, π) avec t un terme et π une preuve de $A[t/x]$;
- Une preuve de $\forall x A$ est une fonction qui associe à chaque terme t une preuve de $A[t/x]$;
- Une preuve de $\neg A$ est une fonction qui à toute preuve de A associe une preuve de $F \wedge \neg F$.

$\Longrightarrow$ **Déduction Naturelle**

Calcul des séquents LJ

Identité

$$\frac{}{A \vdash A}\ ax \qquad \frac{\Gamma_1 \vdash A \quad \Gamma_2, A \vdash \Xi}{\Gamma_1, \Gamma_2 \vdash \Xi}\ coupure$$

Struct.

$$\frac{\Gamma_1, B, A, \Gamma_2 \vdash \Xi}{\Gamma_1, A, B, \Gamma_2 \vdash \Xi}\ LEx \qquad \frac{\Gamma \vdash \Xi}{\Gamma, A \vdash \Xi}\ LW \qquad \frac{\Gamma \vdash}{\Gamma \vdash A}\ RW \qquad \frac{\Gamma, A, A \vdash \Xi}{\Gamma, A \vdash \Xi}\ LC$$

Logique

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash}\ L\neg \qquad \frac{\Gamma, A \vdash}{\Gamma \vdash \neg A}\ R\neg$$

$$\frac{\Gamma_1 \vdash A \quad \Gamma_2, B \vdash \Xi}{\Gamma_1, \Gamma_2, A \Rightarrow B \vdash \Xi}\ L\Rightarrow \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ R\Rightarrow$$

$$\frac{\Gamma, A \vdash \Xi}{\Gamma, A \wedge B \vdash \Xi}\ L\wedge 1 \qquad \frac{\Gamma, B \vdash \Xi}{\Gamma, A \wedge B \vdash \Xi}\ L\wedge 2 \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ R\wedge$$

$$\frac{\Gamma, A \vdash \Xi \quad \Gamma, B \vdash \Xi}{\Gamma, A \vee B \vdash \Xi}\ L\vee \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ R\vee 1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ R\vee 2$$

$$\frac{\Gamma, A[t/x] \vdash \Xi}{\Gamma, \forall x A \vdash \Xi}\ L\forall \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}\ R\forall\ (*) \qquad \frac{\Gamma, A \vdash \Xi}{\Gamma, \exists x A \vdash \Xi}\ L\exists\ (**) \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A}\ R\exists$$

(*) Pour $R\forall$, $x \notin FV(\Gamma)$. (**) Pour $L\exists$, $x \notin FV(\Gamma, \Xi)$.

Propriété de la disjonction et du témoin

Grâce à l'élimination des coupures, on a :

Propriété de la disjunction

Si $\vdash_{LJ} A \vee B$, *alors* $\vdash_{LJ} A$ *ou* $\vdash_{LJ} B$

Propriété du témoin

Si $\vdash_{LJ} \exists x A$, *alors il existe un terme* t *tel que* $\vdash_{LJ} A[t/x]$

LJ est constructive mais pas symétrique.

LJ est clairement plus faible que LK : pour tout liste de formules A, Γ, $\Gamma \vdash_{LJ} A$ implique $\Gamma \vdash_{LK} A$.

Peut-on être plus précis quant à la relation entre ces deux notions de prouvabilité ?

On va voir que LJ peut être considérée non pas comme plus faible mais comme plus fine que LK !

Lien entre prouvabilité classique et intuitioniste (1)

Tiers-exclu intuitioniste

Rappelons-nous que dans LJ, la contraction n'est pas disponible à droite du jugement (ie de $\vdash$) mais peut être librement utilisée à gauche.

$A \vee \neg A$ n'est pas prouvable dans LJ mais $\neg\neg(A \vee \neg A)$ l'est :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,Axiom}{\vdash A, \neg A}\,R\neg}{\vdash A, A \vee \neg A}\,R\vee}{\vdash A \vee \neg A, A \vee \neg A}\,R\vee \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,Axiom}{A \vdash A \vee \neg A}\,R\vee}{\neg(A \vee \neg A), A \vdash}\,L\neg}{\neg(A \vee \neg A) \vdash \neg A}\,R\neg}{\neg(A \vee \neg A) \vdash A \vee \neg A}\,R\vee}{\neg(A \vee \neg A), \neg(A \vee \neg A) \vdash}\,L\neg}{\neg(A \vee \neg A) \vdash}\,LC}{\vdash \neg\neg(A \vee \neg A)}\,R\neg$$

Lien entre prouvabilité classique et intuitioniste (2)

Traduction de Gödel

L'idée de la preuve intuitioniste de $\neg\neg(A \vee \neg A)$ est d'envoyer la formula à gauche de telle sorte qu'il soit possible d'y utiliser la contraction gauche (ie la contraction sur les hypothèses).
L'occurrence de la double négation $\neg\neg$ permet précisément de traverser deux fois $\vdash$ et ainsi d'utiliser la contraction gauche.

Définition: traduction de Gödel

- $A^\star = \neg\neg A$ *pour* A *atomique* ;
- $(A \wedge B)^\star = A^\star \wedge B^\star$;
- $(\forall x A)^\star = \forall x A^\star$;
- $(\neg A)^\star = \neg A^\star$;
- $(A \Rightarrow B)^\star = A^\star \Rightarrow B^\star$;
- $(A \vee B)^\star = \neg\neg(A^\star \vee B^\star)$;
- $(\exists x A)^\star = \neg\neg\exists x A^\star$.

Lien entre prouvabilité classique et intuitioniste (3)

Theorem

$\Gamma \vdash_{LK} A$ *si, et seulement si,* $\Gamma^\star \vdash_{LJ} A^\star$

Lemme

- $\vdash_{LK} A \Leftrightarrow A^\star$;
- *Pour toute formule* A*, on a* $\vdash_{LJ} \neg\neg A^\star \Rightarrow A^\star$;
- *Si* $\Gamma \vdash_{LK} \Delta$ *alors* $\Gamma^\star, \neg\Delta^\star \vdash_{LJ}$.

Dans quel sens peut-on dire que LJ est **plus fine (plus subtile ?)** que LK ?

Même si une personne qui raisonne en logique intuitioniste ne peut pas prouver un théorème classique A, elle pourra démontrer $A^\star$ qu'une personne raisonnant classiquement ne pourra pas distinguer A.

En logique intuitionistique, l'utilisation du tiers-exclus (ou de la contraction à droite) peut être *explicitement mentionnée dans la formule* grâce à l'usage d'une double négation.

Vers la logique linéaire

Et si on retirait toutes les règles structurelles ?

Est-il possible d'être encore plus drastique avec les règles structurelles ? OUI

On a ainsi deux conjonctions et deux disjonctions différentes !
$\wedge$ se décompose en $\&$ et $\otimes$
$\vee$ se décompose en $\parr$ et $\oplus$.

On a besoin de retrouver la contraction et l'affaiblissement, mais d'une manière contrôlée.
On ajoute deux modalités : ! et ? qui expriment le fait qu'une formule est pérenne, c'est-à-dire qu'on peut lui appliquer des règles structurelles.
On obtient ainsi une notion de logique qui est sensible aux ressources.

Calcul des séquents de LL

Fragment Identité :

$$\frac{}{\vdash A^{\perp}, A}\ ax \qquad \frac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}\ cut$$

Fragment Structurel :

$$\frac{\vdash \Gamma, B, A, \Delta}{\vdash \Gamma, A, B, \Delta}\ Ex$$

Fragment Logique :

$$\frac{\vdash F, G, \Gamma}{\vdash F \parr G, \Gamma}\ \parr \qquad \frac{\vdash F, \Gamma \quad \vdash G, \Delta}{\vdash F \otimes G, \Gamma, \Delta}\ \otimes$$

$$\frac{\vdash F, \Gamma \quad \vdash G, \Gamma}{\vdash F \& G, \Gamma}\ \& \qquad \frac{\vdash F, \Gamma}{\vdash F \oplus G, \Gamma}\ \oplus 1 \qquad \frac{\vdash G, \Gamma}{\vdash F \oplus G, \Gamma}\ \oplus 2$$

$$\frac{}{\vdash 1}\ 1 \qquad \frac{\vdash \Gamma}{\vdash \bot, \Gamma}\ \bot \qquad \frac{}{\vdash \top, \Gamma}\ \top$$

$$\frac{\vdash F, \Gamma}{\vdash ?F, \Gamma}\ ? \qquad \frac{\vdash F, ?\Gamma}{\vdash !F, ?\Gamma}\ !$$

$$\frac{\vdash \Gamma}{\vdash ?F, \Gamma}\ ?W \qquad \frac{\vdash ?F, ?F, \Gamma}{\vdash ?F, \Gamma}\ ?C$$

Caractéristiques importantes de la logique linéaire

- Grâce à la structure supplémentaire qui est introduite dans les séquents, on peut capturer des choses au niveau logique et non pas au niveau des termes comme en logique classique ;
- Le contrôle des règles structurelles permet une étude précise de l'élimination des coupures, qui, par le biais de la correspondance de Curry-Howard coincide avec l'exécution d'un programme fonctionnel ;
- Grâce à la richesse des séquents, il est possible de considérer des séquents comme contenant un état de calcul dans un processus de recherche de preuves.
- De nombreuses autres directions...

Curry-Howard : une correspondance entre preuves et programmes

Le λ-calcul : une notation pour les déductions, et bien plus

$$\frac{}{\Gamma, a \in A \vdash a \in A}\ Ax$$

$$\frac{\Gamma, a \in A \vdash p \in B}{\Gamma \vdash \lambda a.p \in A \Rightarrow B}\ \Rightarrow I \qquad \frac{\Gamma \vdash p \in A}{\Gamma \vdash \lambda^1 x.p \in \forall x A}\ \forall I \quad (\star)$$

$$\frac{\Gamma \vdash p \in A \quad \Gamma \vdash q \in B}{\Gamma \vdash (p, q) \in A \wedge B}\ \wedge I$$

$$\frac{\Gamma \vdash p \in A \Rightarrow B \quad \Gamma \vdash q \in A}{\Gamma \vdash (p)q \in B}\ \Rightarrow E \qquad \frac{\Gamma \vdash p \in \forall x A}{\Gamma \vdash (p)t \in A[t/x]}\ \forall E$$

$$\frac{\Gamma \vdash p \in A \wedge B}{\Gamma \vdash \pi_1(p) \in A}\ \wedge E1 \qquad \frac{\Gamma \vdash p \in A \wedge B}{\Gamma \vdash \pi_2(p) \in B}\ \wedge E2$$

$(\star)$ Pour cette règle, x n'est pas libre dans Γ.

Le λ-calcul : une notation pour les déductions, et bien plus

$$\frac{}{\Gamma, a \in A \vdash a \in A}\ Ax$$

$$\frac{\Gamma, a \in A \vdash p \in B}{\Gamma \vdash \lambda a.p \in A \Rightarrow B}\ \Rightarrow I \qquad \frac{\Gamma \vdash p \in A}{\Gamma \vdash \lambda^1 x.p \in \forall x A}\ \forall I \quad (\star)$$

$$\frac{\Gamma \vdash p \in A \quad \Gamma \vdash q \in B}{\Gamma \vdash (p, q) \in A \wedge B}\ \wedge I$$

$$\frac{\Gamma \vdash p \in A \Rightarrow B \quad \Gamma \vdash q \in A}{\Gamma \vdash (p)q \in B}\ \Rightarrow E \qquad \frac{\Gamma \vdash p \in \forall x A}{\Gamma \vdash (p)t \in A[t/x]}\ \forall E$$

$$\frac{\Gamma \vdash p \in A \wedge B}{\Gamma \vdash \pi_1(p) \in A}\ \wedge E1 \qquad \frac{\Gamma \vdash p \in A \wedge B}{\Gamma \vdash \pi_2(p) \in B}\ \wedge E2$$

$(\star)$ Pour cette règle, x n'est pas libre dans Γ.

λ-calcul de Church

Introduit par A. Church, indépendamment de la déduction naturelle. Uniquement trois constructions de λ-termes :

- la variable (x),
- l'abstraction, $\lambda x.p$: la fonction qui à x associe p et
- l'application, $(p)q$, de la fonction p à l'argument q.

NB : $\lambda x.(x)x = \lambda y.(y)y$. Le λ est un lieur qui rend les variables muettes.

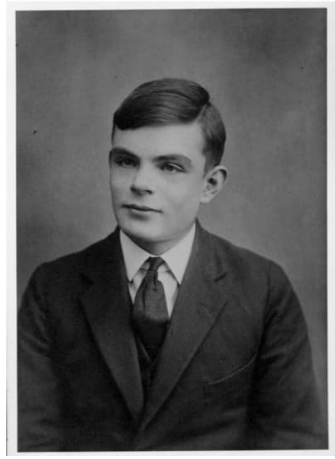
Une unique règle de calcul, la beta-réduction : $(\lambda x.p)q \longrightarrow_\beta p\{q/x\}$

Représenter des données avec des λ-termes :

- $\overline{n} = \lambda s.\lambda z.(s)^n z = \lambda s.\lambda z.(s)(s)...(s)z$
- $\text{add} = \lambda n.\lambda m.\lambda s.\lambda z.((n)s)(m)sz$ $\qquad ((\text{add})\overline{n})\overline{m} \longrightarrow \cdots \longrightarrow \overline{n+m}$
- mult, exp peuvent aussi être définies !
- $\lambda x.(x)x$ fonction qui applique sont argument... à lui-même
- Toute λ-terme p a un point-fixe (ie. un x tel que $(p)x = x$) ; il existe même un λ-terme qui calcule ces points fixes.

Base de la programmation fonctionnelle et récursive.

Le λ-calcul est un modèle de calcul universel



Thèse de Church(-Turing) :
Toute fonction calculable se définit en λ-calcul.

De très bonnes propriétés :

- si un calcul termine, son résultat est unique ;
- on dispose d'une méthode pour trouver, à coup sûr, ce résultat (s'il existe) ;
- mais, des calculs qui ne terminent pas : $(\lambda x.(x)x)\ \lambda y.(y)y \longrightarrow_\beta (x)x\{\lambda y.(y)y/x\} = (\lambda y.(y)y)\ \lambda y.(y)y \longrightarrow_\beta \ldots$ et
- il n'y a pas d'algorithme permettant de décider, quand on lui fournit un λ-terme p, si le calcul de p termine ou non (problème de l'arrêt).

Parce qu'on ne distingue pas les domaines de définition des fonctions : elles s'impliquent à n'importe quel objet : λ-calcul non typé.

λ-calcul typé et correspondance de Curry-Howard

Revenons sur l'annotation (simplifiée) de la déduction naturelle :

$$\frac{}{\Gamma, a : A \vdash a : A}\ Ax \qquad \frac{\Gamma, a : A \vdash p : B}{\Gamma \vdash \lambda a.p : A \Rightarrow B}\ \Rightarrow I \qquad \frac{\Gamma \vdash p : A \Rightarrow B \quad \Gamma \vdash q : A}{\Gamma \vdash (p)q : B}\ \Rightarrow E$$

On voit que cette annotation décrit :

- Les formules décrivent les domaines de définition des λ-termes ;
- Les preuves correspondent à certains λ-termes (qui les annotent) ;
- La β-réduction correspond à la simplification des coupures de NJ ;
- Certains λ-termes ne sont l'annotation d'aucune déduction (par exemple l'auto-application, $\lambda x.(x)x$). Ceux qui le sont sont dit typables.

Theorem (Terminaison / Normalisation forte)

Si un λ-terme est l'annotation d'une déduction naturelle, alors tous ses calculs terminent. En particulier, le calcul fournit un unique résultat.

Des fonctions qui croissent trop vite


La fonction d'Ackermann-Péter :

$$AP(m,n) = \begin{cases} n+1 & \text{si } m = 0 \\ AP(m-1,1) & \text{si } m > 0, n = 0 \\ AP(m-1, AP(m,n-1)) & \text{si } m > 0, n > 0 \end{cases}$$

n'est pas définissable dans le calcul précédent, parce qu'elle croît trop vite : la preuve de termination du λ-calcul typé n'est pas assez puissante.

Des fonctions qui croissent trop vite


La fonction d'Ackermann-Péter :

$$AP(m,n) = \begin{cases} n+1 & \text{si } m = 0 \\ AP(m-1,1) & \text{si } m > 0, n = 0 \\ AP(m-1, AP(m,n-1)) & \text{si } m > 0, n > 0 \end{cases}$$

n'est pas définissable dans le calcul précédent, parce qu'elle croît trop vite : la preuve de termination du λ-calcul typé n'est pas assez puissante.

Le Système T de Gödel étend le λ-calcul typé et permet définir AP. Contient des entiers primitifs et un récurseur dont le type correspond à l'axiome de récurrence de l'arithmétique de Peano.

Le Système F de Girard permet de définir toutes les fonctions définissables dans T, et bien plus. F étend la correspondance de Curry-Howard à la logique du second-ordre (quantification sur les prédicats).

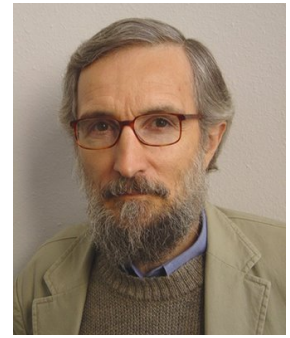
Quoi qu'on fasse pour étendre ces systèmes typés (et **terminant**) il restera des fonctions récursives totales qu'on ne pourra pas représenter.

(La preuve repose sur un argument diagonal.)

λ-calcul typé et correspondance de Curry-Howard

Déduction	Programmation
Formule	Types de données
Déduction naturelle	λ-terme typé
Coupure	β-redex
Simplication d'une coupure	β-réduction
Preuve sans coupure	Programme évalué, valeur
Implication	Type fonctionnel
Conjonction	Type produit (paires)
Disjonction	Type somme (union disjointe)
Constante vrai	Type singleton
Axiome de récurrence	Récursion
Quantification du second-ordre	Polymorphisme
...	...

Théorie des types dépendants



L'interprétation BHK fait apparaître une proximité troublante entre quantification universelle et implication :

- Une preuve de $A \Rightarrow B$ est une *fonction* qui associe à toute preuve de A une preuve de B (c'est donc une transformation de preuves) ;
- Une preuve de $\forall x A$ est une fonction qui associe à chaque terme t une preuve de $A[t/x]$.

Cela conduit Per Martin-Löf à unifier quantification et implication et à introduire la notion de type dépendant.

Idée de base : une famille indexée de type : $T_0 \times T_0 \times \cdots \times T_i \times \ldots$. Ce qu'on notera $\Pi_{i \in \mathbb{N}} T_i$. Un élément de ce type sera une suite $(p_i)_{i \in \mathbb{N}}$ dont le $k$ème élément, p_k appartiendra au type T_k.

$$\frac{\Gamma, a : A \vdash p : B}{\Gamma \vdash \lambda a.p : \Pi a : A.B} \qquad \frac{\Gamma \vdash p : \Pi a : A.B \quad \Gamma \vdash q : A}{\Gamma \vdash (p)q : B\{q/a\}}$$

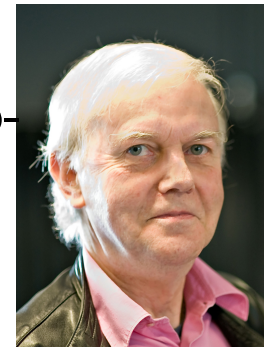
Ainsi qu'une théorie de l'égalité

Les assistants à la preuve

- Des logiciels qui permettent d'énoncer des théories mathématiques dans un cadre logique formel
- Qui proposent des outils d'aide à la démonstration (bibliothèques de résultats, recherche de lemmes, automatisation, etc.)
- Qui fournissent parfois également un environnement de programmation associé (langage de preuves et de programmation en même temps).
- Développement depuis les années 60 environ ;
- Nombreux outils existants : LCF, Isabel/HOL, Coq/Rocq, Mizar, Lean, etc.
- Gros résultats formalisés :
  - Théorème des quatre couleurs, par Gonthier et Werner ;
  - La preuve de la conjecture de Kepler a été formalisé par Hales ;
  - Le théorème de Feit-Thompson, par Gonthier et son équipe.
- Le coût de la formalisation tant à diminuer et il devient de plus en plus réaliste de formaliser des résultats mathématiques récente, voir notamment l'engouement autour de l'assistant Lean et de la bibliothèque Mathlib.

L'assistant de preuves Rocq (anciennement Coq)

Assistant de preuve dont le développement a débuté il y a 40 ans, avec G. Huet et T. Coquand.



- Initialement fondé sur le *calcul des constructions*, qui étend la théorie des types de Martin-Löf, la théorie logique de Coq/Rocq a ensuite été étendu par C. Paulin avec des *types inductifs* qui permettent de définir des types par une construction de plus petit point fixe, c'est le Calcul des Constructions Inductives (CIC).
- Par Curry-Howard, on a des prédicat inductifs, qui viennent avec des principes de raisonnement inductifs (ie par récurrence).
- Coq/Rocq est construit autour d'un langage qui implémente CIC (gallina) et d'un mode interactif de construction de preuves.
- À part l'implication et la quantification, les autres connecteurs logiques sont définis grâce aux types inductifs.

Conclusion

Règles structurelles : Les règles qui semblent, à première vue, être les moins signifiantes de la logique (au point qu'elles n'apparaissent même pas dans la déduction naturelle) se révèlent cruciales pour une analyse preuve-théorique fine de la logique. Par le contrôle des règles structurelles, on peut *zoomer* et obtenir plus de détails sur les preuves.

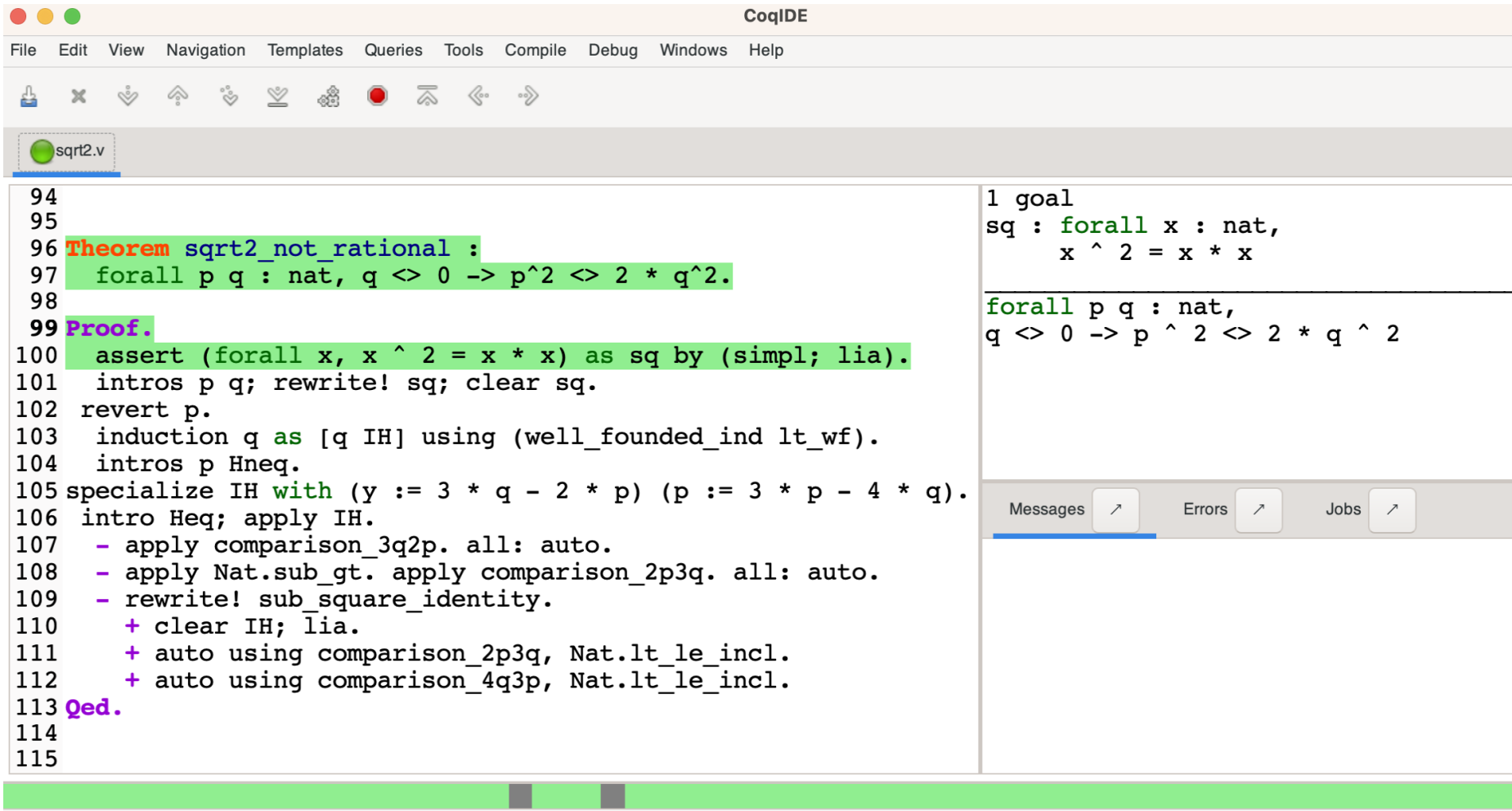
La contrainte intuitionniste / constructive peut être créatrice : où a émergé la correspondance preuves-programmes et s'est développée une passerelle fructueuse entre logique et programmation.

Le déréalisme logique : richesse d'une approche déréaliste de la logique : au lieu de se concentrer uniquement (voire principalement) sur les notions de *vérité ou validité*, on peut concevoir une logique comme l'étude des propriétés calculatoires et géométriques des preuves, l'étude restant logique grâce à des conditions posées par exemple sur l'élimination des coupures, la symétrie, la cohérence, etc.

De la formalisation à la mécanisation des preuves : Une histoire en train de s'écrire... Pour aller plus loin : *Mathématiques assistées par ordinateur*, Assia Mahboubi :

`https://www.college-de-france.fr/fr/agenda/seminaire/programmer-demontrer-la-correspondance-de-curry-howard-au`

Mode de preuve interactif



Impression du terme de preuve