Jean Goubault-Larrecq

λ-calcul

9. Logique et arithmétique du premier ordre

Aujourd'hui

- Suite de notre étude du λ-calcul simplement typé: logique **du premier ordre**
- puis **arithmétique** (de Peano) du premier ordre
- On revient à une version intuitionniste… si vous voulez rajouter **C**, je vous laisse libre!

Et ce sera la fête à…

Qui est-ce?

Et ce sera la fête à… Kurt Gödel

Par Auteur inconnu — Familienalbum der Familie Gödel,
Scan from Gianbruno Guerrerio,
Kurt Gödel - Logische Paradoxien und mathematische Wahrheit, S.24,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=10595692

Kurt Gödel

Pour les articles homonymes, voir Go

Kurt Gödel, né le 28 avril 1906 à Brünn et mort le 14 janvier 1978 à Princeton (New Jersey), est un logicien et mathématicien autrichien naturalisé américain[n 1, 2].

Logique du premier ordre

La logique du premier ordre

- En plus de $\Rightarrow$, on a $\forall$
(aussi $\exists$, j'en parlerai de temps en temps)
- Pour ça, on a besoin:
— d'**expressions** (i+1, $f(g(a,j),i)$, etc.),
— de **formules atomiques** un peu plus complexes qu'avant ($P(i+1)$, $R(a,f(a,j))$, etc.)
— et de variables i, j, … sur lesquelles on peut quantifier (i.e., on peut écrire $\forall i, j \,.\, P(i+j) \Rightarrow R(i,f(i,j))$ par ex.)

Expressions

- On se donne:
- un ensemble dénombrable de **variables d'expressions** i, j, k, … (pour les distinguer des variables du λ-calcul)
- une **signature** $\sum$ = ensemble de couples f/n, f **symbole de fonction**, n son **arité** (= nb. d'arguments)
- Expressions $e, e', \ldots ::= i$
  $\mid f(e_1, \ldots, e_n)$ avec $f/n \in \sum$

Expressions

- Expressions $e, e', \ldots ::= i$
  $\mid f(e_1, \ldots, e_n)$ avec $f/n \in \Sigma$
- Par exemple, plus tard, pour l'arithmétique, on aura:
  $\Sigma = \{0/0, \mathrm{s}/1, +/2, */2\}$
- On écrira i+1 plutôt que +(i, s(0())) (lisibilité…)

Formules atomiques

- On se donne aussi des **symboles de prédicats** P/n
- **Formules atomiques** $A ::= P(e_1, \ldots, e_n)$
- Par ex., pour l'arithmétique, $\approx/2$ (uniquement)
  (oui, j'écris ≈ en syntaxe, pour la distinguer de la relation d'égalité =, qui est de la sémantique)
- On écrira $i+1\approx j$ plutôt que $\approx(i+1, j)$ (lisibilité…)

Formules

- On se donne aussi des **symboles de prédicats** P/n
- **Formules atomiques** $A ::= P(e_1, \ldots, e_n)$
- Formules $F, G, \ldots ::= A$ (formules atomiques)

$$\begin{array}{lll} F, G, \ldots ::= & A & \text{(formules atomiques)} \\ & \mid F \Rightarrow G & \text{(comme en logique prop.)} \\ & \mid \forall i \,.\, F & \text{(nouveau)} \end{array}$$

Déduction naturelle (=typage)

- Types (formules):

$$F, G, \ldots ::= A \mid F \Rightarrow G \mid \forall i \,.\, F$$

- Termes:

$$u, v, \ldots ::= x \mid uv \mid \lambda x.u \mid ue \mid \Lambda i \,.\, u$$

- Réduction:

$(\beta)\quad (\lambda x.u)v \to u[x{:=}v]$

$(B)\quad (\Lambda i \,.\, u)e \to u[i{:=}e]$

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

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

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

$$\frac{\Gamma \vdash u : \forall i \,.\, G}{\Gamma \vdash ue : G[i{:=}e]}\,(\forall\mathrm{E})$$

$$\frac{\Gamma \vdash u : G}{\Gamma \vdash \Lambda i \,.\, u : \forall i \,.\, G}\,(\forall\mathrm{I})$$

(si *i* pas libre dans [aucune des formules de] Γ)

Propriétés fondamentales

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

$$\frac{\Gamma \vdash u : F \Rightarrow G \quad \Gamma \vdash v : F}{\Gamma \vdash uv : G}\ (\Rightarrow\mathrm{E}) \qquad \frac{\Gamma, x{:}F \vdash u : G}{\Gamma \vdash \lambda x.u : F \Rightarrow G}\ (\Rightarrow\mathrm{I})$$

$$\frac{\Gamma \vdash u : \forall i\,.\,G}{\Gamma \vdash ue : G[i{:=}e]}\ (\forall\mathrm{E}) \qquad \frac{\Gamma \vdash u : G}{\Gamma \vdash \Lambda i\,.\,u : \forall i\,.\,G}\ (\forall\mathrm{I})$$

(si i pas libre dans [aucune des formules de] Γ)

$(\beta)\quad (\lambda x.u)v \to u[x{:=}v]$

$(B)\quad (\Lambda i\,.\,u)e \to u[i{:=}e]$

- Ceci est la **logique** (intuitionniste minimale) **du premier ordre**

- **Autoréduction:** si $\Gamma \vdash u : F$ est dérivable et $u \to v$ alors $\Gamma \vdash v : F$ est dérivable.

- **Normalisation forte:** si $\Gamma \vdash u : F$ est dérivable, alors u est fortement normalisable.

- D'où **cohérence:** on ne peut pas prouver toute formule.

Normalisation forte

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

$$\frac{\Gamma \vdash u : F \Rightarrow G \quad \Gamma \vdash v : F}{\Gamma \vdash uv : G}\ (\Rightarrow\mathrm{E}) \qquad \frac{\Gamma, x{:}F \vdash u : G}{\Gamma \vdash \lambda x.u : F \Rightarrow G}\ (\Rightarrow\mathrm{I})$$

$$\frac{\Gamma \vdash u : \forall i\,.\,G}{\Gamma \vdash ue : G[i{:=}e]}\ (\forall\mathrm{E}) \qquad \frac{\Gamma \vdash u : G}{\Gamma \vdash \Lambda i\,.\,u : \forall i\,.\,G}\ (\forall\mathrm{I})$$

(si i pas libre dans [aucune des formules de] Γ)

$(\beta)\quad (\lambda x.u)v \to u[x{:=}v]$

$(B)\quad (\Lambda i\,.\,u)e \to u[i{:=}e]$

- C'est facile!
  (Candidats pas nécessaires.)

- Fonction **d'effacement**:
  enlève tout ce qui est du premier ordre

- $E(P(e_1, \ldots, e_n))=P \quad E(\forall i\,.\,F)=E(F) \quad E(F \Rightarrow G)=E(F)\Rightarrow E(G)$

  $E(\Lambda i\,.\,u)=E(u) \quad E(ue)=E(u)$

  $E(uv)=E(u)E(v) \quad E(\lambda x.u)= \lambda x.E(u) \quad E(x)=x$

- **Observation clé:** Si $\Gamma \vdash u : F$ au premier ordre,
  alors $E(\Gamma) \vdash E(u) : E(F)$ en types simples.

Normalisation forte

- **Observation clé:** Si $\Gamma \vdash u : F$ au premier ordre,
  alors $E(\Gamma) \vdash E(u) : E(F)$ en types simples.
- Si $u \to v$ par (β), alors $E(u) \to E(v)$ par (β)
  Si $u \to v$ par (B), alors $E(u) = E(v)$

$$(\beta) \quad (\lambda x.u)v \to u[x{:=}v]$$
$$(B) \quad (\Lambda i\,.\,u)e \to u[i{:=}e]$$

- Supposons $\Gamma \vdash u : F$ au premier ordre,
  et $u{=}u_0 \to u_1 \to \ldots \to u_n \to^{\infty} \ldots$,
  alors $E(u_0) \to^{\leq 1} E(u_1) \to^{\leq 1} \ldots \to E(u_n) \to^{\leq 1} \ldots$ par (β)
- Or les termes simplement typés **terminent**

Normalisation forte

- Supposons $\Gamma \vdash u : F$ au premier ordre,
  et $u=u_0 \to u_1 \to \ldots \to u_n \to^\infty \ldots$,
  alors $E(u_0) \to^{\leq 1} E(u_1) \to^{\leq 1} \ldots \to E(u_n) \to^{\leq 1} \ldots$ par (β)

$(\beta)\quad (\lambda x.u)v \to u[x:=v]$
$(B)\quad (\Lambda i\,.\,u)e \to u[i:=e]$

- Or les termes simplement typés **terminent**
  donc: nb. fini de (β) dans la réduction
  $u=u_0 \to u_1 \to \ldots \to u_n \to^\infty \ldots$

- i.e., pour tout n assez grand, $u_n \to u_{n+1}$ est par (B):
  impossible car le nb. de Λ diminue strictement! □

Curry-Howard, suite

Curry-Howard

- Un programme de type $\forall i \,.\, F(i)$,
  c'est un programme qui prend une **valeur** *e*, et retourne une preuve de $F(e)$
- ~ types dépendants: **cons**: $\forall n \,.\, \textbf{int} \Rightarrow \textbf{list}(n) \Rightarrow \textbf{list}(n{+}1)$

Le quantificateur existentiel

- Un peu comme ∀,
  mais symétrique

$$\dfrac{\Gamma \vdash u : \forall i \,.\, G}{\Gamma \vdash ue : G[i{:=}e]}\;(\forall E) \qquad \dfrac{\Gamma \vdash u : G}{\Gamma \vdash \Lambda i \,.\, u : \forall i \,.\, G}\;(\forall I)$$

(si i pas libre dans [aucune des formules de] Γ)

$$\dfrac{\Gamma \vdash u : \exists i \,.\, G \qquad \Gamma, x{:}G \vdash v : H}{\Gamma \vdash \texttt{case}\; u \;\texttt{of}\; \iota(i, x) \mapsto v : H}\;(\exists E) \qquad \dfrac{\Gamma \vdash u : G[i{:=}e]}{\Gamma \vdash \iota(e, u) : \exists i \,.\, G}\;(\exists I)$$

(si i pas libre dans [aucune des formules de] Γ, H)

- Vous aurez sans doute aussi remarqué la ressemblance avec les règles du « ou »

Le quantificateur existentiel

- Nouvelle règle de réduction:
  $\texttt{case}\ \iota(e,u)\ \texttt{of}\ \iota(i,x) \mapsto v \;\to\; v[i{:=}e, x{:=}u]$

$$\frac{\Gamma \vdash u : \exists i\,.\,G \qquad \Gamma, x{:}G \vdash v : H}{\Gamma \vdash \texttt{case}\ u\ \texttt{of}\ \iota(i,x) \mapsto v : H}\ (\exists E) \qquad \frac{\Gamma \vdash u : G[i{:=}e]}{\Gamma \vdash \iota(e,u) : \exists i\,.\,G}\ (\exists I)$$

(si i pas libre dans [aucune des formules de] Γ, H)

- Vous aurez sans doute aussi remarqué la ressemblance avec les règles du « ou »

Curry-Howard

- $\texttt{case}\ \iota(e,u)\ \texttt{of}\ \iota(i,x) \mapsto v \ \longrightarrow\ v[i{:=}e, x{:=}u]$

$$\dfrac{\Gamma \vdash u : \exists i\,.\,G \qquad \Gamma, x{:}G \vdash v : H}{\Gamma \vdash \texttt{case}\ u\ \texttt{of}\ \iota(i,x) \mapsto v : H}\ (\exists E) \qquad\qquad \dfrac{\Gamma \vdash u : G[i{:=}e]}{\Gamma \vdash \iota(e,u) : \exists i\,.\,G}\ (\exists I)$$

(si i pas libre dans [aucune des formules de] Γ, H)

- $\exists n\,.\,\mathbf{list}(n)$ est juste le type des listes (de longueur arbitraire)

- Un élément canonique (terme clos en forme normale) de type $\exists n\,.\,\mathbf{list}(n)$ est un **couple** $\iota(e, u)$ où:
  — e est une expression (dénotant un entier, on imagine)
  — u est une liste de longueur e

Curry-Howard

- $\texttt{case}\ \iota(e,u)\ \texttt{of}\ \iota(i,x) \mapsto v \ \rightarrow\ v[i{:=}e, x{:=}u]$

$$\frac{\Gamma \vdash u : \exists i \,.\, G \qquad \Gamma, x{:}G \vdash v : H}{\Gamma \vdash \texttt{case}\ u\ \texttt{of}\ \iota(i,x) \mapsto v : H}\ (\exists E) \qquad \frac{\Gamma \vdash u : G[i{:=}e]}{\Gamma \vdash \iota(e,u) : \exists i \,.\, G}\ (\exists I)$$

(si i pas libre dans [aucune des formules de] Γ, H)

- En général, $\exists n \,.\, F(n)$ est un **type abstrait** (on cache la valeur de n)

- Un élément canonique (terme clos en forme normale) de type $\exists n \,.\, F(n)$ est un **couple** $\iota(e, u)$ où:
— e est une expression (dénotant un entier par ex.)
— u est un λ-terme / une preuve de type $F(e)$

Arithmétique du premier ordre
($\mathbf{PA}_1$, $\mathbf{HA}_1$)

PA_1 = logique du premier ordre + …

- Une **théorie** du premier ordre, c'est-à-dire un ensemble d'axiomes (qu'on mettrait donc dans Γ)

« Axiomes de Peano »

pour chaque formule F

- (Refl) $\forall i \,.\, i \approx i$
- (Subst) $\forall i, j \,.\, i{\approx}j \Rightarrow F(i) \Rightarrow F(j)$

  (plus formellement, $\forall i, j \,.\, i{\approx}j \Rightarrow F \Rightarrow F[i{:=}j]$)
- $\forall i \,.\, \neg 0{\approx}\mathrm{s}(i)$
- $\forall i, j \,.\, \mathrm{s}(i){\approx}\mathrm{s}(j) \Rightarrow i{\approx}j$
- $\forall i \,.\, i{+}0{\approx}i$
- $\forall i, j \,.\, i{+}\mathrm{s}(j){\approx}\mathrm{s}(i{+}j)$
- $\forall i \,.\, i{*}0{\approx}0$
- $\forall i, j \,.\, i{*}\mathrm{s}(j){\approx}i{*}j{+}i$

pour chaque formule F

- **Principe de récurrence:** $F(0) \Rightarrow (\forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))) \Rightarrow \forall j \,.\, F(j)$

Note

- **PA**$_1$ = arithmétique de Peano du 1er ordre
  = logique classique + ax. de Peano + récurrence
- **HA**$_1$ = arithmétique de **Heyting** du 1er ordre
  = log. **intuitionniste** + ax. de Peano + récurrence
- C'est cette dernière que nous allons étudier
  … les stakhanovistes ajouteront
  l'opérateur **C** de Felleisen pour obtenir **PA**$_1$!

La récurrence

- C'est la récurrence le (schéma d')axiome(s) important. On en fait une règle en tant que telle:

$$\frac{\Gamma \vdash u : F(0) \qquad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathtt{R}uve : F(e)}\ (\mathrm{Rec})$$

- On va évacuer le cas des axiomes de Peano par une ruse (un format de **preuve modulo**, comme en Coq; plus tard)

Simplifications de preuve (1/2)

$$\dfrac{\Gamma \vdash u : F(0) \qquad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathtt{R}uv0 : F(0)}\,(\mathrm{Rec})$$

$$\longrightarrow$$

$$\Gamma \vdash u : F(0)$$

Simplifications de preuve (2/2)

$$\dfrac{\Gamma \vdash u : F(0) \qquad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathtt{R}uv(\mathrm{s}(e)) : F(\mathrm{s}(e))}\ (\mathrm{Rec})$$

$$\longrightarrow$$

$$\dfrac{\dfrac{\Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash ve : F(e) \Rightarrow F(\mathrm{s}(e))}\ (\forall \mathrm{E}) \qquad \dfrac{\Gamma \vdash u : F(0) \qquad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathtt{R}uve : F(e)}\ (\mathrm{Rec})}{\Gamma \vdash ve(\mathtt{R}uve) : F(\mathrm{s}(e))}\ (\Rightarrow \mathrm{E})$$

La récurrence

$$\frac{\Gamma \vdash u : F(0) \qquad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathtt{R}uve : F(e)}\ \text{(Rec)}$$

$$\mathtt{R}uv0 \longrightarrow u$$

$$\mathtt{R}uv(\mathrm{s}(e)) \longrightarrow ve(\mathtt{R}uve)$$

- $\mathtt{R}$ est le **récurseur**: $\mathtt{R}uv$ est, moralement, la fonction g définie par:

$$g(0)=u \quad g(n+1) = v(n, g(n))$$

- Principe de **récurrence primitive**
  … mais à tous les types:
  le type de retour de g n'est pas juste **N**

ÜBER EINE BISHER NOCH NICHT BENÜTZTE
ERWEITERUNG DES FINITEN STANDPUNKTES

von Kurt Gödel, Princeton

P. Bernays hat wiederholt darauf hingewies
der Tatsache der Unbeweisbarkeit der Widers
Systems mit geringeren Beweismitteln als dene
eine Überschreitung des Rahmens der im Hilb
Mathematik nötig ist, um die Widerspruchsfre
Mathematik, ja sogar um die der klassische
beweisen. Da die finite Mathematik als die de
denz definiert ist[2], so bedeutet das (wie auch v
seignement mathématique, 34 (1935), p. 62 und 69

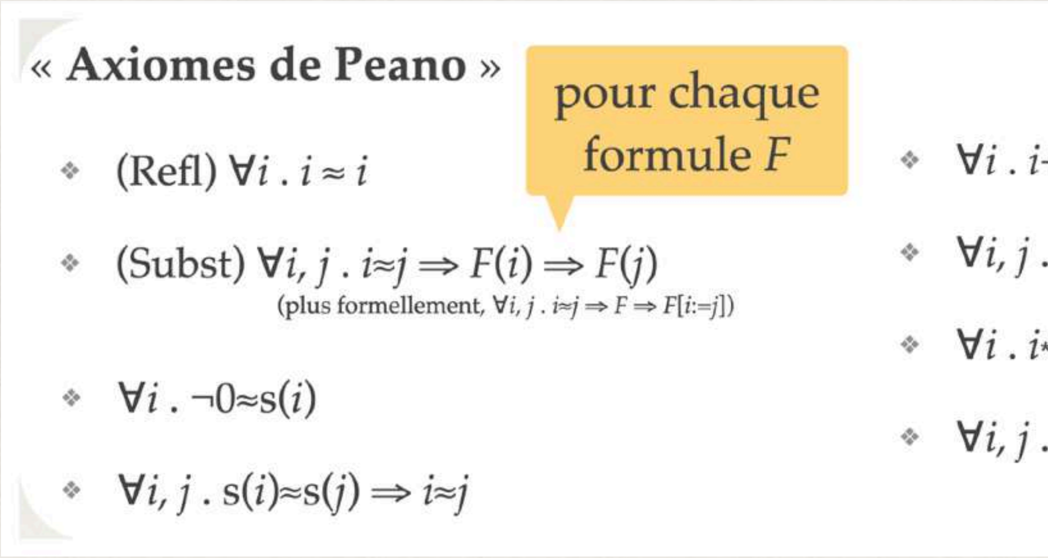
Par Auteur inconnu — Familienalbum der Familie Gödel,
Scan from Gianbruno Guerrerio,
Kurt Gödel - Logische Paradoxien und mathematische Wahrheit, S.24,
Domaine public,
`https://commons.wikimedia.org/w/index.php?curid=10595692`

Axiomes de Peano

- En principe, pour chaque axiome G, je devrais rajouter une constante $c_G : G$
- … et une palanquée de règles de simplification, par exemple:

  $$c_{(\mathrm{Subst})} e e (c_{(\mathrm{Refl})} e) u \to u$$

- Non, on va ruser.



Preuve modulo

- On va directement se donner un système de réécriture

$(0{\approx}\mathrm{s})$	$0{\approx}\mathrm{s}(e)$	$\rightarrow_{\mathbb{N}}$	$\bot$
$(\mathrm{s}{\approx}\mathrm{s})$	$\mathrm{s}(e){\approx}\mathrm{s}(e')$	$\rightarrow_{\mathbb{N}}$	$e{\approx}e'$
$(+0)$	$e+0$	$\rightarrow_{\mathbb{N}}$	e
$(+\mathrm{s})$	$e+\mathrm{s}(e')$	$\rightarrow_{\mathbb{N}}$	$\mathrm{s}(e+e')$
$({*}0)$	$e*0$	$\rightarrow_{\mathbb{N}}$	0
$({*}\mathrm{s})$	$e*\mathrm{s}(e')$	$\rightarrow_{\mathbb{N}}$	$e*e'+e$

- … et s'autoriser à simplifier les expressions et les formules via ce système de réécriture
(on remplace des **preuves** par des **calculs**)

HA_1 en preuve modulo

Logique du premier ordre (intuitionniste, et avec faux)

$$\frac{\Gamma \vdash u : \bot}{\Gamma \vdash \nabla u : F}\ (\bot E) \qquad \frac{}{\Gamma, x : F \vdash x : F}\ (Ax)$$

$$\frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2}\ (\Rightarrow E) \qquad \frac{\Gamma, x : F_1 \vdash u : F_2}{\Gamma \vdash \lambda x \cdot u : F_1 \Rightarrow F_2}\ (\Rightarrow I)$$

$$\frac{\Gamma \vdash u : \forall i \cdot F}{\Gamma \vdash ue : F[i{:=}e]}\ (\forall E) \qquad \frac{\Gamma \vdash u : F}{\Gamma \vdash \Lambda i \cdot u : \forall i \cdot F}\ (\forall I)$$

(où i n'est libre dans aucune formule de Γ)

$$\frac{}{\Gamma \vdash r_0 : 0 \approx 0}\ (Refl_0) \qquad \frac{\Gamma \vdash u : F_1 \quad F_1 \leftrightarrow^*_{\mathbb{N}} F_2}{\Gamma \vdash u : F_2}\ (\leftrightarrow^*_{\mathbb{N}})$$

Preuve modulo

Récurrence

$$\frac{\Gamma \vdash u : F[i := 0] \quad \Gamma \vdash v : \forall j \cdot F[i := j] \Rightarrow F[i := \mathtt{S}(j)]}{\Gamma \vdash \mathtt{R}uve : F[i := e]}\ (Rec)$$

Ah, et ça, c'est pour démarrer les preuves d'égalité!

(r_0 est une constante inerte, sans règle de réduction)

$\mathbf{HA}_1$ en preuve modulo

Logique du premier ordre (intuitionniste, et avec faux)

$$\frac{\Gamma \vdash u : \bot}{\Gamma \vdash \nabla u : F}\ (\bot E) \qquad \frac{}{\Gamma, x : F \vdash x : F}\ (Ax)$$

$$\frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2}\ (\Rightarrow E) \qquad \frac{\Gamma, x : F_1 \vdash u : F_2}{\Gamma \vdash \lambda x \cdot u : F_1 \Rightarrow F_2}\ (\Rightarrow I)$$

$$\frac{\Gamma \vdash u : \forall i \cdot F}{\Gamma \vdash ue : F[i{:=}e]}\ (\forall E) \qquad \frac{\Gamma \vdash u : F}{\Gamma \vdash \Lambda i \cdot u : \forall i \cdot F}\ (\forall I)$$

(où i n'est libre dans aucune formule de Γ)

$$\frac{}{\Gamma \vdash r_0 : 0 \approx 0}\ (Refl_0) \qquad \frac{\Gamma \vdash u : F_1 \quad F_1 \leftrightarrow^*_{\mathbb{N}} F_2}{\Gamma \vdash u : F_2}\ (\leftrightarrow^*_{\mathbb{N}})$$

Preuve modulo

$$\frac{\Gamma \vdash u : F[i := 0] \quad \Gamma \vdash v : \forall j \cdot F[i := j] \Rightarrow F[i := \mathtt{S}(j)]}{\Gamma \vdash \mathrm{R}uve : F[i := e]}\ (Rec)$$

Récurrence

Ceci prouve exactement la même chose que $\mathbf{HA}_1$…
voir Exercices 25–27 du poly (`types.pdf`)!

Réductions

Logique du premier ordre (intuitionniste, et avec faux)

$$\frac{\Gamma \vdash u : \bot}{\Gamma \vdash \nabla u : F}\ (\bot E) \qquad \frac{}{\Gamma, x : F \vdash x : F}\ (Ax)$$

$$\frac{\Gamma \vdash u : F_1 \Rightarrow F_2 \quad \Gamma \vdash v : F_1}{\Gamma \vdash uv : F_2}\ (\Rightarrow E) \qquad \frac{\Gamma, x : F_1 \vdash u : F_2}{\Gamma \vdash \lambda x \cdot u : F_1 \Rightarrow F_2}\ (\Rightarrow I)$$

$$\frac{\Gamma \vdash u : \forall i \cdot F}{\Gamma \vdash ue : F[i{:=}e]}\ (\forall E) \qquad \frac{\Gamma \vdash u : F}{\Gamma \vdash \Lambda i \cdot u : \forall i \cdot F}\ (\forall I)$$

(où i n'est libre dans aucune formule de Γ)

$$\frac{}{\Gamma \vdash r_0 : 0 \approx 0}\ (Refl_0)$$

Preuve modulo

$$\frac{\Gamma \vdash u : F_1 \quad F_1 \leftrightarrow^*_{\mathbb{N}} F_2}{\Gamma \vdash u : F_2}\ (\leftrightarrow^*_{\mathbb{N}})$$

Récurrence

$$\frac{\Gamma \vdash u : F[i := 0] \quad \Gamma \vdash v : \forall j \cdot F[i := j] \Rightarrow F[i := \mathsf{S}(j)]}{\Gamma \vdash \mathsf{R}uve : F[i := e]}\ (Rec)$$

Premier ordre (avec faux)

(β)	$(\lambda x \cdot u)v$	$\to$	$u[x := v]$	
(B)	$(\Lambda i \cdot u)e \to u[i{:=}e]$			
(∇)	∇uv	$\to$	∇u	$\nabla ue \to \nabla u$

Récurseur

$(\mathsf{R}0)$	$\mathsf{R}uv0$	$\to$	u
(RS)	$\mathsf{R}uv(\mathsf{s}(e))$	$\to$	$ve(\mathsf{R}uve)$

$\to_{\mathbb{N}}$

$(+0)$	$e{+}0$	$\to$	e
$(+\mathsf{S})$	$e{+}\mathsf{s}(e')$	$\to$	$\mathsf{s}(e{+}e')$
$(*0)$	$e{*}0$	$\to$	0
$(*\mathsf{S})$	$e{*}\mathsf{s}(e')$	$\to$	$e{*}e'{+}e$

Normalisation forte

Une mauvaise nouvelle

- Non, on ne pourra pas s'en tirer à coup d'effacement de tout ce qui est premier ordre…
- Si vous effacez le premier ordre dans:

$$\mathtt{R}uv0 \to u$$

$$\mathtt{R}uv(\mathrm{s}(e)) \to ve(\mathtt{R}uve)$$

vous obtenez:

$$\mathtt{R}uv \to u$$

$$\mathtt{R}uv \to v(\mathtt{R}uv)$$

qui ne termine plus…

Candidats de réductibilité

- Donc on va réutiliser les candidats de réductibilité
- $\mathrm{RED}_A = \mathrm{RED}_\perp = \mathrm{SN}$, $\mathrm{RED}_{F\Rightarrow G} = \mathrm{RED}_F \Rightarrow \mathrm{RED}_G$
  $\mathrm{RED}_{\forall i\,.\,F} = \{u \mid \text{pour tout } e,\ ue \in \mathrm{RED}_{F[i:=e]}\}$
- Juste un petit souci: pourquoi ceci est-il une définition valide? (par récurrence sur quoi?)

W.W. Tait

https://i1.rgstatic.net/ii/profile.image/279214973571093-1443581445569_Q512/William-Tait-3.jpg

- par récurrence sur $|F|$ par exemple, avec:
  $|A|=|\perp|=1 \quad |F\Rightarrow G|=|F|+|G|+1 \quad |\forall i\,.\,F|=|F|+1$
  Note: $|F[i:=e]| = |F|$ (exercice!) $< |\forall i\,.\,F|$

Candidats de réductibilité

- $\mathrm{RED}_A = \mathrm{RED}_\perp = \mathrm{SN}$, $\mathrm{RED}_{F\Rightarrow G} = \mathrm{RED}_F \Rightarrow \mathrm{RED}_G$
  $\mathrm{RED}_{\forall i\,.\,F} = \{u \mid \text{pour tout } e,\ ue \in \mathrm{RED}_{F[i:=e]}\}$

- Comme d'habitude:

  (neutre=ne commence pas par λ, Λ, ∇)

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

- **Lemme C.** Si (pour tout $v \in \mathrm{RED}_F$, $s[x:=v] \in \mathrm{RED}_G$) alors $\lambda x.s \in \mathrm{RED}_{F\Rightarrow G}$

- **Lemme D.** Si $u \in \mathrm{RED}_\perp$, alors pour tout type F, $\nabla u \in \mathrm{RED}_F$

Nouveaux résultats

(0≈s)	$0 \approx s(e)$	$\to_{\mathbb{N}}$	$\perp$
(s≈s)	$s(e) \approx s(e')$	$\to_{\mathbb{N}}$	$e \approx e'$
(+0)	$e+0$	$\to_{\mathbb{N}}$	e
(+s)	$e+s(e')$	$\to_{\mathbb{N}}$	$s(e+e')$
(*0)	$e*0$	$\to_{\mathbb{N}}$	0
(*s)	$e*s(e')$	$\to_{\mathbb{N}}$	$e*e'+e$

- **Lemme N.** $\to_{\mathbb{N}}$ termine.
- On définit une mesure $[e] \in \mathbb{N}$ telle que:
  — pour toute règle $e \to_{\mathbb{N}} e'$, $[e] > [e']$
  — si $[e] > [e']$ alors $[f(\ldots, e, \ldots)] > [f(\ldots, e', \ldots)]$
  pour tout symbole de fonction f
- Donc si $e \to_{\mathbb{N}} e'$ alors $[e] > [e']$.
  Or il n'y a pas de suites ∞ strict. décroissantes dans $\mathbb{N}$.
- Par ex. $[0]=1$, $[s(e)]=[e]+1$, $[e+e']=[e]+2[e']$, $[e*e']=[e](3[e']+1)$
  $[e \approx e']=[e]+[e']$, $[\perp]=0$

Deux invariants

(0≈s)	$0 \approx s(e)$	$\to_{\mathbb{N}}$	$\bot$
(s≈s)	$s(e) \approx s(e')$	$\to_{\mathbb{N}}$	$e \approx e'$
(+0)	$e+0$	$\to_{\mathbb{N}}$	e
(+s)	$e+s(e')$	$\to_{\mathbb{N}}$	$s(e+e')$
(*0)	$e*0$	$\to_{\mathbb{N}}$	0
(*s)	$e*s(e')$	$\to_{\mathbb{N}}$	$e*e'+e$

- $[\![i]\!]=[\![0]\!]=0 \quad [\![s(e)]\!]=[\![e]\!]+1 \quad [\![e+e']\!]=[\![e]\!]+[\![e']\!] \quad [\![e*e']\!]=[\![e]\!]\times[\![e']\!]$
  $[\![e \approx e']\!]=([\![e]\!]=[\![e']\!]) \quad [\![\bot]\!]=\text{faux}$

- Si $e \to_{\mathbb{N}} e'$ alors $[\![e]\!]=[\![e']\!]$ (exercice).

- **Lemme I.** si $F \to_{\mathbb{N}} F'$ alors $\mathrm{RED}_F = \mathrm{RED}_{F'}$.

- Par récurrence sur l'endroit où se passe la réduction… qui est forcément dans une formule atomique.

- Or si A, B atomiques (ou $\bot$), alors $\mathrm{RED}_A = \mathrm{RED}_B$ (=SN).

Le lemme dont on a besoin pour (Rec)

- **Lemme R.** Si $u \in \mathrm{RED}_{F(0)}$ et $v \in \mathrm{RED}_{\forall j\,.\,F(j) \Rightarrow F(\mathrm{s}(j))}$,
  alors $\mathsf{R}uve \in \mathrm{RED}_{F(e)}$ pour toute expression e.

- Avant de commencer à le prouver, notez que
  $\mathsf{R}uve$
  est une construction de notre λ-calcul étendu,
  pas R, pas $\mathsf{R}u$, pas $\mathsf{R}uv$.

- Ceci va simplifier la preuve, même si ce n'est pas indispensable: usuellement, on se contente de rajouter une constante de récurseur R.

Le lemme dont on a besoin pour (Rec)

- **Lemme R.** Si $u \in \mathrm{RED}_{F(0)}$ et $v \in \mathrm{RED}_{\forall j\,.\,F(j) \Rightarrow F(\mathrm{s}(j))}$,
  alors $\mathtt{R}uve \in \mathrm{RED}_{F(e)}$ pour toute expression e.

par récurrence sur quoi?

- Par (CR3)! $\mathtt{R}uve$ est neutre.
  Il y a **cinq cas:**

$$
\begin{tikzcd}
 & & & \mathtt{R}uve \arrow[dlll] \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathtt{R}u've & \mathtt{R}uv'e & \mathtt{R}uve' & u & ve^*(\mathtt{R}uve^*)
\end{tikzcd}
$$

(si e=0) (si e=s(e^*))

(comme d'habitude, u' est un réduit en une étape de u, etc.)

Le lemme dont on a besoin pour (Rec)

- **Lemme R.** Si $u \in \mathrm{RED}_{F(0)}$ et $v \in \mathrm{RED}_{\forall j\,.\,F(j) \Rightarrow F(\mathrm{s}(j))}$,
  alors $\mathtt{R}uve \in \mathrm{RED}_{F(e)}$ pour toute expression e.

par récurrence sur
$(\llbracket e \rrbracket, u, v, e)$,
prod. lexico de $\leq$, $\rightarrow$, $\rightarrow$, $\rightarrow_{\mathbb{N}}$

- Par (CR3)! $\mathtt{R}uve$ est neutre.
  Il y a **cinq cas**:

$\mathtt{R}uve$ $\rightarrow$

- $\mathtt{R}u've$: $\in \mathrm{RED}_{F(e)}$ (hyp. rec.)
- $\mathtt{R}uv'e$: $\in \mathrm{RED}_{F(e)}$ (hyp. rec.)
- $\mathtt{R}uve'$: $\in \mathrm{RED}_{F(e')} = \mathrm{RED}_{F(e)}$ (hyp. rec. + Lemme I)
- u (si e=0): (hyp.1)
- $ve^*(\mathtt{R}uve^*)$ (si e=s(e^*)): Ah… voyons ça en détail

Le cinquième cas

- On a $\mathtt{R}uve \to ve^*(\mathtt{R}uve^*)$,
  avec e=s(e^*)

par récurrence sur
($[\![e]\!]$, u, v, e),
prod. lexico de $\leq$, $\to$, $\to$, $\to_{\mathbb{N}}$

- Donc $[\![e^*]\!] < [\![e]\!]$ (qui vaut $[\![e^*]\!]+1$)
- On peut donc appliquer l'hyp. de récurrence:
  $$\mathtt{R}uve^* \in \mathrm{RED}_{F(e^*)}.$$
- Or $v \in \mathrm{RED}_{\forall j\,.\,F(j) \Rightarrow F(\mathrm{s}(j))}$,
  donc $ve^* \in \mathrm{RED}_{F(e^*) \Rightarrow F(\mathrm{s}(e^*))}$, i.e., $ve^* \in \mathrm{RED}_{F(e^*) \Rightarrow F(e)}$
- et donc $ve^*(\mathtt{R}uve^*) \in \mathrm{RED}_{F(e)}$.

Le lemme dont on a besoin pour (Rec)

- **Lemme R.** Si $u \in \mathrm{RED}_{F(0)}$ et $v \in \mathrm{RED}_{\forall j\,.\,F(j) \Rightarrow F(\mathrm{s}(j))}$,
  alors $\mathtt{R}uve \in \mathrm{RED}_{F(e)}$ pour toute expression e.

par récurrence sur
$(\llbracket e \rrbracket, u, v, e)$,
prod. lexico de $\leq$, $\to$, $\to$, $\to_{\mathbb{N}}$

- Par (CR3)! $\mathtt{R}uve$ est neutre.
  Il y a **cinq cas**:

$\mathtt{R}uve$

$\mathtt{R}u've$	$\mathtt{R}uv'e$	$\mathtt{R}uve'$	u	$ve^*(\mathtt{R}uve^*)$
			(si e=0)	(si e=s(e^*))
$\in \mathrm{RED}_{F(e)}$ (hyp. rec.)	$\in \mathrm{RED}_{F(e)}$ (hyp. rec.)	$\in \mathrm{RED}_{F(e')}$ $= \mathrm{RED}_{F(e)}$ (hyp. rec. + Lemme I)	(hyp.1)	$\in \mathrm{RED}_{F(e)}$ (cool.)

$\square$

Normalisation forte

- **Def:** $\theta \in \underline{\mathrm{RED}}_\Gamma$ ssi pour tout $x{:}F$ dans Γ, $\theta(x) \in \mathrm{RED}_F$
- **Thm.** si $\Gamma \vdash u : G$ dérivable alors
  pour toute $\theta \in \underline{\mathrm{RED}}_\Gamma$, $u\theta \in \mathrm{RED}_G$.
- Preuve: par récurrence sur la dérivation de $\Gamma \vdash u : G$,
  comme les dernières fois;
  on utilise la déf. de $\mathrm{RED}_{F \Rightarrow G}$ dans le cas de ($\Rightarrow$E),
  le Lemme C pour ($\Rightarrow$I), etc.
  Trois cas nouveaux… (prochains transparents)

Normalisation forte

- **Def:** $\theta \in \underline{\mathrm{RED}}_\Gamma$ ssi pour tout $x{:}F$ dans Γ, $\theta(x) \in \mathrm{RED}_F$
- **Thm.** si $\Gamma \vdash u : G$ dérivable alors
  pour toute $\theta \in \underline{\mathrm{RED}}_\Gamma$, $u\theta \in \mathrm{RED}_G$.
- **Cas (Rec):**

$$\frac{\Gamma \vdash u : F(0) \quad \Gamma \vdash v : \forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}{\Gamma \vdash \mathrm{R}uve : F(e)}\,(\mathrm{Rec})$$

- $u\theta \in \mathrm{RED}_{F(0)}$ et $v\theta \in \mathrm{RED}_{\forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}$ (hyp. réc.)
- donc $(\mathrm{R}uve)\theta \in \mathrm{RED}_{F(e)}$

Lemme R. Si $u \in \mathrm{RED}_{F(0)}$ et $v \in \mathrm{RED}_{\forall j \,.\, F(j) \Rightarrow F(\mathrm{s}(j))}$,
alors $\mathrm{R}uve \in \mathrm{RED}_{F(e)}$ pour toute expression e.

Normalisation forte

- **Def:** $\theta \in \underline{\mathrm{RED}}_\Gamma$ ssi pour tout $x{:}F$ dans Γ, $\theta(x) \in \mathrm{RED}_F$
- **Thm.** si $\Gamma \vdash u : G$ dérivable alors

  pour toute $\theta \in \underline{\mathrm{RED}}_\Gamma$, $u\theta \in \mathrm{RED}_G$.
- **Cas ($\longleftrightarrow_{\mathbb{N}}^*$):**

$$\frac{\Gamma \vdash u : F_1 \quad F_1 \leftrightarrow_{\mathbb{N}}^* F_2}{\Gamma \vdash u : F_2}\,(\leftrightarrow_{\mathbb{N}}^*)$$

Lemme I. si $F \rightarrow_{\mathbb{N}} F'$ alors $\mathrm{RED}_F = \mathrm{RED}_{F'}$.

Normalisation forte

- **Def:** $\theta \in \underline{\mathrm{RED}}_\Gamma$ ssi pour tout $x{:}F$ dans Γ, $\theta(x) \in \mathrm{RED}_F$
- **Thm.** si $\Gamma \vdash u : G$ dérivable alors

  pour toute $\theta \in \underline{\mathrm{RED}}_\Gamma$, $u\theta \in \mathrm{RED}_G$.
- **Cas (*Refl*$_0$):**

$$\frac{}{\Gamma \vdash r_0 : 0 \approx 0}\,(Refl_0)$$

- r_0 est normal… donc dans $\mathrm{SN} = \mathrm{RED}_{0\approx 0}$. $\square$

Normalisation forte

- **Thm.** Tout terme typable en $\mathbf{HA}_1$ est fortement normalisable.
- Voilà!
- Ceci implique la cohérence de $\mathbf{HA}_1$…

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre [sinon remplacer i par 0])
- … et de taille minimale
- u est de la forme $h\ t_1 \ldots t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est une variable ou ∇ ($n{\geq}1$) ou r_0 ($n{\geq}0$) ou $\mathtt{R}$ ($n{\geq}3$)

non: u est clos

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre [sinon remplacer i par 0])
- … et de taille minimale
- u est de la forme $h\ t_1 \ldots t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est ~~une variable~~ ou ∇ ($n{\geq}1$) ou r_0 ($n{\geq}0$) ou $\mathtt{R}$ ($n{\geq}3$)

non: $u{=}\nabla v$ par normalité,
avec $\vdash v : \bot$… contredit minimalité

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre [sinon remplacer i par 0])
- … et de taille minimale
- u est de la forme $h\ t_1 \ldots t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est ~~une variable ou ∇ (n≥1)~~ ou r_0 (n≥0) ou R (n≥3)

non: pas le bon type

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre [sinon remplacer i par 0])
- … et de taille minimale
- u est de la forme $h\ t_1 \ldots t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est ~~une variable ou ∇ ($n \geq 1$) ou r_0 ($n \geq 0$)~~ ou $\mathtt{R}$ ($n \geq 3$)

quelles sont les termes $\mathtt{R}uve$ normaux clos?

Les termes Ruve normaux clos

(0≈s)	$0 \approx s(e)$	$\to_{\mathbb{N}}$	$\perp$
(s≈s)	$s(e) \approx s(e')$	$\to_{\mathbb{N}}$	$e \approx e'$
(+0)	$e+0$	$\to_{\mathbb{N}}$	e
(+s)	$e+s(e')$	$\to_{\mathbb{N}}$	$s(e+e')$
(*0)	$e*0$	$\to_{\mathbb{N}}$	0
(*s)	$e*s(e')$	$\to_{\mathbb{N}}$	$e*e'+e$

- Les expr. e normales closes sont les $s^n(0)$ (exercice!)
- Mais Ruve n'est pas normal…
  - si $e=0$ (règle R$uv0 \to u$)
  - si $e=s(e^*)$ (règle R$uv(s(e^*)) \to ve^*(\mathrm{R}uve^*)$)
- Il n'y a **aucun** terme normal clos de la forme Ruve.

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre [sinon remplacer i par 0])
- … et de taille minimale
- u est de la forme $h\ t_1 \dots t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est ~~une variable ou ∇ ($n \geq 1$) ou r_0 ($n \geq 0$)~~ ou $\mathtt{R}$ ($n \geq 3$)

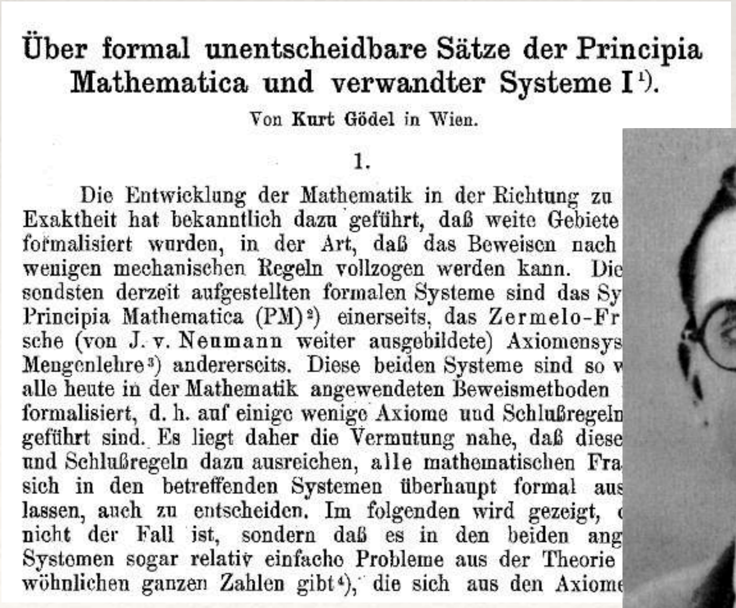
impossible

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Sinon, il en existerait une preuve **normale** u
- … et close (sans variable x ou i libre)
- … et de taille minimale
- u est de la forme $h\ t_0\ t_1\ \ldots\ t_n$ où:
  — chaque t_i est un λ-terme ou une expression
  — h est ~~une variable ou ∇ (n=1) ou r_0 (n=0) ou R (n≥3)~~ $\square$

Cohérence de l'arithmétique

- **Thm.** Il n'y a pas de preuve de $\vdash \bot$ en $\mathbf{HA}_1$.
- Par le second théorème d'incomplétude de Gödel, ce théorème n'est pas démontrable en $\mathbf{HA}_1$ (ou en $\mathbf{PA}_1$).



Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I[1].

Von **Kurt Gödel** in Wien.

1.

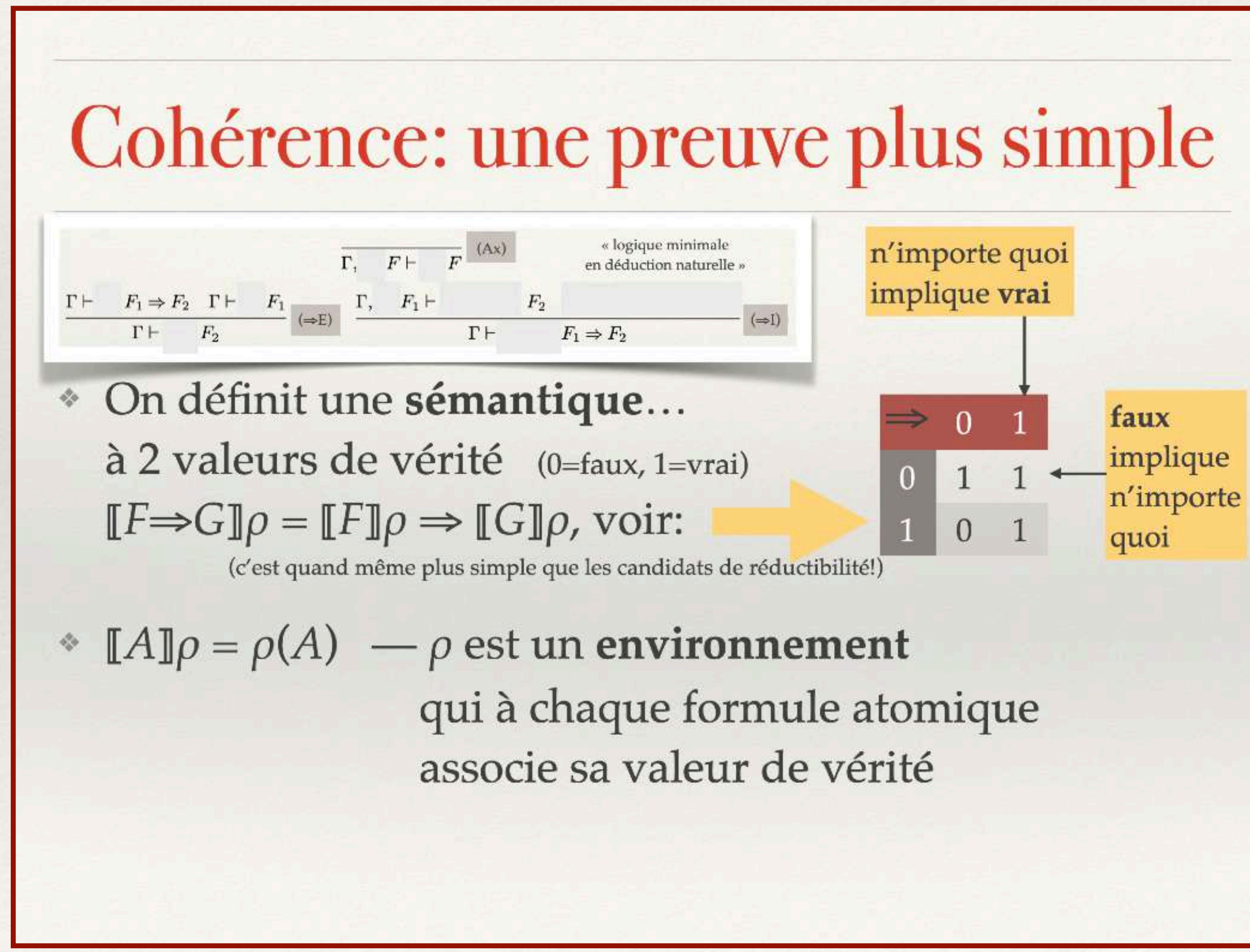
Die Entwicklung der Mathematik in der Richtung zu Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete formalisiert wurden, in der Art, daß das Beweisen nach wenigen mechanischen Regeln vollzogen werden kann. Die sondsten derzeit aufgestellten formalen Systeme sind das Sy Principia Mathematica (PM)[2] einerseits, das Zermelo-Fr sche (von J. v. Neumann weiter ausgebildete) Axiomensys Mengenlehre[3] andererseits. Diese beiden Systeme sind so w alle heute in der Mathematik angewendeten Beweismethoden formalisiert, d. h. auf einige wenige Axiome und Schlußregeln geführt sind. Es liegt daher die Vermutung nahe, daß diese und Schlußregeln dazu ausreichen, alle mathematischen Fra sich in den betreffenden Systemen überhaupt formal aus lassen, auch zu entscheiden. Im folgenden wird gezeigt, d nicht der Fall ist, sondern daß es in den beiden ang Systemen sogar relativ einfache Probleme aus der Theorie wöhnlichen ganzen Zahlen gibt[4], die sich aus den Axiome

Par Auteur inconnu — Familienalbum der Familie Gödel,
Scan from Gianbruno Guerrerio,
Kurt Gödel - Logische Paradoxien und mathematische Wahrheit, S.24,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=10595692

Une preuve de cohérence plus simple?

- Souvenez-vous de notre preuve de cohérence de la logique minimale intuitionniste

- Ici aussi, on peut donner une preuve **sémantique** de la cohérence de **HA**$_1$ (et de **PA**$_1$)



Cohérence: une preuve plus simple

$$\frac{}{\Gamma, F \vdash F}\ (\text{Ax}) \qquad \text{« logique minimale en déduction naturelle »}$$

$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2}\ (\Rightarrow\text{E}) \qquad \frac{\Gamma, F_1 \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}\ (\Rightarrow\text{I})$$

- On définit une **sémantique**…
  à 2 valeurs de vérité (0=faux, 1=vrai)
  $[\![F \Rightarrow G]\!]\rho = [\![F]\!]\rho \Rightarrow [\![G]\!]\rho$, voir:
  (c'est quand même plus simple que les candidats de réductibilité!)

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

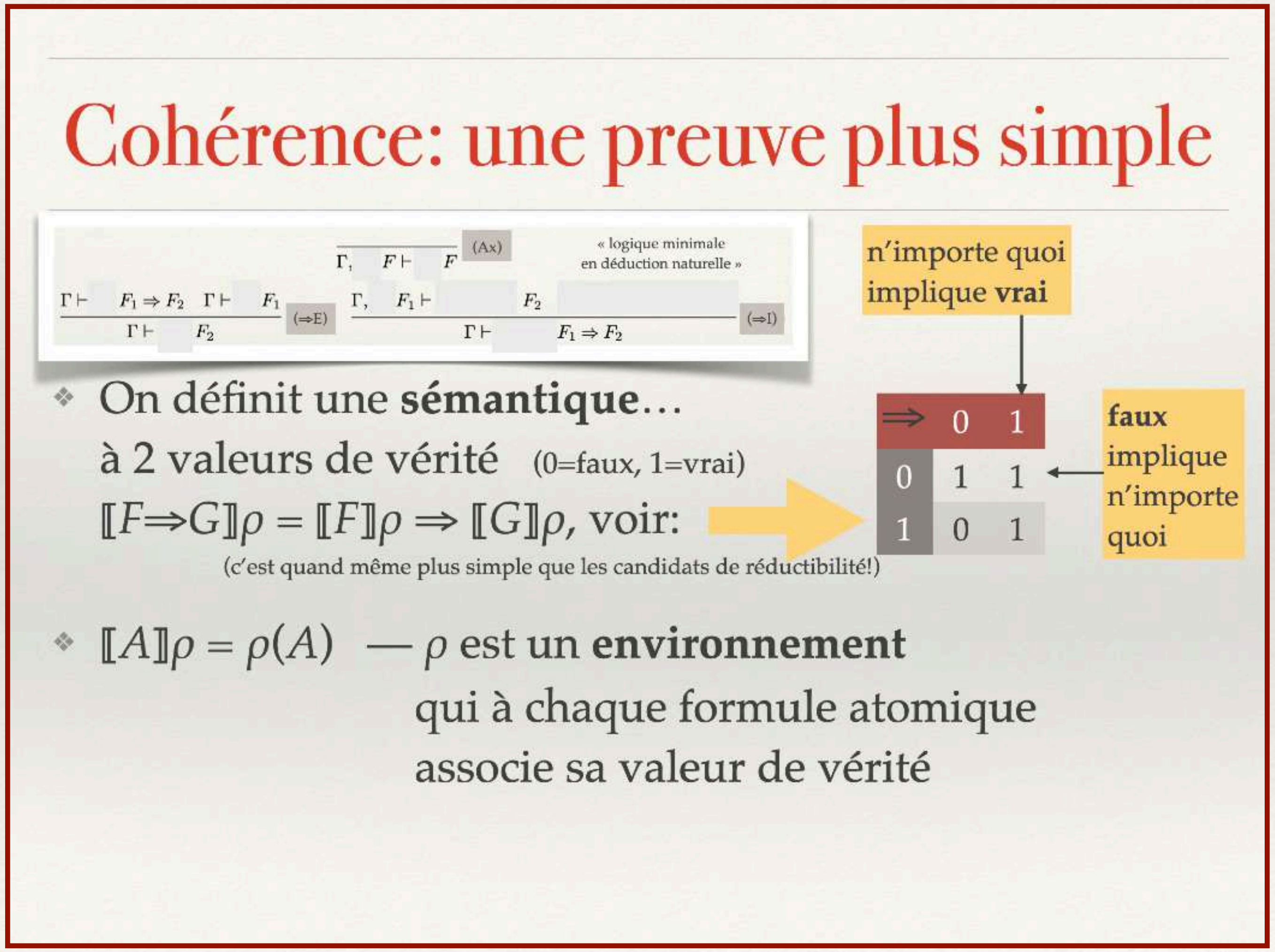
n'importe quoi implique **vrai**

faux implique n'importe quoi

- $[\![A]\!]\rho = \rho(A)$ — ρ est un **environnement** qui à chaque formule atomique associe sa valeur de vérité

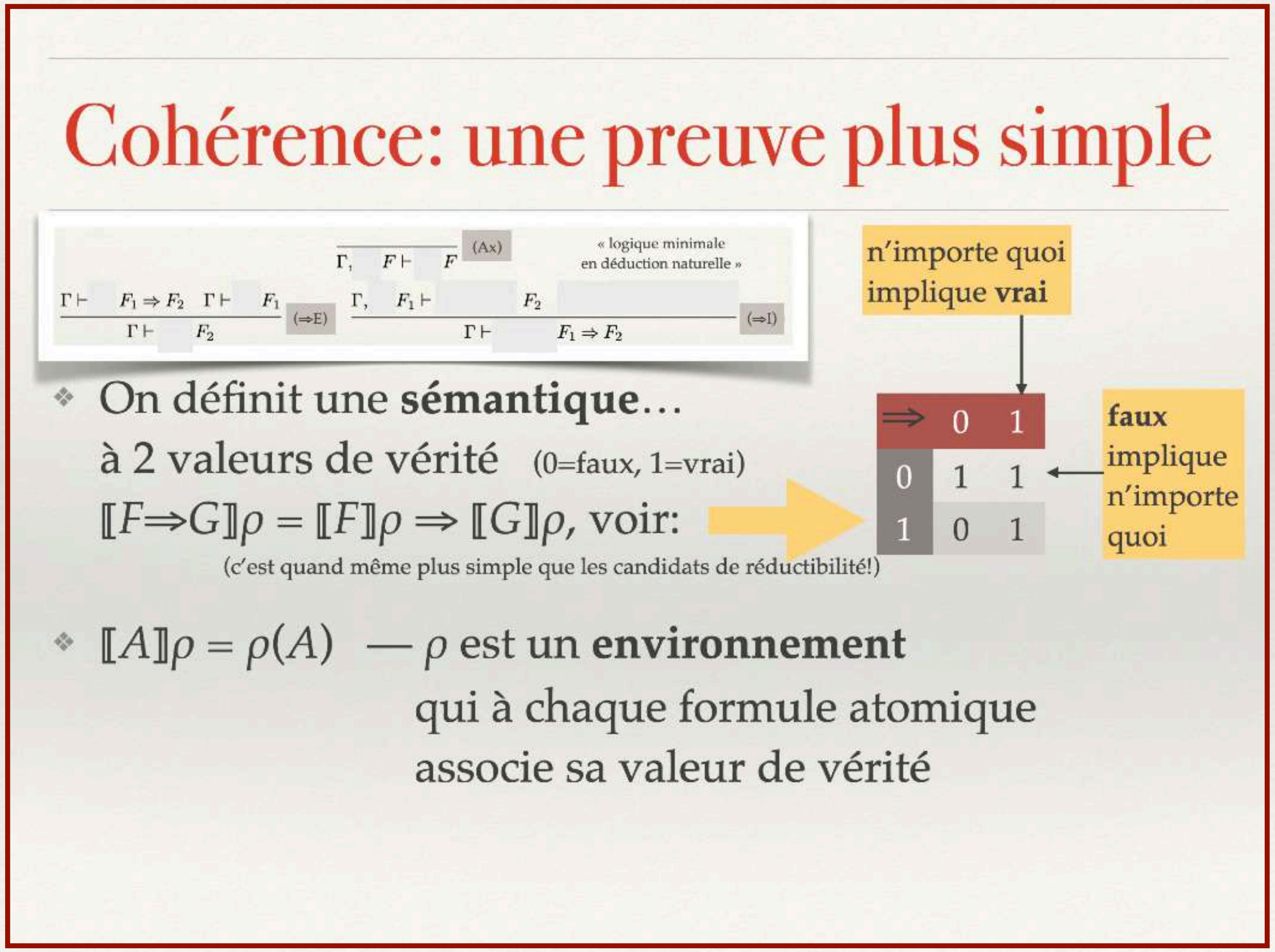
Une preuve de cohérence plus simple?

- Une preuve **sémantique** de la cohérence de $\mathbf{HA}_1$ (et $\mathbf{PA}_1$)
- On considère le **modèle standard**:
  les expressions sont interprétées comme des éléments de $\mathbb{N}$,
  $+$ comme $+$, $*$ comme $\times$,
  $\approx$ comme $=$, etc.



Une preuve de cohérence plus simple?

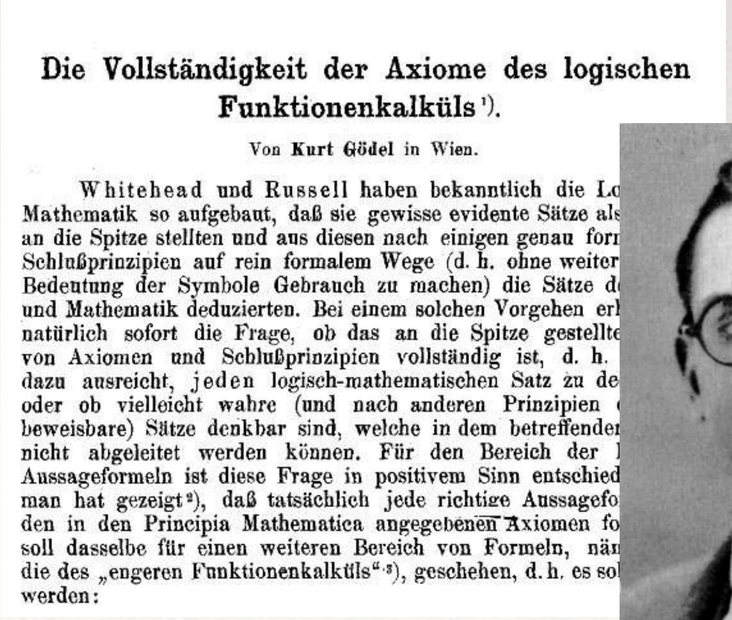
- Une preuve **sémantique** de la cohérence de $\mathbf{HA}_1$ (et $\mathbf{PA}_1$)
- On considère le **modèle standard**
- Si $\vdash F$ est dérivable, alors $[\![F]\!]$=vrai
- Or $[\![\bot]\!]\neq$vrai!



Une preuve de cohérence plus simple?

- Une preuve **sémantique** de la cohérence de $\mathbf{HA}_1$ (et $\mathbf{PA}_1$)
- On considère le **modèle standard**
- Si $\vdash F$ est dérivable, alors $[\![F]\!]$=vrai
- Or $[\![\perp]\!]\neq$vrai!

- … c'est une preuve circulaire:
- elle suppose qu'on a un modèle ($\mathbb{N}$) de $\mathbf{PA}_1$, or ceci est équivalent à la cohérence de $\mathbf{PA}_1$.



Die Vollständigkeit der Axiome des logischen Funktionenkalküls [1]).

Von **Kurt Gödel** in Wien.

Whitehead und Russell haben bekanntlich die Lo
Mathematik so aufgebaut, daß sie gewisse evidente Sätze als
an die Spitze stellten und aus diesen nach einigen genau forr
Schlußprinzipien auf rein formalem Wege (d. h. ohne weiter
Bedeutung der Symbole Gebrauch zu machen) die Sätze d
und Mathematik deduzierten. Bei einem solchen Vorgehen erl
natürlich sofort die Frage, ob das an die Spitze gestellte
von Axiomen und Schlußprinzipien vollständig ist, d. h.
dazu ausreicht, jeden logisch-mathematischen Satz zu de
oder ob vielleicht wahre (und nach anderen Prinzipien
beweisbare) Sätze denkbar sind, welche in dem betreffender
nicht abgeleitet werden können. Für den Bereich der
Aussageformeln ist diese Frage in positivem Sinn entschied
man hat gezeigt [2]), daß tatsächlich jede richtige Aussagefo
den in den Principia Mathematica angegebenen Axiomen fo
soll dasselbe für einen weiteren Bereich von Formeln, när
die des „engeren Funktionenkalküls" [3]), geschehen, d. h. es sol
werden:

Par Auteur inconnu — Familienalbum der Familie Gödel,
Scan from Gianbruno Guerrerio,
Kurt Gödel - Logische Paradoxien und mathematische Wahrheit, S.24,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=10595692

Un retour historique

- En 1900, David Hilbert propose 23 problèmes,
- dont le **deuxième:**

Par Auteur inconnu — Possibly Reid, Constance (1970)
Hilbert, Berlin, Heidelberg : Springer Berlin Heidelberg Imprint Springer, p. 230
ISBN : 978-3-662-27132-2.,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=36302

SUR LES

PROBLÈMES FUTURS DES MA

PAR M. DAVID HILBERT (Götti

II. — De la non-contradiction des axiomes de l'Arithmétique.

Lorsqu'il s'agit de poser les principes fondamentaux d'une science, l'on doit établir un système d'axiomes renfermant une description complète et exacte des relations entre les concepts élémentaires de cette science. Ces axiomes sont en même temps les définitions de

'avenir afin
t les secrets
s? Dans ce
quels seront
ides de la
eront, dans
découvertes

L'histoire enseigne la continuité du développement de la Science. Nous savons que chaque époque a ses problèmes que l'époque suivante résout, ou laisse de côté comme stériles, en les remplaçant

Un retour historique

- On a souvent interprété ce que dit Hilbert comme la recherche d'une preuve **finitiste** de non-contradiction de $\mathbf{PA}_1$
- i.e. n'utilisant que des quantifications sur des nombres, pas sur des ensembles

Par Auteur inconnu — Possibly Reid, Constance (1970)
g : Springer Berlin Heidelberg Imprint Springer, p. 230
ISBN : 978-3-662-27132-2.,
Domaine public,
wikimedia.org/w/index.php?curid=36302

II. — De la non-contradiction des axiomes de l'Arithmétique.

Lorsqu'il s'agit de poser les principes fondamentaux d'une science, l'on doit établir un système d'axiomes renfermant une description complète et exacte des relations entre les concepts élémentaires de cette science. Ces axiomes sont en même temps les définitions de

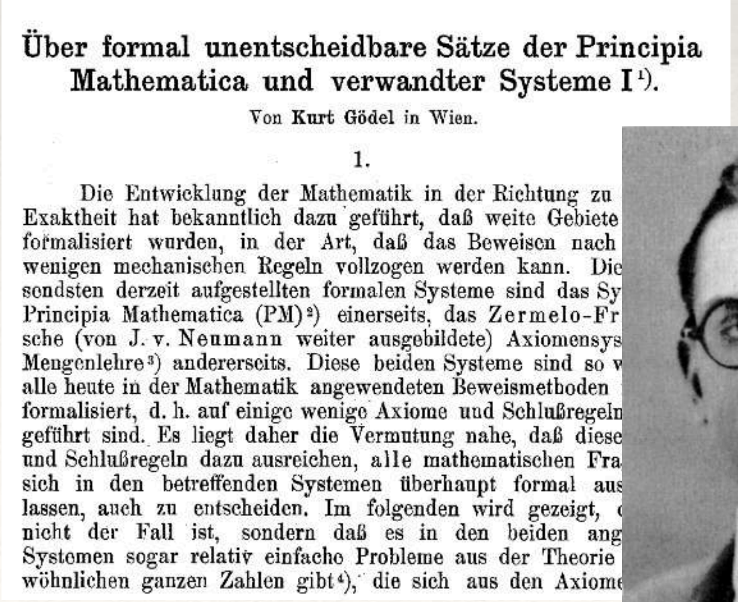
Un retour historique

- On a souvent interprété ce que dit Hilbert comme la recherche d'une preuve **finitiste** de non-contradiction de $\mathbf{PA}_1$
- i.e. ne travaillant que sur des nombres, pas sur des ensembles (comme $\mathbb{N}$)
- Nous avons obtenu une démonstration de non-contradiction de $\mathbf{HA}_1$

  (donc de $\mathbf{PA}_1$, en fait, par une autre astuce de Gödel)

  … elle n'est donc pas **finitiste**

Par Auteur inconnu — Possibly Reid, Constance (1970)
Hilbert, Berlin, Heidelberg : Springer Berlin Heidelberg Imprint Springer, p. 230
ISBN : 978-3-662-27132-2.,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=36302



Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I[1]).

Von Kurt Gödel in Wien.

1.

Die Entwicklung der Mathematik in der Richtung zu
Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete
formalisiert wurden, in der Art, daß das Beweisen nach
wenigen mechanischen Regeln vollzogen werden kann. Die
sondsten derzeit aufgestellten formalen Systeme sind das Sy
Principia Mathematica (PM)[2]) einerseits, das Zermelo-Fr
sche (von J. v. Neumann weiter ausgebildete) Axiomensys
Mengenlehre[3]) andererseits. Diese beiden Systeme sind so w
alle heute in der Mathematik angewendeten Beweismethoden
formalisiert, d. h. auf einige wenige Axiome und Schlußregeln
geführt sind. Es liegt daher die Vermutung nahe, daß diese
und Schlußregeln dazu ausreichen, alle mathematischen Fra
sich in den betreffenden Systemen überhaupt formal aus
lassen, auch zu entscheiden. Im folgenden wird gezeigt,
nicht der Fall ist, sondern daß es in den beiden ang
Systemen sogar relativ einfache Probleme aus der Theorie
wöhnlichen ganzen Zahlen gibt[4]), die sich aus den Axiome

Par Auteur inconnu — Familienalbum der Familie Gödel,
Scan from Gianbruno Guerrerio,
Kurt Gödel - Logische Paradoxien und mathematische Wahrheit, S.24,
Domaine public,
https://commons.wikimedia.org/w/index.php?curid=10595692

Quoi de finitiste dans notre preuve?

- Tous les objets 'informatiques'
(formules, preuves, termes, expressions, types)
sont **codables** comme des entiers
- Notre argument de cohérence:
'il n'existe pas de forme normale close de type $\perp$'
est finitiste
- Donc c'est quelque chose dans notre preuve de terminaison qui ne l'est pas… mais quoi?

Quoi de finitiste dans notre preuve?

- Donc c'est quelque chose dans notre preuve de terminaison qui ne l'est pas… mais quoi?
- Evidemment, la notion d'**ensemble** RED_F…
  mais ce n'est pas si simple.
- Au lieu d'écrire 'soit $u \in \mathrm{RED}_{F \Rightarrow G}$'
  on peut écrire
  'soit u tel que (pour tout $v \in \mathrm{RED}_F$, $uv \in \mathrm{RED}_G$)'
  et par récurrence sur le type, éliminer toute mention d'ensembles RED_F

Quoi de finitiste dans notre preuve?

- En fait, si je vous donne une dérivation d'un jugement **fixé** $\Gamma \vdash u : F$ en $\mathbf{HA}_1$,
- je peux vous refaire toute la preuve que u est fortement normalisant…
- en inlinant toutes les mentions d'ensembles RED_G et SN
- et cette preuve est formalisable en $\mathbf{HA}_1$ (« finitiste »)

Quoi de finitiste dans notre preuve?

- La seule chose non finitiste dans notre preuve, c'est la quantification universelle:
  pour tout jugement $\Gamma \vdash u : F$ en $\mathbf{HA}_1$, u termine.
- Phénomène bien connu (depuis Gödel): l'arithmétique n'est pas **ω-complète:**
  il existe une propriété P telle qu'on peut prouver $P(0)$, $P(1)$, …, $P(n)$, … (pour tout entier n), mais pas $\forall i \,.\, P(i)$

Curry-Howard

- Ce que nous dit notre formalisation de $\mathbf{HA}_1$, c'est que: les fonctions de $\mathbb{N}$ dans $\mathbb{N}$ prouvablement totales en $\mathbf{HA}_1$ sont celles codables en λ-calcul typé

  \+ **récurrence primitive à tous les types**

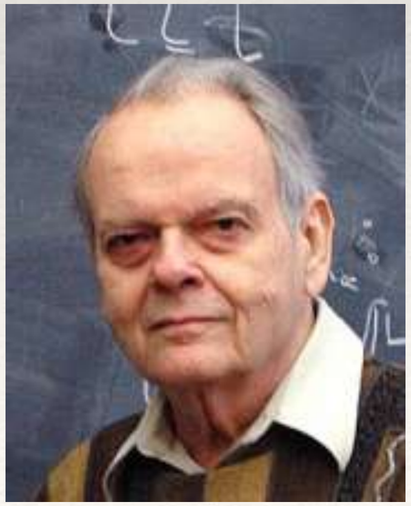
Curry-Howard

- Une **fonction prouvablement totale** (en $\mathbf{HA}_1$ avec $\exists$)
  est une formule $R(i,j)$
  telle qu'on peut prouver $\vdash \forall i \,.\, \exists j \,.\, R(i,j)$ en $\mathbf{HA}_1(+\exists)$.
- Soit u le terme de preuve associé, en forme normale.
- … u est de la forme $\Lambda i \,.\, \iota(e(i), \pi(i))$,
  où pour tout n, $e(n)$ termine
  et définit donc une valeur $f(n)$ — donc f est totale
  et $\vdash \pi(n) : R(n, e(n))$ est prouvable en $\mathbf{HA}_1(+\exists)$.

La prochaine fois

- Nous passerons à la quantification ∀ du **second ordre**
- C'est le **système F**,
  inventé en logique (Girard, 1971)
  pour donner une preuve « finitiste »
  de la cohérence de $\mathbf{PA}_2$
- et en informatique (Reynolds, 1974)
  pour donner un modèle
  du **polymorphisme** (préfigurant ML)

Jean-Yves Girard
(les candidats de réductibilité, c'est lui)
http://ekouter.net/img/img/JeanYvesGirard.jpg



John C. Reynolds
https://www.cs.cmu.edu/sites/default/files/styles/news_item_image/public/john-reynolds.jpg?itok=FGDq9ABS