Université Henri Poincaré – LORIA (INRIA)

Unbounded Proof-Length Speed-up in Deduction Modulo

16th EACSL Annual Conference on Computer Science and Logic

Guillaume Burel

September 14$^{\text{th}}$, 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)

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

$Even(x)$ (i)

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

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

$Even(x)$ (i)

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

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

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

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

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

$Even(x)$ (i)

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

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

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

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

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

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

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

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

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

$$
\begin{prooftree}
\AxiomC{$Even(x)$ (i)}
\AxiomC{$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$ (def)}
\LeftLabel{$\forall$-e}
\UnaryInfC{$Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$}
\LeftLabel{$\Rightarrow$-e}
\BinaryInfC{$\exists y.\ x = 2 \cdot y$}
\LeftLabel{$\exists$-e}
\UnaryInfC{$x = 2 \cdot y$}
\doubleLine
\RightLabel{??}
\UnaryInfC{$x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$}
\LeftLabel{$\exists$-i}
\UnaryInfC{$\exists y.\ x \cdot x = 2 \cdot y$}
\AxiomC{$\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)$ (def)}
\LeftLabel{$\forall$-e}
\UnaryInfC{$(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)$}
\LeftLabel{$\Rightarrow$-e}
\BinaryInfC{$Even(x \cdot x)$}
\LeftLabel{$\Rightarrow$-i}
\RightLabel{(i)}
\UnaryInfC{$Even(x) \Rightarrow Even(x \cdot x)$}
\LeftLabel{$\forall$-i}
\UnaryInfC{$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$}
\end{prooftree}
$$

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

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

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

$$\forall\text{-e}$$

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

$$\Rightarrow\text{-e}$$

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

$$\exists\text{-e}$$

$$x = 2 \cdot y$$

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

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

$$\exists\text{-i} \qquad \forall\text{-e}$$

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

$$\Rightarrow\text{-e}$$

$$Even(x \cdot x)$$

$$\Rightarrow\text{-i} \quad \text{(i)}$$

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

$$\forall\text{-i}$$

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

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

$$\forall\text{-e}\ \dfrac{}{}$$

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

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

$$\forall\text{-e}\ \dfrac{\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)\ \text{(ax)}}{(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y))} \times 3$$

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

$$\forall x.$$

$$\forall\text{-e}\ \dfrac{}{(\exists}$$

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

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

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

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

π

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

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

π

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

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

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

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

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

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

$$\pi$$

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

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

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)\ (\mathrm{ax})}{(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y))}\ \forall\text{-e}\ \times 3 \quad \dfrac{\dfrac{\dfrac{Even(x)\ (\mathrm{i}) \quad \dfrac{\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y\ (\mathrm{de}}{Even(x) \Rightarrow \exists y.\ x = 2 \cdot y}\ \forall\text{-e}}{\exists y.\ x = 2 \cdot y}\ \Rightarrow\text{-e}}{x = 2 \cdot y}\ \exists\text{-e} \quad \dfrac{\forall x\ y\ z}{x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2}\ \forall\text{-e}}{(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}\ \Rightarrow\text{-e}}{x \cdot x = 2 \cdot (y \cdot (2 \cdot y))}\ \Rightarrow\text{-e}}{\exists y.\ x \cdot x = 2 \cdot y}\ \exists\text{-i} \quad \dfrac{\forall x.}{(\exists}\ \forall\text{-e}}{\dfrac{\dfrac{Even(x \cdot x)}{Even(x) \Rightarrow Even(x \cdot x)}\ \Rightarrow\text{-i}\ (\mathrm{i})}{\forall x.\ Even(x) \Rightarrow Even(x \cdot x)}\ \forall\text{-i}}\ \Rightarrow\text{-e}$$

$$
\begin{prooftree}
\AxiomC{π}
\AxiomC{$Even(x)$ (i)}
\AxiomC{$\forall x.\ Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$ (def)}
\LeftLabel{$\forall$-e}
\UnaryInfC{$Even(x) \Rightarrow \exists y.\ x = 2 \cdot y$}
\LeftLabel{$\Rightarrow$ -e}
\BinaryInfC{$\exists y.\ x = 2 \cdot y$}
\LeftLabel{$\exists$-e}
\UnaryInfC{$x = 2 \cdot y$}
\doubleLine
\RightLabel{??}
\UnaryInfC{$x \cdot x = (2 \cdot y) \cdot (2 \cdot y)$}
\AxiomC{$\forall x\ y\ z.\ x = y \Rightarrow y = z \Rightarrow x = z$ (ax)}
\LeftLabel{$\forall$-e}
\UnaryInfC{$x \cdot x = (2 \cdot y) \cdot (2 \cdot y) \Rightarrow (2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot$}
\LeftLabel{$\Rightarrow$ -e}
\BinaryInfC{$(2 \cdot y) \cdot (2 \cdot y) = 2 \cdot (y \cdot (2 \cdot y)) \Rightarrow x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$}
\LeftLabel{$\Rightarrow$ -e}
\BinaryInfC{$x \cdot x = 2 \cdot (y \cdot (2 \cdot y))$}
\LeftLabel{$\exists$-i}
\UnaryInfC{$\exists y.\ x \cdot x = 2 \cdot y$}
\AxiomC{$\forall x.\ (\exists y.\ x = 2 \cdot y) \Rightarrow Even(x)$ (def)}
\LeftLabel{$\forall$-e}
\UnaryInfC{$(\exists y.\ x \cdot x = 2 \cdot y) \Rightarrow Even(x \cdot x)$}
\LeftLabel{$\Rightarrow$ -e}
\BinaryInfC{$Even(x \cdot x)$}
\LeftLabel{$\Rightarrow$ -i}
\RightLabel{(i)}
\UnaryInfC{$Even(x) \Rightarrow Even(x \cdot x)$}
\LeftLabel{$\forall$-i}
\UnaryInfC{$\forall x.\ Even(x) \Rightarrow Even(x \cdot x)$}
\end{prooftree}
$$

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

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

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

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

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

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

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

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

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

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

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

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

Deduction modulo [Dowek et al., 2003]

Computational part expressed as a rewrite system over terms and propositions

Deduction modulo [Dowek et al., 2003]

Computational part expressed as a rewrite system over terms and propositions

For instance

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

Deduction modulo [Dowek et al., 2003]

Computational part expressed as a rewrite system over terms and propositions

For instance

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

Inferences performed modulo this congruence:

$$\exists\text{-e}\ \frac{A \qquad \begin{array}{c}[B] \\ \vdots \\ C\end{array}}{C}\ A \xleftrightarrow{*} \exists x.D \text{ and } B \xleftrightarrow{*} \{y/x\}D$$

$Even(x)$ (i)

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

Motivations

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

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

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

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

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

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

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

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

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

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

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

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

Arithmetic

First-order arithmetic:

0, s, $+$, $\cdot$, induction principle

$$P(0) \Rightarrow (\forall x.\ P(x) \Rightarrow P(s(x))) \Rightarrow \forall x.\ P(x)$$

Arithmetic

First-order arithmetic:
0, s, $+$, $\cdot$, induction principle

$$P(0) \Rightarrow (\forall x.\ P(x) \Rightarrow P(s(x))) \Rightarrow \forall x.\ P(x)$$

Second-order arithmetic:
sets of natural numbers, $\in$, comprehension schema:

$$\exists S.\ \forall n.\ n \in S \Leftrightarrow P(n)$$

Arithmetic

First-order arithmetic:
0, s, $+$, $\cdot$, induction principle

$$P(0) \Rightarrow (\forall x.\ P(x) \Rightarrow P(s(x))) \Rightarrow \forall x.\ P(x)$$

Second-order arithmetic:
sets of natural numbers, $\in$, comprehension schema:

$$\exists S.\ \forall n.\ n \in S \Leftrightarrow P(n)$$

Possibility to prove stronger principles (e.g. transfinite induction up to ϵ_0)

Theorem 1 (Buss (conjectured by Gödel)).

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

- Motivations
  - Deduction modulo
  - Proof length in arithmetic
- **Speed-up in deduction modulo**
- Speed-ups in arithmetic and computation
  - Schematic systems
  - Translations
  - Speed-up
- Conclusion

Reducing proof length in deduction modulo

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

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

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

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

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

Computational vs. deductive complexity

Do not suppress the complexity of the proofs, but separate it between deduction and computation.

Computational vs. deductive complexity

Do not suppress the complexity of the proofs, but separate it between deduction and computation.

$$\begin{array}{ccc} \text{computation} & \text{vs.} & \text{deduction} \\ \simeq & & \simeq \\ \text{verification} & \text{vs.} & \text{inference} \end{array}$$

Not acceptable: a rewrite system semi-deciding validity of formulæ

Here: finite, terminating, confluent, linear rewrite systems

Outline

- Motivations
  - Deduction modulo
  - Proof length in arithmetic
- Speed-up in deduction modulo
- Speed-ups in arithmetic and computation
  - Schematic systems
  - Translations
  - Speed-up
- Conclusion

Sketch of proof

$$
\begin{tikzcd}
Z_{i+1} \arrow[rr, "\mathsf{O}(n)"] & & Z_i \ \mathsf{mod}\ \mathcal{R}_i \\
& Z_i \arrow[ul, "\text{speedup (Buss)}"] \arrow[ur, twoheadrightarrow, "\text{computational speed-up}"'] &
\end{tikzcd}
$$

Sketch of proof

$$
\begin{tikzcd}
Z_{i+1} \arrow[rr, "\mathsf{O}(n)"] & & Z_i \text{ mod } \mathcal{R}_i \\
& Z_i \arrow[ul, "\text{speedup (Buss)}"] \arrow[ur, "\text{computational speed-up}"'] &
\end{tikzcd}
$$

But: Buss' theorem proved for schematic systems, deduction modulo defined for natural deduction

Schematic systems

Buss theorem is true if proofs are done in schematic systems

$\simeq$ Hilbert-type systems

$\simeq$ Frege systems

Metaformulæ

Definition 2 (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 3 (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 instantiating an inference rule.

Schematic System for i^{th}-Order Arithmetic

- Axiom schemata for classical logic with equality:
  $\overline{A \Rightarrow B \Rightarrow A}$ $\overline{\forall \alpha^0 \beta^0.\ \alpha^0 = \beta^0 \Rightarrow A(\alpha^0) \Rightarrow A(\beta^0)}$
- Inference rules for classical logic:
  Modus Ponens: $\dfrac{A \Rightarrow B \quad A}{B}$
  $\dfrac{A \Rightarrow B(\beta^j)}{A \Rightarrow \forall \alpha^j.\ B(\alpha^j)}$ (β^j is not free in $A \Rightarrow \forall \alpha^j.\ B(\alpha^j)$)

Schematic System for i^{th}-Order Arithmetic (cont.)

- Robinson axioms: $\overline{\forall \alpha^0.\ 0 + \alpha^0 = \alpha^0}$, $\overline{\forall \alpha^0 \beta^0.\ s(\alpha^0) + \beta^0 = s(\alpha^0 + \beta^0)}$
- Induction for all formulæ of Z_i: $\overline{A(0) \Rightarrow (\forall \beta^0.\ A(\beta^0) \Rightarrow A(s(\beta^0))) \Rightarrow \forall \alpha^0.\ A(\alpha^0)}$
- Comprehension schema: $\overline{\exists \alpha^{j+1}.\ \forall \beta^j.\ \beta^j \in \alpha^{j+1} \Leftrightarrow A(\beta^j)}$ provided α^{j+1} is not free in A, for $j < i$

Schematic System for i^{th}-Order Arithmetic (cont.)

- Robinson axioms: $\overline{\forall\alpha^0.\ 0+\alpha^0=\alpha^0}$, $\overline{\forall\alpha^0\beta^0.\ s(\alpha^0)+\beta^0=s(\alpha^0+\beta^0)}$
- Induction for all formulæ of Z_i: $\overline{A(0)\Rightarrow(\forall\beta^0.\ A(\beta^0)\Rightarrow A(s(\beta^0)))\Rightarrow\forall\alpha^0.\ A(\alpha^0)}$
- Comprehension schema: $\overline{\exists\alpha^{j+1}.\ \forall\beta^j.\ \beta^j\in\alpha^{j+1}\Leftrightarrow A(\beta^j)}$ 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 Leibniz' equality, 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 Leibniz' equality, 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 the same assumptions

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

classical logic	translated as in [Gentzen, 1934]
Robinson axioms	kept as assumption
Leibniz' equality, 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

$$\Rightarrow\text{-i}\ \frac{\begin{array}{c}[Q]\\ \\ P\end{array}}{Q \Rightarrow P} \quad\rightsquigarrow\quad MP\ \frac{P \qquad \overline{P \Rightarrow Q \Rightarrow P}}{Q \Rightarrow P}$$

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 $i+1^{\text{st}}$-order using computations

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

c: some term representing the formula substituted for A
For instance: $P = (x = 0 \vee \exists y.\ x \in^0 y) \quad \rightsquigarrow$
$$c_P^x \quad = \quad \dot{=}(1, S(0)) \ \cup \ \mathcal{P}^1\left(\dot{\in}^0(S(1), 1)\right)$$

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

Rewriting classes

Terminating and confluent rewrite system:

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

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

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

From axiom schemata to axioms

The instance of the induction schema

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

becomes

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

$$\left(\text{for all } t,\ \langle t \rangle \ \epsilon\ c^x_{P(x)} \xrightarrow{*} P(t)\right)$$

From axiom schemata to axioms

The instance of the induction schema

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

becomes

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

(for all t, $\langle t \rangle \,\epsilon\, c^x_{P(x)} \xrightarrow{*} P(t)$)

New axioms Γ replacing the axiom schemata for Leibniz' equality, induction and comprehension

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

Instance of axiom schemata for $i+1^{\text{st}}$-order arithmetic can be simulated by axioms, using the modulo.

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

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

Instance of axiom schemata for $i+1^{\text{st}}$-order arithmetic can be simulated by axioms, using the modulo.

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

also for natural deduction:

Theorem 4.
For all $i \geq 0$, there exists a (finite terminating confluent linear) rewrite system $\mathcal{R}_i$ and a finite set of axioms Γ such that for all formulæ P, if $Z_{i+1} \vdash^{\mathsf{N}}_{k} P$ then $Z_i, \Gamma \vdash^{\mathsf{N}}_{O(k)}{}_{\mathcal{R}_i} P$.

Adding computation creates a speed-up

Theorem 5.
For all $i \geq 0$, there is a (finite terminating confluent linear) 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 $P \in \mathcal{F}$,* $Z_i \vdash^{\mathsf{N}}_{\overline{k \text{ steps}}\ \mathcal{R}_i} P$
3. *there is no fixed $k \in \mathbb{N}$ such that for all $P \in \mathcal{F}$,* $Z_i \vdash^{\mathsf{N}}_{\overline{k \text{ steps}}} P$

Proof.

$P' = \Gamma \Rightarrow P$

Proof.

$P' = \Gamma \Rightarrow P$

$$Z_{i+1} \vdash_k^{\mathsf{S}} P$$

$$\text{Theo. 1} \updownarrow$$

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

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

$$Z_{i+1} \vdash^{\mathsf{S}}_{k} P \quad \leadsto \quad Z_i, \Gamma \vdash^{\mathsf{N}}_{K}{}_{\mathcal{R}_i} P \quad \leadsto \quad Z_i \vdash^{\mathsf{N}}_{K+3}{}_{\mathcal{R}_i} P'$$

$$\text{Theo. 1} \updownarrow$$

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

□

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

$$
\begin{tikzcd}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P \arrow[r, squiggly] \arrow[d, leftrightarrow, "\text{Theo. 1}"'] & Z_i, \Gamma \vdash^{\mathsf{N}}_{K\,\mathcal{R}_i} P \arrow[r, squiggly] & Z_i \vdash^{\mathsf{N}}_{K+3\,\mathcal{R}_i} P' \\
Z_i \vdash^{\mathsf{S}} P \arrow[r, squiggly] & Z_i, \Gamma \vdash^{\mathsf{N}} P &
\end{tikzcd}
$$

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

$$
\begin{tikzcd}
Z_{i+1} \vdash^{\mathsf{S}}_{k} P \arrow[r, rightsquigarrow] \arrow[d, leftrightarrow, "\text{Theo. 1}"'] & Z_i, \Gamma \vdash^{\mathsf{N}}_{K}{}_{\mathcal{R}_i} P \arrow[r, rightsquigarrow] & Z_i \vdash^{\mathsf{N}}_{K+3}{}_{\mathcal{R}_i} P' \\
Z_i \vdash^{\mathsf{S}} P \arrow[r, rightsquigarrow] & Z_i, \Gamma \vdash^{\mathsf{N}} P \arrow[r, rightsquigarrow] & Z_i \vdash^{\mathsf{N}} P'
\end{tikzcd}
$$

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Speed-ups in arithmetic and computation

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

$$\begin{array}{ccccc}
Z_{i+1} \mathrel{|}\!\!\frac{\mathsf{S}}{k}\ P & \leadsto & Z_i, \Gamma \mathrel{|}\!\!\frac{\mathsf{N}}{K}{}_{\mathcal{R}_i}\ P & \leadsto & Z_i \mathrel{|}\!\!\frac{\mathsf{N}}{K+3}{}_{\mathcal{R}_i}\ P' \\
\text{Theo. 1} \updownarrow & & & & \\
Z_i \mathrel{|}\!\!\frac{\mathsf{S}}{\cancel{3^{k+3}}}\ P & \rightleftarrows & Z_i, \Gamma \mathrel{|}\!\!\frac{\mathsf{N}}{k+3}\ P & \leadsto & Z_i \mathrel{|}\!\!\frac{\mathsf{N}}{k}\ P'
\end{array}$$

$\square$

Proof.

$P' = \Gamma \Rightarrow P$

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

$\square$

Outline

- Motivations
  - Deduction modulo
  - Proof length in arithmetic
- Speed-up in deduction modulo
- Speed-ups in arithmetic and computation
  - Schematic systems
  - Translations
  - Speed-up
- Conclusion

Difference between $i+1^{\text{st}}$- and i^{th}-order arithmetic : expressed as a confluent and terminating rewrite system

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

Difference between $i+1^{\text{st}}$- and i^{th}-order arithmetic : expressed as a confluent and terminating rewrite system

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

$$\begin{tikzcd}
Z_{i+1} \arrow[rr, "\mathrm{O}(n)"] & & Z_i \text{ mod } \mathcal{R}_i \\
& Z_i \arrow[ul] \arrow[ur, "\text{computational speed-up}"'] &
\end{tikzcd}$$

Difference between $i+1^{\text{st}}$- and i^{th}-order arithmetic : expressed as a confluent and terminating rewrite system

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

$$
\begin{tikzcd}
Z_{i+1} \arrow[rr, "\mathrm{O}(n)"] & & Z_i \text{ mod } \mathcal{R}_i \\
& Z_i + T_i \arrow[ul] \arrow[ur, "\text{computational speed-up}"'] & \\
& Z_i \arrow[u, "\text{speedup (Buss)}"] &
\end{tikzcd}
$$

Perspectives

It is possible to give a full axiomatization of higher-order arithmetic entirely as a theory modulo (`http://www.loria.fr/~burel/download/hhamod.pdf`)

Perspectives

It is possible to give a full axiomatization of higher-order arithmetic entirely as a theory modulo (`http://www.loria.fr/~burel/download/hhamod.pdf`)

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	[D. Cousineau et al., 2007]
$\lambda\Pi$	"	FOL modulo	[Work in progress]

Cousineau, D. and Dowek, G. (2007).
Embedding pure type systems in the lambda-pi-calculus modulo.
In Ronchi Della Rocca, S., editor, *TLCA*, volume 4583 of *Lecture Notes in Computer Science*, pages 102–117. Springer-Verlag.

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.

Dowek, G., Hardin, T., and Kirchner, C. (2003).
Theorem proving modulo.
Journal of Automated Reasoning, 31(1):33–72.

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.
In *Proc. 2006 Int. Workshop on Proofs and Programs*, Lecture Notes in Computer Science. Springer-Verlag.