On specifications and proofs

Claude Kirchner

INRIA
Bordeaux—Nancy

December 2007

Some French projects on specification, language and proof

- Synchrone Languages
  Esterel, Signal, Lustre
- Proof environments
  Coq, B, Focal, CADP,
  Why platform : for C (Caduceus) and Java (Krakatoa)
- Languages
  OCAML, TOM
- Certified compiler
  Gallium Team
- 4 colors theorem formal proof
  INRIA and MSR
- Specification and proof of protocols properties
  AVISPA-TOOL
- Rewriting calculus

The computational telescope

Computers profoundly change our way to make science because of the power of computation

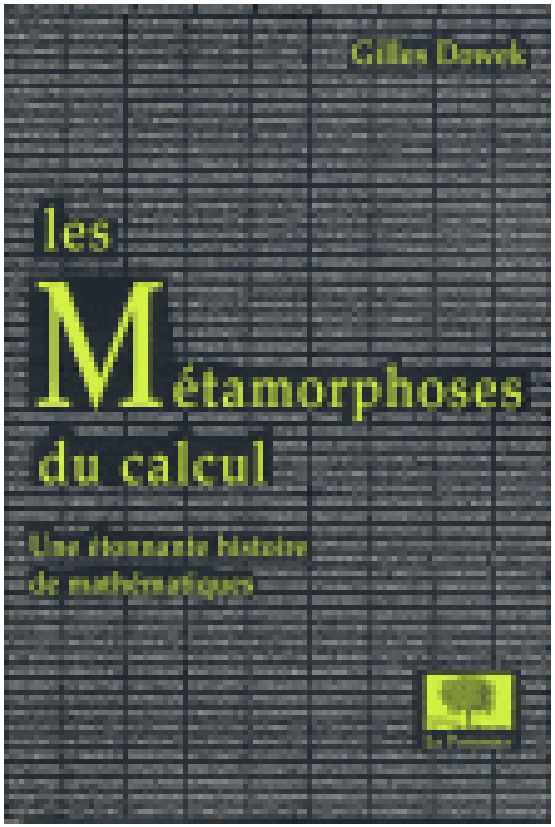
It is reasonable to hope that the relationship between computation and mathematical logic will be as fruitful in the next century as that between analysis and physics in the last.

The development of this relationship demands a concern for both applications and for mathematical elegance.

John McCarthy

Towards a new generation of proof assistants

Computation
and
Deduction
are both
first-class citizen



Gilles Dowek
Grand prix de philosophie de l'Académie Française 2007

Good proofs

Proofs are fundamental certificates

Certificates should be informative, communicable and checkable

So proof should be good...

What is a good proof ?

Peano's axioms in modern notations

$$\forall y.(0 + y = y)$$
$$\forall x.\forall y.(S(x) + y = x + S(y))$$
$$\forall x.(x = x)$$
$$\forall x.\forall y.\forall z.((x = y \wedge y = z) \Rightarrow x = z)$$

Let us look at the well known example of $1 + 1 = 2$
(not speaking of $2 + 2 = 4$!)

written here $S(0) + S(0) = S(S(0))$

The proof of 1+1 = 2

The proof of 1+1 = 2

$$
(\Rightarrow E)\ \dfrac{
\begin{array}{l}
(\forall E)\ \dfrac{
\begin{array}{l}
(\forall E)\ \dfrac{
\begin{array}{l}
(\forall E)\ \dfrac{
(Ax)\ \dfrac{}{\Gamma \vdash \forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)}
}{\Gamma \vdash \forall y.\forall z.(S(0) + S(0) = y \wedge y = z \Rightarrow S(0) + S(0) = z)}
\end{array}
}{\Gamma \vdash \forall z.(S(0) + S(0) = 0 + S(S(0)) \wedge 0 + S(S(0)) = z \Rightarrow S(0) + S(0) = z)}
\end{array}
}{\Gamma \vdash S(0) + S(0) = 0 + S(S(0)) \wedge 0 + S(S(0)) = S(S(0)) \Rightarrow S(0) + S(0) = S(S(0))}
\\
(\wedge I)\ \dfrac{
\begin{array}{l}
(\forall E)\ \dfrac{
\begin{array}{l}
(\forall E)\ \dfrac{
(Ax)\ \dfrac{}{\Gamma \vdash \forall x.\forall y.(S(x) + y = x + S(y))}
}{\Gamma \vdash \forall y.(S(0) + y = 0 + S(y))}
\end{array}
}{\Gamma \vdash S(0) + S(0) = 0 + S(S(0))}
\end{array}
\qquad
\begin{array}{l}
(\forall E)\ \dfrac{
(Ax)\ \dfrac{}{\Gamma \vdash \forall y.(0 + y = y)}
}{\Gamma \vdash 0 + S(S(0)) = S(S(0))}
\end{array}
}{\Gamma \vdash S(0) + S(0) = 0 + S(S(0)) \wedge 0 + S(S(0)) = S(S(0))}
\end{array}
}{\Gamma \vdash S(0) + S(0) = S(S(0))}
$$

Integrating computation : a new proof

Defining the computation by :

$$\begin{aligned} 0 + y &\rightarrow y \\ S(x) + y &\rightarrow x + S(y) \end{aligned}$$

The proof becomes :

Integrating computation : a new proof

Defining the computation by :

$$\begin{aligned} 0 + y &\rightarrow y \\ S(x) + y &\rightarrow x + S(y) \end{aligned}$$

The proof becomes :

$$(\forall E)\langle x,\ x{=}x,\ S(S(0))\rangle \ \frac{(Ax)\ \dfrac{}{\Gamma \vdash_{\cong} \forall x.(x = x)}}{\Gamma \vdash_{\cong} S(0) + S(0) = S(S(0))}$$

Super Deduction Modulo

Towards a new generation of proof assistants where the computation process is a first class citizen and proofs are designed modulo computation.

Towards the essence of proofs

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

Towards the essence of proofs

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

Theorem (Burel, CSL 2007)

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

A remarquable result :

Guillaume Burel.
Unbounded proof-length speed-up in deduction modulo.
In *CSL*, 2007.