Benjamin Werner

Benjamin.Werner@inria.fr

INRIA–Rocquencourt/Futurs

projet Logical

http://logical.inria.fr/~werner/

Logique du premier ordre

Les objets :

Un ensemble de symboles de fonction, chacun avec une arité $(f, g, h, \ldots)$

Un ensemble de variables :$x, y, z, \ldots$

• x est un objet,

• si $t_1, \ldots, t_n$ sont des objets, si f est d'arité n, alors $f(t_1, \ldots, t_n)$ est un objet.

Remarque : les constantes sont des fonctions d'arité 0.

Les objets sont essentiellement des arbres.

Les propositions

Un ensemble de symboles de prédicats, chacun muni d'une arité : $(P, Q, R, \ldots)$

Les connecteurs : $\wedge, \vee, \Rightarrow, \perp$

Les quantificateurs : $\forall, \exists$.

$$P(x, f(x, y)), \forall x. R(x, y) \Rightarrow \perp, x \leq y \Rightarrow x = y \wedge x \leq y - 1$$

Une théorie, c'est un tel langage avec un ensemble de propositions appellées les axiomes.

Théorie des ensembles, arithmétique de Peano. . .

$\boxed{\text{Substitution}}$

On note $A[x \setminus t]$ la substitution des ocurrences libres de x par t dans A.

$$
\begin{aligned}
P(t_1, \ldots, t_n)[x \setminus t] &\equiv P(t_1[x \setminus t, \ldots, t_n[x \setminus t]) \\
(A \wedge B)[x \setminus t] &\equiv A[x \setminus t] \wedge B[x \setminus t] \\
(\forall x.A)[x \setminus t] &\equiv \forall x.A \\
(\forall y.A)[x \setminus t] &\equiv \forall y.A[x \setminus t] \text{ si } y \text{ pas libre dans } t \\
(\forall y.A)[x \setminus t] &\equiv \forall y'.A[y \setminus y'][x \setminus t] \\
& \qquad\qquad \text{avec } y' \text{ pas libre dans } t \text{ et } A
\end{aligned}
$$

cf. cours de λ-calcul.

FOL, déduction naturelle

On note Γ un ensemble de propositions.

Un jugement $\Gamma \vdash P$ signifie : la proposition P est prouvée sous les hypothèses Γ.

On peut distinguer deux sortes de règles pour chaque connecteur/quantificateurs. Les règles d'introduction et les règles d'élimination.
Exemple :

$$\frac{\Gamma; A \vdash B}{\Gamma \vdash A \Rightarrow B} \ (\Rightarrow\text{-i}) \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \ (\Rightarrow\text{-e})$$

$$\boxed{\dfrac{}{\Gamma \vdash A} \ (\mathsf{Ax}) \ A \in \Gamma}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \ (\wedge\text{-i})$$

$$\frac{\Gamma; A \vdash B}{\Gamma \vdash A \Rightarrow B} \ (\Rightarrow\text{-i})$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \ (\Rightarrow\text{-e})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \ (\wedge\text{-e1})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \ (\wedge\text{-e2})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \ (\vee\text{-i1})$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \ (\vee\text{-i2})$$

$$\frac{\Gamma; A \vdash C \qquad \Gamma; B \vdash C \qquad \Gamma \vdash A \vee B}{\Gamma \vdash C} \ (\vee\text{-e})$$

Quantificateurs

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}$$ (∀-i) avec x pas libre dans Γ

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[x \setminus t]}$$ (∀-e)

$$\frac{\Gamma \vdash A[x \setminus t]}{\Gamma \vdash \exists x.A}$$ (∃-i)

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma; A \vdash B}{\Gamma \vdash B}$$ (∃-E)avec x pas libre dans $\Gamma; B$

Ces règles définissent la logique minimale.

Logique intuitioniste

On ajoute la règle pour la proposition fausse :

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P} \ (\bot\text{-}\mathsf{E})$$

$\boxed{\text{Logique Classique}}$

On ajoute le tiers-exclu :

$$\Gamma \vdash P \vee (P \Rightarrow \perp)$$

Arithmétique de Peano

Symboles de fonction : 0, S, +, *

Symbole de prédicat : =

axiomes :

$$\forall x\ .\ \neg 0 = S(x)$$

$$\forall xy\ .\ S(x) = S(y) \Rightarrow x = y$$

$$\forall x\ .\ x + 0 = x$$

$$\forall xy\ .\ x + S(y) = S(x + y)$$

$$\forall x\ .\ x * 0 = 0$$

$$\forall xy\ .\ x * S(y) = x + (x * y)$$

$$P(0) \wedge (\forall y.P(y) \Rightarrow P(S(y))) \Rightarrow \forall x.P(x)$$

Le dernier est en fait un schéma d'axiomes.

. . .et les axiomes de l'égalité :

– reflexivité : $\forall x \ . \ x = x$

– le schéma de Leibniz :

$$\forall xy \ . \ x = y \wedge P \Rightarrow P[x \setminus y]$$

Arithmétique de Peano : logique classique

Arithmétique de Heyting : logique intuitioniste

La déduction modulo

On se donne une *congruence* $=_R$ sur le langage.

Par exemple $x + 0 =_R x$,

$x * y = 0 \;\; =_R \;\; x = 0 \wedge y = 0 \ldots$

On identifie les propositions modulo $=_R$.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A'} A =_R A'$$

(on changera cette règle plus tard)

Un peu de modulo dans Peano

On prend pour $=_R$ la clôture reflexive, symétrique et transitive des règles de réécriture suivantes :

$$
\begin{array}{rcl}
0 + x & \rhd & x \\
S(x) + y & \rhd & S(x + y) \\
0 * x & \rhd & 0 \\
S(x) * y & \rhd & y + (x * y)
\end{array}
$$

On peut alors suprimer les quatre axiomes correspondants.

2+2=4 est prouvé par reflexivité.

La relation $=_R$ est décidable.

$\boxed{\text{Les Coupures}}$

La notion de coupure logique

$$\forall x.(x^2 - 1) = (x+1)(x-1)$$

On utilise le théorème général :

$$\forall a.\forall b.(a^2 - b^2) = (a+b)(a-b)$$

On peut transformer cette démonstration, en démonstration particulière au cas $a = x$ et $b = 1$

$$\cfrac{\cfrac{\cfrac{\ldots}{\Gamma \vdash A}\ (\forall\text{-i})}{\Gamma \vdash \forall x.A}\ (\forall\text{-e})}{\Gamma \vdash A[x \setminus t]} \quad \text{devient} \quad \cfrac{\ldots [x \setminus t]}{\Gamma \vdash A[x \setminus t]}$$

En déduction naturelle, une coupure est une règle d'introduction suivie d'une règle d'elimination.

$$\dfrac{\dfrac{\dfrac{\ldots}{\Gamma \vdash A} \qquad \dfrac{\ldots}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ (\wedge\text{-i})}{\Gamma \vdash A}\ (\wedge\text{-e1}) \qquad \dfrac{\dfrac{\dfrac{\ldots}{\Gamma; A \vdash B}}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow\text{-i}) \qquad \dfrac{\ldots}{\Gamma \vdash A}}{\Gamma \vdash B}\ (\Rightarrow\text{-e})$$

Il existe un moyen d'éliminer une coupure

Lemme : *Si* $\Gamma \vdash A$ *est dérivable, alors* $\Gamma[x \setminus t] \vdash A[x \setminus t]$ *est dérivable.*

Preuve : Par récurrence sur la structure (la taille) de la dérivation.

Lemme*(Affaiblissement)* : *Si* $\Gamma \vdash A$ *est dérivable, alors* $\Gamma; B \vdash A$ *est dérivable.*

Lemme : *Si* $\Gamma; A \vdash B$ *et* $\Gamma \vdash A$ *sont dérivables, alors* $\Gamma \vdash B$ *est dérivable*.

Cela suffit à définir une étape d'elimination de coupure pour chaque sorte de coupures.

Mais. . .

. . .chaque élimination peut créer de nouvelles coupures ! (substitution de preuves)

En fait, le processus termine, mais la preuve est compliquée. Nous l'admettons pour l'instant.

Théorème *(Hauptsatz)* : *Si* $\Gamma \vdash A$ *est dérivable, il existe une dérivation sans coupures de* $\Gamma \vdash A$*.*

Les preuves sans coupures En logique intuitioniste, une preuve sans coupures et sans hypothèses se termine toujours par une règle d'introduction.

Preuve : facile, par récurrence structurelle.

Si $\vdash A \vee B$ est prouvable en logique intuitioniste, alors on a $\vdash A$ ou $\vdash B$.

Si $\vdash \exists X.A$ est prouvable en logique intuitioniste, alors on peut trouver un terme t tel que $\vdash A[x \setminus t]$.

On ne peut pas prouver $\vdash \perp$.

Non-constructivité du tiers-exclu

Proposition : Il existe $a, b \in \mathbb{R} \setminus \mathbb{Q}$ tels que $a^b \in \mathbb{Q}$.

- $\sqrt{2} \notin \mathbb{Q}$ (facile).
- Si $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, on prend $a = b = \sqrt{2}$.
- Si $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, prenons $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$.

On a $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

CQFD.

Mais qui sont a et b ?

La forme de la preuve ne permet pas de le dire.

Coupures en déduction modulo

Une coupure est :

une règle introduction

un certain nombre de conversions

une règle d'elimination.

On simplifie en changeant un peu les règles.

Coupures en déduction modulo

- On suprime la règle de conversion.
- On la distribue dans les autres règles.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash C} \text{ ($\wedge$-i) } C =_R A \wedge B$$

Une coupure est bien une intro/élim.

L'élimination des coupures n'est pas toujours préservée.

Mais il n'y a pas de preuve sans coupure de $\vdash \bot$.

Exemple d'incohérence/non-terminaison :
$A \;\triangleright\; A \Rightarrow \bot$.

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\mathsf{Ax}) \quad \dfrac{}{A \vdash A \Rightarrow \bot}\,(\mathsf{Ax})}{\dfrac{A \vdash \bot}{\vdash A \Rightarrow \bot}\,(\Rightarrow\text{-i})}\,(\Rightarrow\text{-e}) \qquad \dfrac{\dfrac{}{A \vdash A}\,(\mathsf{Ax}) \quad \dfrac{}{A \vdash A \Rightarrow \bot}\,(\mathsf{Ax})}{\dfrac{A \vdash \bot}{\vdash A}\,(\Rightarrow\text{-i})}\,(\Rightarrow\text{-e})}{\bot}\,(\Rightarrow\text{-e})$$

$$\dfrac{\dfrac{\dfrac{\sigma}{A \vdash \bot}}{\vdash A \Rightarrow \bot}\,(\Rightarrow\text{-i}) \qquad \dfrac{\dfrac{\sigma}{A \vdash \bot}}{\vdash A}\,(\Rightarrow\text{-i})}{\bot}\,(\Rightarrow\text{-e})$$

$\boxed{\text{Cette preuve se réécrie en elle-même}}$

Coupures Axiomatiques

En présence d'axiomes, les preuves sans coupures de $\Gamma \vdash A$ sont a priori moins interessantes.

Dans certains cas, on peut retrouver les propriétés de constructivité en étendant la notion de coupure pour chaque axiome.

Ça marche très bien pour l'arithmétique de Heyting

Coupures d'égalité

$$
\dfrac{
  \dfrac{
    \dfrac{\dfrac{}{\Gamma \vdash \forall x.x = x}\;\text{(Ax)}}{t = t}\;(\forall\text{-e})
    \qquad
    \dfrac{\dfrac{}{\forall xy.x = y \Rightarrow A \Rightarrow A[x \setminus y]}\;\text{(Ax)}}{t = t \Rightarrow A[x \setminus t] \Rightarrow A[x \setminus t]}\;\forall\text{-e}
  }{A[x \setminus y] \Rightarrow A[x \setminus y]}
  \qquad
  \dfrac{\sigma}{A[x \setminus t]}
}{A[x \setminus t]}
$$

devient

$$
\dfrac{\sigma}{A[x \setminus t]}
$$

Ce type de coupure n'est pas spécifique à l'arithmétique.

$\boxed{\text{Coupures de récurrence}}$