LORIA – Université Henri Poincaré

Unbounded Proof-Length Speed-up in Deduction Modulo

Groupe de travail Logique, Algèbre et Calcul

Guillaume Burel

February 9th, 2007

Proving that the square of an even number is even:

Proving that the square of an even number is even:

Take a number x.

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Then it is the double of some number y. $(x = 2 \cdot y)$

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Then it is the double of some number y. $(x = 2 \cdot y)$

Then one can compute that the square of x is the double of the double of the square of y. $(x^2 = 2 \cdot (2 \cdot y^2))$

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Then it is the double of some number y. $(x = 2 \cdot y)$

Then one can compute that the square of x is the double of the double of the square of y. $(x^2 = 2 \cdot (2 \cdot y^2))$

Therefore the square of x is even.

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Then it is the double of some number y. $(x = 2 \cdot y)$

Then one can compute that the square of x is the double of the double of the square of y. $(x^2 = 2 \cdot (2 \cdot y^2))$

Therefore the square of x is even.

QED.

Proving that the square of an even number is even:

Take a number x.

Suppose it is even.

Then it is the double of some number y. $(x = 2 \cdot y)$

Then one can compute that the square of x is the double of the double of the square of y. $(x^2 = 2 \cdot (2 \cdot y^2))$

Therefore the square of x is even.

QED.

$$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$$

$$\forall\text{-i}\ \frac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$Even(x)$ (i)

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$Even(x)$ (i)

$\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)$ (def)

$$\dfrac{\dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \Rightarrow\text{-i (i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}\ \forall\text{-i}$$

$Even(x)$ (i)

$$\forall\text{-e}\ \frac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$Even(x)$ (i)

$$\dfrac{\exists y.\ x \cdot x = 2 \cdot y \qquad \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}\ \forall\text{-e}}{\dfrac{Even(x \cdot x)}{\dfrac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}\ \forall\text{-i}}\ \Rightarrow\text{-i}\ \text{(i)}}\ \Rightarrow\text{-e}$$

$$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \text{ (def)}$$

$$Even(x) \text{ (i)}$$

$$\Rightarrow\text{-e}\ \dfrac{\exists y.\ x \cdot x = 2 \cdot y \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x) \text{ (def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)} \text{ (i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}}$$

$$
Even(x)\ \text{(i)} \qquad \forall\text{-e}\ \frac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}
$$

$$
\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{\exists y.\ x \cdot x = 2 \cdot y \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{Even(x \cdot x)}}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}
$$

$$\Rightarrow\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad \forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}}{\exists y.\ x = 2 \cdot y}$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{\exists y.\ x \cdot x = 2 \cdot y \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{Even(x \cdot x)}\ \text{(i)}}{Even(x) \Rightarrow Even(x \cdot x)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$\Rightarrow\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad \forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2\cdot y\ \text{(def)}}{Even(x)\Rightarrow \exists y.\ x=2\cdot y}}{\exists\text{-e}\ \dfrac{\exists y.\ x = 2\cdot y}{x = 2\cdot y}}$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{\exists y.\ x\cdot x = 2\cdot y \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x=2\cdot y)\Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x\cdot x = 2\cdot y)\Rightarrow Even(x\cdot x)}}{Even(x\cdot x)}}{Even(x)\Rightarrow Even(x\cdot x)}\ \text{(i)}}{\forall x.\ Even(x)\Rightarrow Even(x\cdot x)}$$

$$\Rightarrow\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad \forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}}{\exists\text{-e}\ \dfrac{\exists y.\ x = 2 \cdot y}{x = 2 \cdot y}}$$

$$\Rightarrow\text{-e}\ \dfrac{\exists\text{-i}\ \dfrac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y} \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}}$$

$$
\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{\exists\text{-i}\ \dfrac{\dfrac{\exists\text{-e}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad \forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}}{\exists y.\ x = 2 \cdot y}}{x = 2 \cdot y}}{\overline{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}}\ ??}{\exists y.\ x \cdot x = 2 \cdot y} \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{Even(x \cdot x)}}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}
$$

Motivations

$$\exists\text{-e}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{Even(x)\ (\text{i}) \qquad \forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ (\text{def})}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}}{\exists y.\ x = 2 \cdot y}}{x = 2 \cdot y}$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{\Rightarrow\text{-e}\ \dfrac{\exists\text{-i}\ \dfrac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y} \qquad \forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ (\text{def})}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}}{Even(x \cdot x)}\ (\text{i})}{Even(x) \Rightarrow Even(x \cdot x)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$ (de

$\forall$-e

$Even(x)$ (i) $\quad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$

$\Rightarrow$ -e

$\exists y.\ x = 2 \cdot y$

$\exists$-e

$x = 2 \cdot y$

$\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (ax)

$x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$

$\exists$-i

$\exists y.\ x \cdot x = 2 \cdot y$

$\forall x.$

$\forall$-e

$(\exists$

$\Rightarrow$ -e

$Even(x \cdot x)$

$\Rightarrow$ -i (i)

$Even(x) \Rightarrow Even(x \cdot x)$

$\forall$-i

$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$

$$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \text{ (de}$$

∀-e

$$Even(x) \text{ (i)} \qquad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$$

⇒ -e

$$\exists y.\ x = 2 \cdot y$$

∃-e

$$x = 2 \cdot y$$

$$\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ (ax)}$$

∀-e ×3

$$(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y))$$

$$x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$$

∃-i

$$\exists y.\ x \cdot x = 2 \cdot y$$

$$\forall x.$$

∀-e

$$(\exists$$

⇒ -e

$$Even(x \cdot x)$$

⇒ -i (i)

$$Even(x) \Rightarrow Even(x \cdot x)$$

∀-i

$$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$$

Motivations

$$\dfrac{Even(x)\ \text{(i)} \qquad \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}\ \forall\text{-e}}{\dfrac{\exists y.\ x = 2 \cdot y}{x = 2 \cdot y}\ \exists\text{-e}}\ \Rightarrow\text{-e}$$

$$\forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z\ \text{(ax)}$$

π

$$\dfrac{\dfrac{\dfrac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y}\ \exists\text{-i} \qquad \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}\ \forall\text{-e}}{Even(x \cdot x)}\ \Rightarrow\text{-e}}{\dfrac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}\ \forall\text{-i}}\ \Rightarrow\text{-i (i)}$$

Motivations

$$\forall\text{-e}\ \frac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \ \text{(def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}$$

$$\Rightarrow\text{-e}\ \frac{Even(x)\ \text{(i)} \qquad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}{\exists y.\ x = 2 \cdot y}$$

$$\exists\text{-e}\ \frac{\exists y.\ x = 2 \cdot y}{x = 2 \cdot y}$$

$$\forall\text{-e}\ \frac{\forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z\ \text{(ax)}}{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot}$$

$$\pi$$

$$\exists\text{-i}\ \frac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y}$$

$$\forall\text{-e}\ \frac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}$$

$$\Rightarrow\text{-e}\ \frac{\exists y.\ x \cdot x = 2 \cdot y \qquad (\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}{Even(x \cdot x)}$$

$$\Rightarrow\text{-i}\ \frac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}$$

$$\forall\text{-i}\ \frac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \ \text{(def)}$$

$\forall$-e

$$Even(x)\ \text{(i)} \qquad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$$

$\Rightarrow$ -e

$$\exists y.\ x = 2 \cdot y$$

$\exists$-e

$$x = 2 \cdot y \qquad\qquad \forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z\ \text{(ax)}$$

$\forall$-e

$$x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \qquad x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot \ldots$$

$\Rightarrow$ -e

$$\pi \qquad (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$$

$$x \cdot x = 2 \cdot (y \cdot (2 \cdot y)) \qquad\qquad \forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)\ \text{(def)}$$

$\exists$-i $\qquad\qquad$ $\forall$-e

$$\exists y.\ x \cdot x = 2 \cdot y \qquad\qquad (\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)$$

$\Rightarrow$ -e

$$Even(x \cdot x)$$

$\Rightarrow$ -i (i)

$$Even(x) \Rightarrow Even(x \cdot x)$$

$\forall$-i

$$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$$

$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$ (de

∀-e

$Even(x)$ (i) $\quad$ $Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$

⇒ -e

$\exists y.\ x = 2 \cdot y$

∃-e

$x = 2 \cdot y$ $\quad$ $\forall x\ y\ z$

∀-e

$\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (ax) $\quad$ $x \cdot x = (2 \cdot y) \cdot (2 \cdot y)$ $\quad$ $x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2$

∀-e ×3 $\quad$ ⇒ -e

$(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y))$ $\quad$ $(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$

⇒ -e

$x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$ $\quad$ $\forall x.$

∃-i $\quad$ ∀-e

$\exists y.\ x \cdot x = 2 \cdot y$ $\quad$ $(\exists$

⇒ -e

$Even(x \cdot x)$

⇒ -i (i)

$Even(x) \Rightarrow Even(x \cdot x)$

∀-i

$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$

$$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \text{ (def)}$$

$$\forall\text{-e} \quad \frac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \text{ (def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}$$

$$\Rightarrow\text{-e} \quad \frac{Even(x) \text{ (i)} \qquad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}{\exists y.\ x = 2 \cdot y}$$

$$\exists\text{-e} \quad \frac{\exists y.\ x = 2 \cdot y}{x = 2 \cdot y}$$

$$\frac{x = 2 \cdot y}{x \cdot x = (2 \cdot y) \cdot (2 \cdot y)} \qquad ??\ \forall\text{-e} \quad \frac{\forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z \text{ (ax)}}{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot}$$

$$\Rightarrow\text{-e} \quad \frac{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \qquad x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot}{(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}$$

$$\Rightarrow\text{-e} \quad \frac{\pi \qquad (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}$$

$$\exists\text{-i} \quad \frac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y} \qquad \forall\text{-e} \quad \frac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x) \text{ (def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}$$

$$\Rightarrow\text{-e} \quad \frac{\exists y.\ x \cdot x = 2 \cdot y \qquad (\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}{Even(x \cdot x)}$$

$$\Rightarrow\text{-i} \quad \frac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)} \text{ (i)}$$

$$\forall\text{-i} \quad \frac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$\forall\text{-e}\ \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y \text{ (def)}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}$$

$$\Rightarrow\text{-e}\ \dfrac{Even(x) \text{ (i)} \qquad Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}{\exists y.\ x = 2 \cdot y}$$

$$\exists\text{-e}\ \dfrac{\exists y.\ x = 2 \cdot y}{x = 2 \cdot y}$$

$$\dfrac{x = 2 \cdot y}{\overline{x \cdot x = (2 \cdot y) \cdot (2 \cdot y)}}\ ??$$

$$\forall\text{-e}\ \dfrac{\forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z \text{ (ax)}}{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot}$$

$$\Rightarrow\text{-e}\ \dfrac{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \qquad x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot}{(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}$$

$$\Rightarrow\text{-e}\ \dfrac{\pi \qquad (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}$$

$$\exists\text{-i}\ \dfrac{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}{\exists y.\ x \cdot x = 2 \cdot y}$$

$$\forall\text{-e}\ \dfrac{\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x) \text{ (def)}}{(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}$$

$$\Rightarrow\text{-e}\ \dfrac{\exists y.\ x \cdot x = 2 \cdot y \qquad (\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)}{Even(x \cdot x)}$$

$$\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}$$

$$\forall\text{-i}\ \dfrac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

Deduction modulo

Computational part expressed as a rewrite system over term and propositions

Deduction modulo

Computational part expressed as a rewrite system over term and propositions

For instance

$$s(x) \cdot y \to x \cdot y + y$$
$$Even(x) \to \exists y.\ x = 2 \cdot y$$

Deduction modulo

Computational part expressed as a rewrite system over term and propositions
For instance

$$s(x) \cdot y \to x \cdot y + y$$
$$Even(x) \to \exists y.\ x = 2 \cdot y$$

Inferences performed modulo this congruence:

$$\exists\text{-e}\ \frac{A \qquad \begin{matrix}[B] \\ \\ C\end{matrix}}{C}\ A \overset{*}{\longleftrightarrow} \exists x.D \text{ and } B \overset{*}{\longleftrightarrow} \{y/x\}D$$

$Even(x)$ (i)

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$\exists\text{-e}\ \frac{Even(x)\ \text{(i)}}{\qquad\qquad}\ \text{(ii)} \qquad Even(x) \overset{*}{\longleftrightarrow} \exists y.\ x = 2 \cdot y$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$\exists\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad x = 2\cdot y\ \text{(ii)}}{\quad}\ \text{(ii)} \qquad Even(x) \xleftrightarrow{*} \exists y.\ x = 2\cdot y$$

$$\forall\text{-i}\ \dfrac{\Rightarrow\text{-i}\ \dfrac{Even(x\cdot x)}{Even(x) \Rightarrow Even(x\cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x\cdot x)}$$

$$\exists\text{-e}\ \dfrac{Even(x)\ \text{(i)} \qquad x = 2 \cdot y\ \text{(ii)}}{x \cdot x = 2 \cdot (2 \cdot y \cdot y)}\ \text{(ii)}$$

$$\Rightarrow\text{-i}\ \dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}$$

$$\forall\text{-i}\ \dfrac{Even(x) \Rightarrow Even(x \cdot x)}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}$$

$$Even(x) \overset{*}{\longleftrightarrow} \exists y.\ x = 2 \cdot y$$
$$x = 2 \cdot y \overset{*}{\longleftrightarrow} x \cdot x = 2 \cdot (2 \cdot y \cdot y)$$

$$
\forall\text{-i}\ \cfrac{\Rightarrow\text{-i}\ \cfrac{\exists\text{-i}\ \cfrac{\exists\text{-e}\ \cfrac{Even(x)\ \text{(i)} \qquad x = 2 \cdot y\ \text{(ii)}}{x \cdot x = 2 \cdot (2 \cdot y \cdot y)}\ \text{(ii)}}{Even(x \cdot x)}}{Even(x) \Rightarrow Even(x \cdot x)}\ \text{(i)}}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}
$$

$$Even(x) \xleftrightarrow{*} \exists y.\ x = 2 \cdot y$$

$$x = 2 \cdot y \xleftrightarrow{*} x \cdot x = 2 \cdot (2 \cdot y \cdot y)$$

$$Even(x \cdot x) \xleftrightarrow{*} \exists y.\ x \cdot x = 2 \cdot y$$

Theorem 1 (Buss (conjectured by Gödel)).

Let $i \geq 0$. Then there is an infinite family $\mathcal{F}$ of $\prod_1^0$-formulas such that

1. *for all $\varphi \in \mathcal{F}$, $Z_i \vdash \varphi$*
2. *there is a fixed $k \in \mathbb{N}$ such that for all $\varphi \in \mathcal{F}$, $Z_{i+1} \vdash_{\overline{k \text{ steps}}} \varphi$*
3. *there is no fixed $k \in \mathbb{N}$ such that for all $\varphi \in \mathcal{F}$, $Z_i \vdash_{\overline{k \text{ steps}}} \varphi$*

Questions

Same proof length speed-up in deduction modulo ?

Questions

Same proof length speed-up in deduction modulo ?

Speed-up in arithmetic : due to computation or to deduction ?

Outline

Reducing proof length in deduction modulo

Hide the computation part in the side conditions
$\Rightarrow$ proofs are smaller

Take $s(x) + y \to x + s(y)$.

$$\vdash_{\overline{\text{1 step}}} \underline{n} + \underline{n} = \underline{n+n} \text{ in deduction modulo}$$

$$\forall x\, y.\ s(x)+y = x+s(y) \vdash_{\overline{O(n) \text{ steps}}} \underline{n}+\underline{n} = \underline{n+n} \text{ in pure deduction}$$

$$\left(\underline{n} = \underbrace{s(s(\cdots(s}_{n \text{ times}}(0))))\right)$$

Outline

Schematic systems

Buss theorem is true if proofs are done in schematic systems

$\simeq$ Hilbert-type systems

$\simeq$ Frege systems

Metaformulæ

Definition 1 (Metaformulæ).

First-order signature $+$

- *metavariables* α^i *(substituted by variables)*
- *term variables* τ^i *(substituted by terms)*
- *formula variables* $A(x_1, \ldots, x_n)$ *(substituted by formulæ)*

Schematic System

Definition 2 (Schematic System).

Set of inference rules

$$\Phi_1, \ldots, \Phi_n / \Psi \quad (C)$$

with $\Phi_1, \ldots, \Phi_n, \Psi$ *metaformulæ and* C *side-condition of the form*
α^j *is not free in* Φ
τ^j *is freely substitutable for* α^j *in* Φ

A proof consists of a sequence of formulæ where each formula is derived from earlier formulæ by substituting an inference rule.

Schematic System for i^{th} Order Arithmetic

- Axiom schemata for classical logic with equality:
  $/A \Rightarrow B \Rightarrow A$, $/A \Rightarrow B \Rightarrow (A \wedge B)$, $/\tau^0 = \tau^0$,
  $/\forall \alpha^j.\ A(\alpha^j) \Rightarrow A(\tau^j)$ $\quad (\tau^j$ is freely substitutable for α^j in $A(\alpha^j))$
  etc.
- Inference rules for classical logic:
  Modus Ponens $A \Rightarrow B, A/B$,
  $A \Rightarrow B(\beta^j)/A \Rightarrow \forall \alpha^j.\ B(\alpha^j)$ $(\beta^j$ is not free in $A \Rightarrow \forall \alpha^j.\ B(\alpha^j))$
- Robinson axioms $/\forall \alpha^0.\ 0 + \alpha^0 = \alpha^0$,
  $/\forall \alpha^0 \beta^0.\ s(\alpha^0) + \beta^0 = s(\alpha^0 + \beta^0)$, etc.
- Induction for all formulæ of Z_i:
  $/A(0) \Rightarrow (\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))) \Rightarrow \forall \alpha^0.\ A(\alpha^0)$
- Comprehension schema:
  $/\exists \alpha^{j+1}.\ \forall \beta^j.\ \beta^j \in \alpha^{j+1} \Leftrightarrow A(\beta^j)$ $\quad ($provided α^{j+1} is not free in $A)$
  for $j < i$

Notations

$$Z_i \vdash^{\mathsf{S}}_{k} P :$$

P is provable in this schematic system in at most k steps

Notations

$$Z_i \vdash^{\mathsf{S}}_{k} P :$$

P is provable in this schematic system in at most k steps

$$Z_i \vdash^{\mathsf{N}}_{k} P :$$

P is provable in natural deduction using as assumptions Robinson axioms and a finite number of *instances* of Induction and Comprehension schemata (for i-th order arithmetic)

Notations

$$Z_i \vdash^{\mathsf{S}}_{k} P :$$

P is provable in this schematic system in at most k steps

$$Z_i \vdash^{\mathsf{N}}_{k} P :$$

P is provable in natural deduction using as assumptions Robinson axioms and a finite number of *instances* of Induction and Comprehension schemata (for i-th order arithmetic)

$$Z_i \vdash^{\mathsf{N}}_{k\,\mathcal{R}} P :$$

P is provable in natural deduction modulo $\mathcal{R}$ using as assumptions Robinson axioms and a finite number of instances of Induction and Comprehension schemata

From $Z_i \vdash^{\mathsf{S}}$ to $Z_i \vdash^{\mathsf{N}}$

classical logic	translated as in [Gentzen, 1934]
Robinson axioms	kept as assumption
Induction and comprehension schemata	*instances* kept as assumptions (finite number in a proof)

$$Z_i \vdash^{\mathsf{S}}_{k} P \rightsquigarrow Z_i \vdash^{\mathsf{N}}_{O(k)} P$$

From $Z_i \vdash^{\mathsf{N}}$ to $Z_i \vdash^{\mathsf{S}}$

Quite similar to the translation of a λ-term into a term of combinatory logic

For instance $\Rightarrow\text{-i}\ \dfrac{\begin{matrix}[Q]\\ P\end{matrix}}{Q \Rightarrow P} \quad \rightsquigarrow \quad MP\ \dfrac{P \qquad \overline{P \Rightarrow Q \Rightarrow P}}{Q \Rightarrow P}$ if Q is actually not used as assumption

$$Z_i \vdash^{\mathsf{N}}_{k} P \rightsquigarrow Z_i \vdash^{\mathsf{S}}_{O(3^k)} P$$

Simulating $i+1$-order using computations

Work of [Kirchner, 2006]:
Metaformula $A(x_1,\ldots,x_n)$ is replaced by a formula
$\langle x_1,\ldots,x_n\rangle \mathrel{\epsilon} \gamma$

γ: some term representing the formula substituted for A
For instance: $P = (x = 0 \vee \exists y.\ x \in^0 y) \quad \leadsto$

$$E_P^x \quad = \quad \langle x\rangle \mathrel{\epsilon} \ \dot{=}(1, S(0)) \ \cup \ \mathcal{P}^1\left(\dot{\in}^0(S(1),1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \rightarrow & t \\ 1^j[t ::^j l]^j & \rightarrow & t \\ S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\ s(n)[l]^0 & \rightarrow & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\ l \, \epsilon \, \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \, \epsilon \, \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \, \epsilon \, A \cup B & \rightarrow & l \, \epsilon \, A \vee l \, \epsilon \, B \\ l \, \epsilon \, A \cap B & \rightarrow & l \, \epsilon \, A \wedge l \, \epsilon \, B \\ l \, \epsilon \, A \supset B & \rightarrow & l \, \epsilon \, A \Rightarrow l \, \epsilon \, B \\ l \, \epsilon \, \emptyset & \rightarrow & \bot \\ l \, \epsilon \, \mathcal{P}^j(A) & \rightarrow & \exists x. \, x ::^j l \, \epsilon \, A \\ l \, \epsilon \, \mathcal{C}^j(A) & \rightarrow & \forall x. \, x ::^j l \, \epsilon \, A \end{array}$$

$$\langle t \rangle \, \epsilon \, E_P^x \quad = \quad \langle t \rangle \, \epsilon \, \doteq(1, S(0)) \cup \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \rightarrow & t \\ 1^j[t ::^j l]^j & \rightarrow & t \\ S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\ s(n)[l]^0 & \rightarrow & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\ l \;\epsilon\; \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \;\epsilon\; \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \;\epsilon\; A \cup B & \rightarrow & l \;\epsilon\; A \vee l \;\epsilon\; B \\ l \;\epsilon\; A \cap B & \rightarrow & l \;\epsilon\; A \wedge l \;\epsilon\; B \\ l \;\epsilon\; A \supset B & \rightarrow & l \;\epsilon\; A \Rightarrow l \;\epsilon\; B \\ l \;\epsilon\; \emptyset & \rightarrow & \bot \\ l \;\epsilon\; \mathcal{P}^j(A) & \rightarrow & \exists x.\; x ::^j l \;\epsilon\; A \\ l \;\epsilon\; \mathcal{C}^j(A) & \rightarrow & \forall x.\; x ::^j l \;\epsilon\; A \end{array}$$

$$\langle t \rangle \;\epsilon\; E_P^x \quad = \quad \langle t \rangle \;\epsilon\; \dot{=}(1, S(0)) \cup \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \rightarrow & t \\ 1^j[t ::^j l]^j & \rightarrow & t \\ S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\ s(n)[l]^0 & \rightarrow & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\ l \mathrel{\epsilon} \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \mathrel{\epsilon} \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \mathrel{\epsilon} A \cup B & \rightarrow & l \mathrel{\epsilon} A \vee l \mathrel{\epsilon} B \\ l \mathrel{\epsilon} A \cap B & \rightarrow & l \mathrel{\epsilon} A \wedge l \mathrel{\epsilon} B \\ l \mathrel{\epsilon} A \supset B & \rightarrow & l \mathrel{\epsilon} A \Rightarrow l \mathrel{\epsilon} B \\ l \mathrel{\epsilon} \emptyset & \rightarrow & \bot \\ l \mathrel{\epsilon} \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \mathrel{\epsilon} A \\ l \mathrel{\epsilon} \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \mathrel{\epsilon} A \end{array}$$

$$\langle t \rangle \mathrel{\epsilon} E_P^x \xrightarrow{*} \langle t \rangle \mathrel{\epsilon} \doteq(1, S(0)) \vee \langle t \rangle \mathrel{\epsilon} \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \ \epsilon \ \doteq (t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
\qquad
\begin{array}{rcl}
l \ \epsilon \ \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \ \epsilon \ A \cup B & \rightarrow & l \ \epsilon \ A \vee l \ \epsilon \ B \\
l \ \epsilon \ A \cap B & \rightarrow & l \ \epsilon \ A \wedge l \ \epsilon \ B \\
l \ \epsilon \ A \supset B & \rightarrow & l \ \epsilon \ A \Rightarrow l \ \epsilon \ B \\
l \ \epsilon \ \emptyset & \rightarrow & \bot \\
l \ \epsilon \ \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \ \epsilon \ A \\
l \ \epsilon \ \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \ \epsilon \ A
\end{array}
$$

$$
\langle t \rangle \ \epsilon \ E_P^x \xrightarrow{*} \langle t \rangle \ \epsilon \ \doteq (1, S(0)) \vee \langle t \rangle \ \epsilon \ \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)
$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \in \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \in \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \in A \cup B & \rightarrow & l \in A \vee l \in B \\
l \in A \cap B & \rightarrow & l \in A \wedge l \in B \\
l \in A \supset B & \rightarrow & l \in A \Rightarrow l \in B \\
l \in \emptyset & \rightarrow & \bot \\
l \in \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \in A \\
l \in \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \in A
\end{array}
$$

$$\langle t \rangle \in E_P^x \xrightarrow{*} 1[t] = S(0)[t] \vee \langle t \rangle \in \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \in \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \in \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \in A \cup B & \rightarrow & l \in A \vee l \in B \\
l \in A \cap B & \rightarrow & l \in A \wedge l \in B \\
l \in A \supset B & \rightarrow & l \in A \Rightarrow l \in B \\
l \in \emptyset & \rightarrow & \bot \\
l \in \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \in A \\
l \in \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \in A
\end{array}
$$

$$
\langle t \rangle \in E_P^x \xrightarrow{*} 1[t] = S(0)[t] \vee \langle t \rangle \in \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)
$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \,\epsilon\, \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \,\epsilon\, \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \,\epsilon\, A \cup B & \rightarrow & l \,\epsilon\, A \vee l \,\epsilon\, B \\
l \,\epsilon\, A \cap B & \rightarrow & l \,\epsilon\, A \wedge l \,\epsilon\, B \\
l \,\epsilon\, A \supset B & \rightarrow & l \,\epsilon\, A \Rightarrow l \,\epsilon\, B \\
l \,\epsilon\, \emptyset & \rightarrow & \bot \\
l \,\epsilon\, \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \,\epsilon\, A \\
l \,\epsilon\, \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \,\epsilon\, A
\end{array}
$$

$$
\langle t \rangle \,\epsilon\, E_P^x \xrightarrow{*} t = S(0)[t] \ \vee\ \langle t \rangle \,\epsilon\, \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)
$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \to & t \\ 1^j[t ::^j l]^j & \to & t \\ S^j(n)[t ::^j l]^j & \to & n[l]^j \\ s(n)[l]^0 & \to & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \to & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \to & t_1[l]^0 \times t_2[l]^0 \\ l \,\epsilon\, \doteq(t_1, t_2) & \to & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \,\epsilon\, \dot{\in}^j(t_1, t_2) & \to & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \,\epsilon\, A \cup B & \to & l \,\epsilon\, A \vee l \,\epsilon\, B \\ l \,\epsilon\, A \cap B & \to & l \,\epsilon\, A \wedge l \,\epsilon\, B \\ l \,\epsilon\, A \supset B & \to & l \,\epsilon\, A \Rightarrow l \,\epsilon\, B \\ l \,\epsilon\, \emptyset & \to & \bot \\ l \,\epsilon\, \mathcal{P}^j(A) & \to & \exists x.\ x ::^j l \,\epsilon\, A \\ l \,\epsilon\, \mathcal{C}^j(A) & \to & \forall x.\ x ::^j l \,\epsilon\, A \end{array}$$

$$\langle t \rangle \,\epsilon\, E_P^x \xrightarrow{*} t = S(0)[t] \ \vee\ \langle t \rangle \,\epsilon\, \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \in \doteq (t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \in \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \in A \cup B & \rightarrow & l \in A \vee l \in B \\
l \in A \cap B & \rightarrow & l \in A \wedge l \in B \\
l \in A \supset B & \rightarrow & l \in A \Rightarrow l \in B \\
l \in \emptyset & \rightarrow & \bot \\
l \in \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \in A \\
l \in \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \in A
\end{array}
$$

$$\langle t \rangle \in E_P^x \xrightarrow{*} t = 0[nil] \ \vee \ \langle t \rangle \in \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \,\epsilon\, \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
\qquad
\begin{array}{rcl}
l \,\epsilon\, \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \,\epsilon\, A \cup B & \rightarrow & l \,\epsilon\, A \vee l \,\epsilon\, B \\
l \,\epsilon\, A \cap B & \rightarrow & l \,\epsilon\, A \wedge l \,\epsilon\, B \\
l \,\epsilon\, A \supset B & \rightarrow & l \,\epsilon\, A \Rightarrow l \,\epsilon\, B \\
l \,\epsilon\, \emptyset & \rightarrow & \bot \\
l \,\epsilon\, \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \,\epsilon\, A \\
l \,\epsilon\, \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \,\epsilon\, A
\end{array}
$$

$$\langle t \rangle \,\epsilon\, E_P^x \xrightarrow{*} t = 0[nil] \;\vee\; \langle t \rangle \,\epsilon\, \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \mathrel{\epsilon} \doteq(t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}$$

$$\begin{aligned}
l \mathrel{\epsilon} \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \mathrel{\epsilon} A \cup B &\rightarrow l \mathrel{\epsilon} A \vee l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} A \cap B &\rightarrow l \mathrel{\epsilon} A \wedge l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} A \supset B &\rightarrow l \mathrel{\epsilon} A \Rightarrow l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} \emptyset &\rightarrow \bot \\
l \mathrel{\epsilon} \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \mathrel{\epsilon} A \\
l \mathrel{\epsilon} \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \mathrel{\epsilon} A
\end{aligned}$$

$$\langle t \rangle \mathrel{\epsilon} E_P^x \xrightarrow{*} t = 0 \ \vee\ \langle t \rangle \mathrel{\epsilon} \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \in \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \in \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \in A \cup B & \rightarrow & l \in A \vee l \in B \\
l \in A \cap B & \rightarrow & l \in A \wedge l \in B \\
l \in A \supset B & \rightarrow & l \in A \Rightarrow l \in B \\
l \in \emptyset & \rightarrow & \bot \\
l \in \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \in A \\
l \in \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \in A
\end{array}
$$

$$\langle t \rangle \in E_P^x \xrightarrow{*} t = 0 \ \vee\ \langle t \rangle \in \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \,\epsilon\, \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \,\epsilon\, \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \,\epsilon\, A \cup B & \rightarrow & l \,\epsilon\, A \vee l \,\epsilon\, B \\
l \,\epsilon\, A \cap B & \rightarrow & l \,\epsilon\, A \wedge l \,\epsilon\, B \\
l \,\epsilon\, A \supset B & \rightarrow & l \,\epsilon\, A \Rightarrow l \,\epsilon\, B \\
l \,\epsilon\, \emptyset & \rightarrow & \bot \\
l \,\epsilon\, \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \,\epsilon\, A \\
l \,\epsilon\, \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \,\epsilon\, A
\end{array}
$$

$$\langle t \rangle \,\epsilon\, E_P^x \xrightarrow{*} t = 0 \ \vee\ \exists y.\ \langle y ::^1 t \rangle \,\epsilon\, \dot{\in}^0(S(1), 1)$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \rightarrow & t \\ 1^j[t ::^j l]^j & \rightarrow & t \\ S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\ s(n)[l]^0 & \rightarrow & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\ l \ \epsilon \ \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \ \epsilon \ \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \ \epsilon \ A \cup B & \rightarrow & l \ \epsilon \ A \vee l \ \epsilon \ B \\ l \ \epsilon \ A \cap B & \rightarrow & l \ \epsilon \ A \wedge l \ \epsilon \ B \\ l \ \epsilon \ A \supset B & \rightarrow & l \ \epsilon \ A \Rightarrow l \ \epsilon \ B \\ l \ \epsilon \ \emptyset & \rightarrow & \bot \\ l \ \epsilon \ \mathcal{P}^j(A) & \rightarrow & \exists x. \ x ::^j l \ \epsilon \ A \\ l \ \epsilon \ \mathcal{C}^j(A) & \rightarrow & \forall x. \ x ::^j l \ \epsilon \ A \end{array}$$

$$\langle t \rangle \ \epsilon \ E_P^x \xrightarrow{*} t = 0 \ \vee \ \exists y. \ \langle y ::^1 t \rangle \ \epsilon \ \dot{\in}^0(S(1), 1)$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \ \epsilon \ \doteq(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \ \epsilon \ \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \ \epsilon \ A \cup B & \rightarrow & l \ \epsilon \ A \vee l \ \epsilon \ B \\
l \ \epsilon \ A \cap B & \rightarrow & l \ \epsilon \ A \wedge l \ \epsilon \ B \\
l \ \epsilon \ A \supset B & \rightarrow & l \ \epsilon \ A \Rightarrow l \ \epsilon \ B \\
l \ \epsilon \ \emptyset & \rightarrow & \bot \\
l \ \epsilon \ \mathcal{P}^j(A) & \rightarrow & \exists x.\ x ::^j l \ \epsilon \ A \\
l \ \epsilon \ \mathcal{C}^j(A) & \rightarrow & \forall x.\ x ::^j l \ \epsilon \ A
\end{array}
$$

$$\langle t \rangle \ \epsilon \ E_P^x \xrightarrow{*} t = 0 \ \vee \ \exists y.\ S(1)[y :: t] \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \in \doteq (t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}
$$

$$
\begin{aligned}
l \in \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \in A \cup B &\rightarrow l \in A \vee l \in B \\
l \in A \cap B &\rightarrow l \in A \wedge l \in B \\
l \in A \supset B &\rightarrow l \in A \Rightarrow l \in B \\
l \in \emptyset &\rightarrow \bot \\
l \in \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \in A \\
l \in \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \in A
\end{aligned}
$$

$$\langle t \rangle \in E_P^x \xrightarrow{*} t = 0 \ \vee\ \exists y.\ S(1)[y :: t] \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{array}{rcl} t[nil]^j & \rightarrow & t \\ 1^j[t ::^j l]^j & \rightarrow & t \\ S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\ s(n)[l]^0 & \rightarrow & s(n[l]^0) \\ (t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\ (t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\ l \;\epsilon\; \doteq (t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0 \end{array}$$

$$\begin{array}{rcl} l \;\epsilon\; \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\ l \;\epsilon\; A \cup B & \rightarrow & l \;\epsilon\; A \vee l \;\epsilon\; B \\ l \;\epsilon\; A \cap B & \rightarrow & l \;\epsilon\; A \wedge l \;\epsilon\; B \\ l \;\epsilon\; A \supset B & \rightarrow & l \;\epsilon\; A \Rightarrow l \;\epsilon\; B \\ l \;\epsilon\; \emptyset & \rightarrow & \bot \\ l \;\epsilon\; \mathcal{P}^j(A) & \rightarrow & \exists x.\; x ::^j l \;\epsilon\; A \\ l \;\epsilon\; \mathcal{C}^j(A) & \rightarrow & \forall x.\; x ::^j l \;\epsilon\; A \end{array}$$

$$\langle t \rangle \;\epsilon\; E_P^x \xrightarrow{*} t = 0 \;\vee\; \exists y.\; 1[t] \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \mathrel{\epsilon} \doteq (t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}
$$

$$
\begin{aligned}
l \mathrel{\epsilon} \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \mathrel{\epsilon} A \cup B &\rightarrow l \mathrel{\epsilon} A \vee l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} A \cap B &\rightarrow l \mathrel{\epsilon} A \wedge l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} A \supset B &\rightarrow l \mathrel{\epsilon} A \Rightarrow l \mathrel{\epsilon} B \\
l \mathrel{\epsilon} \emptyset &\rightarrow \bot \\
l \mathrel{\epsilon} \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \mathrel{\epsilon} A \\
l \mathrel{\epsilon} \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \mathrel{\epsilon} A
\end{aligned}
$$

$$\langle t \rangle \mathrel{\epsilon} E_P^x \xrightarrow{*} t = 0 \ \vee \ \exists y.\ 1[t] \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \,\epsilon\, \doteq(t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}
$$

$$
\begin{aligned}
l \,\epsilon\, \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \,\epsilon\, A \cup B &\rightarrow l \,\epsilon\, A \vee l \,\epsilon\, B \\
l \,\epsilon\, A \cap B &\rightarrow l \,\epsilon\, A \wedge l \,\epsilon\, B \\
l \,\epsilon\, A \supset B &\rightarrow l \,\epsilon\, A \Rightarrow l \,\epsilon\, B \\
l \,\epsilon\, \emptyset &\rightarrow \bot \\
l \,\epsilon\, \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \,\epsilon\, A \\
l \,\epsilon\, \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \,\epsilon\, A
\end{aligned}
$$

$$\langle t \rangle \,\epsilon\, E_P^x \xrightarrow{*} t = 0 \;\vee\; \exists y.\ t \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \ \epsilon \ \dot{=}(t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}$$

$$\begin{aligned}
l \ \epsilon \ \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \ \epsilon \ A \cup B &\rightarrow l \ \epsilon \ A \vee l \ \epsilon \ B \\
l \ \epsilon \ A \cap B &\rightarrow l \ \epsilon \ A \wedge l \ \epsilon \ B \\
l \ \epsilon \ A \supset B &\rightarrow l \ \epsilon \ A \Rightarrow l \ \epsilon \ B \\
l \ \epsilon \ \emptyset &\rightarrow \bot \\
l \ \epsilon \ \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \ \epsilon \ A \\
l \ \epsilon \ \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \ \epsilon \ A
\end{aligned}$$

$$\langle t \rangle \ \epsilon \ E_P^x \xrightarrow{*} t = 0 \ \vee \ \exists y.\ t \in 1[y :: t]$$

Rewriting classes

Terminating and confluent rewrite system:

$$
\begin{array}{rcl}
t[nil]^j & \rightarrow & t \\
1^j[t ::^j l]^j & \rightarrow & t \\
S^j(n)[t ::^j l]^j & \rightarrow & n[l]^j \\
s(n)[l]^0 & \rightarrow & s(n[l]^0) \\
(t_1 + t_2)[l]^0 & \rightarrow & t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 & \rightarrow & t_1[l]^0 \times t_2[l]^0 \\
l \;\epsilon\; \dot{=}(t_1, t_2) & \rightarrow & t_1[l]^0 = t_2[l]^0
\end{array}
$$

$$
\begin{array}{rcl}
l \;\epsilon\; \dot{\in}^j(t_1, t_2) & \rightarrow & t_1[l]^j \in^j t_2[l]^{j+1} \\
l \;\epsilon\; A \cup B & \rightarrow & l \;\epsilon\; A \vee l \;\epsilon\; B \\
l \;\epsilon\; A \cap B & \rightarrow & l \;\epsilon\; A \wedge l \;\epsilon\; B \\
l \;\epsilon\; A \supset B & \rightarrow & l \;\epsilon\; A \Rightarrow l \;\epsilon\; B \\
l \;\epsilon\; \emptyset & \rightarrow & \bot \\
l \;\epsilon\; \mathcal{P}^j(A) & \rightarrow & \exists x.\; x ::^j l \;\epsilon\; A \\
l \;\epsilon\; \mathcal{C}^j(A) & \rightarrow & \forall x.\; x ::^j l \;\epsilon\; A
\end{array}
$$

$$\langle t \rangle \;\epsilon\; E_P^x \xrightarrow{*} t = 0 \;\vee\; \exists y.\; t \in y$$

Rewriting classes

Terminating and confluent rewrite system:

$$\begin{aligned}
t[nil]^j &\rightarrow t \\
1^j[t ::^j l]^j &\rightarrow t \\
S^j(n)[t ::^j l]^j &\rightarrow n[l]^j \\
s(n)[l]^0 &\rightarrow s(n[l]^0) \\
(t_1 + t_2)[l]^0 &\rightarrow t_1[l]^0 + t_2[l]^0 \\
(t_1 \times t_2)[l]^0 &\rightarrow t_1[l]^0 \times t_2[l]^0 \\
l \ \epsilon \ \dot{=}(t_1, t_2) &\rightarrow t_1[l]^0 = t_2[l]^0
\end{aligned}$$

$$\begin{aligned}
l \ \epsilon \ \dot{\in}^j(t_1, t_2) &\rightarrow t_1[l]^j \in^j t_2[l]^{j+1} \\
l \ \epsilon \ A \cup B &\rightarrow l \ \epsilon \ A \vee l \ \epsilon \ B \\
l \ \epsilon \ A \cap B &\rightarrow l \ \epsilon \ A \wedge l \ \epsilon \ B \\
l \ \epsilon \ A \supset B &\rightarrow l \ \epsilon \ A \Rightarrow l \ \epsilon \ B \\
l \ \epsilon \ \emptyset &\rightarrow \bot \\
l \ \epsilon \ \mathcal{P}^j(A) &\rightarrow \exists x.\ x ::^j l \ \epsilon \ A \\
l \ \epsilon \ \mathcal{C}^j(A) &\rightarrow \forall x.\ x ::^j l \ \epsilon \ A
\end{aligned}$$

$$\langle t \rangle \ \epsilon \ E_P^x \xrightarrow{*} t = 0 \ \vee \ \exists y.\ t \in y \quad = \quad \{t/x\}P$$

From axiom schemata to axioms

$$A(0) \Rightarrow \big(\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))\big) \Rightarrow \forall \alpha^0.\ A(\alpha^0)$$

becomes

$$\forall\text{-e}\ \frac{\forall \gamma^c . \langle 0 \rangle \mathrel{\epsilon} \gamma^c \Rightarrow \big(\forall \beta^0.\ \langle \beta^0 \rangle \mathrel{\epsilon} \gamma^c \Rightarrow \langle s(\beta^0) \rangle \mathrel{\epsilon} \gamma^c\big) \Rightarrow \forall \alpha^0.\ \langle \alpha^0 \rangle \mathrel{\epsilon} \gamma^c \ \text{(IA)}}{A(0) \Rightarrow \big(\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))\big) \Rightarrow \forall \alpha^0.\ A(\alpha^0)}$$

(for all t, $\langle t \rangle \mathrel{\epsilon} E_A^x \xrightarrow{*} A(t)$)

From axiom schemata to axioms

$$A(0) \Rightarrow \left(\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))\right) \Rightarrow \forall \alpha^0.\ A(\alpha^0)$$

becomes

$$\forall\text{-e}\ \frac{\forall \gamma^c. \langle 0 \rangle \in \gamma^c \Rightarrow \left(\forall \beta^0.\ \langle \beta^0 \rangle \in \gamma^c \Rightarrow \langle s(\beta^0) \rangle \in \gamma^c\right) \Rightarrow \forall \alpha^0.\ \langle \alpha^0 \rangle \in \gamma^c \ (\mathsf{IA})}{A(0) \Rightarrow \left(\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))\right) \Rightarrow \forall \alpha^0.\ A(\alpha^0)}$$

$$\left(\text{for all } t,\ \langle t \rangle \in E_A^x \xrightarrow{*} A(t)\right)$$

New axioms IA and CA.

From $Z_{i+1} \vdash^{\mathsf{S}}$ to $Z_i \vdash^{\mathsf{N}}_{\mathcal{R}_i}$

Instance of axiom schemata for $i+1$-th order arithmetic can be simulated by axioms, using the modulo.

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P \rightsquigarrow Z_i, IA, CA \vdash^{\mathsf{N}}_{O(k)}{}_{\mathcal{R}_i} P$$

Outline

- Motivations
- Speed-up in deduction modulo
- Technical details
  - Schematic systems
  - Translations
- **Speed-up in arithmetic and computation**
- Conclusion

Adding computation creates a speed-up

Theorem 2.
For all $i \geq 0$, there is a rewrite system $\mathcal{R}_i$ such that there is an infinite family $\mathcal{F}$ such that

1. *for all $P \in \mathcal{F}$, $Z_i \vdash^{\mathsf{N}} P$*
2. *there is a fixed $k \in \mathbb{N}$ such that for all $P \in \mathcal{F}$, $Z_i \vdash^{\mathsf{N}}_{k \text{ steps}}{}_{\mathcal{R}_i} P$*
3. *there is no fixed $k \in \mathbb{N}$ such that for all $P \in \mathcal{F}$, $Z_i \vdash^{\mathsf{N}}_{k \text{ steps}} P$*

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P$$

Theo. 1 $\updownarrow$

$$Z_i \vdash^{\mathsf{S}}_{} P$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P \quad \rightsquigarrow \quad Z_i, \Gamma \vdash^{\mathsf{N}}_{K\, \mathcal{R}_i} P$$

Theo. 1 $\updownarrow$

$$Z_i \vdash^{\mathsf{S}} P$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P \quad \leadsto \quad Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P \quad \leadsto \quad Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P'$$

Theo. 1 $\updownarrow$

$$Z_i \vdash^{\mathsf{S}} P$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}} P & \leadsto & Z_i \vdash^{\mathsf{N}} P & &
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash_{k}^{\mathsf{S}} P & \leadsto & Z_i, \Gamma \vdash_{K}^{\mathsf{N}}{}_{\mathcal{R}_i} P & \leadsto & Z_i \vdash_{K+2}^{\mathsf{N}}{}_{\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}} P & &
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \rightsquigarrow & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P & \rightsquigarrow & Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}} P & \rightsquigarrow & Z_i, \Gamma \vdash^{\mathsf{N}} P & \rightsquigarrow & Z_i \vdash^{\mathsf{N}} P'
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{k} P'
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}}_{} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}}_{k+2} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{k} P'
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$
\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \rightsquigarrow & Z_i, \Gamma \vdash^{\mathsf{N}}_{K}{}_{\mathcal{R}_i} P & \rightsquigarrow & Z_i \vdash^{\mathsf{N}}_{K+2}{}_{\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}}_{3^{k+2}} P & \overset{\rightsquigarrow}{\leftsquigarrow} & Z_i, \Gamma \vdash^{\mathsf{N}}_{k+2} P & \rightsquigarrow & Z_i \vdash^{\mathsf{N}}_{k} P'
\end{array}
$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$\begin{array}{ccccc}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P & \leadsto & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{K+2\,\mathcal{R}_i} P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \vdash^{\mathsf{S}}_{\not{3}^{k+2}} P & \begin{array}{c}\leadsto \\ \leftsquigarrow\end{array} & Z_i, \Gamma \vdash^{\mathsf{N}}_{k+2} P & \leadsto & Z_i \vdash^{\mathsf{N}}_{k} P'
\end{array}$$

□

Proof.

$\Gamma = IA, CA$

$P' = IA \Rightarrow CA \Rightarrow P$

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P \quad \leadsto \quad Z_i, \Gamma \vdash^{\mathsf{N}}_{K\ \mathcal{R}_i} P \quad \leadsto \quad Z_i \vdash^{\mathsf{N}}_{K+2\ \mathcal{R}_i} P'$$

Theo. 1 $\updownarrow$

$$Z_i \vdash^{\mathsf{S}}_{\not{3}^{\not{k}+\not{2}}} P \quad \begin{matrix}\leadsto \\ \leftsquigarrow\end{matrix} \quad Z_i, \Gamma \vdash^{\mathsf{N}}_{\not{k}\not{+}\not{2}} P \quad \leadsto \quad Z_i \vdash^{\mathsf{N}}_{\not{k}} P'$$

□

Linear simulation of Z_{i+1} in Z_i modulo

Theorem 3.
For all $i \geq 0$, there exists a (finite) rewrite system $\mathcal{R}_i$ and a finite set of axioms Γ such that for all formulæ P, if $Z_{i+1} \vdash_k^{\mathsf{N}} P$ then $Z_i, \Gamma \vdash_{O(k)}^{\mathsf{N}}{}_{\mathcal{R}_i} P$.

Linear simulation of Z_{i+1} in Z_i modulo

Theorem 3.
For all $i \geq 0$, there exists a (finite) rewrite system $\mathcal{R}_i$ and a finite set of axioms Γ such that for all formulæ P, if $Z_{i+1} \vdash_k^{\mathsf{N}} P$ then $Z_i, \Gamma \vdash_{O(k)}^{\mathsf{N}}{}_{\mathcal{R}_i} P$.

Proof.
$\mathcal{R}_i$ defined as before
$\Gamma = IA, CA$
Replace the instances of axiom schemata by the axioms with classes. □

Outline

- Motivations
- Speed-up in deduction modulo
- Technical details
  - Schematic systems
  - Translations
- Speed-up in arithmetic and computation
- Conclusion

Difference between $i+1$-th and i-th order arithmetic : expressed as a confluent and terminating rewrite system

The length of the deduction part of the proofs remains the same

Difference between $i+1$-th and i-th order arithmetic : expressed as a confluent and terminating rewrite system
The length of the deduction part of the proofs remains the same

Next step: difference between higher order logic and first order logic modulo

HOL	simulated by	HOL-$\lambda\sigma$	[Dowek et al., 2001]
every PTS	"	$\lambda\Pi$ modulo	[Cousineau and Dowek, 2006]

Cousineau, D. and Dowek, G. (2006).
Embedding pure type systems in the lambda-pi-calculus modulo.

Dowek, G., Hardin, T., and Kirchner, C. (2001).
HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic.
Mathematical Structures in Computer Science, 11(1):1–25.

Gentzen, G. (1934).
Untersuchungen über das logische Schliessen.
Mathematische Zeitschrift, 39:176–210, 405–431.
Translated in Szabo, editor., *The Collected Papers of Gerhard Gentzen* as "Investigations into Logical Deduction".

Kirchner, F. (2006).
A finite first-order theory of classes.

Available at `http://www.lix.polytechnique.fr/Labo/Florent.Kirchner/doc/fotc2006.pdf`.