Proof by computation

Benjamin Grégoire

INRIA Sophia Antipolis

Types Summer School
August 31th

How to prove $2 + 2 = 4$ in Coq ?
Demo
Why it is a correct proof ?

Conversion rule

$$\frac{\Gamma \vdash t : T \quad T \equiv U}{\Gamma \vdash t : U}$$

Definition

- $T \equiv U$: T is convertible with U
- $\equiv$ is the reflexive, symmetric and transitive closure of the reduction rules
- the conversion use strong reduction (i.e. reduction under binder)

Remarks:

- T and U are types but (can contain programs) like in $2 + 2 = 4$
- Confluence of reduction rules + strong normalization imply decidability of the convertibility (so of the type checking)

Derivation of

$$\vdash \mathsf{refl\_equal}\ Z\ 4 : 2 + 2 = 4$$

Application: proof by computation (reflection)

- Let $P : A \to \mathrm{Prop}$ a property over element of A
- Let $\mathrm{test} : A \to \mathrm{bool}$ a semi-decision procedure for P
- Let $\mathrm{test\_correct} : \forall x : A.\ \mathrm{test}\ x = \mathrm{true} \to P\ x$ a proof that the semi-decision procedure is correct

Assuming that $\mathrm{test}\ a$ reduce to true, a proof of $P\ a$ is

$$\mathrm{test\_correct}\ a\ (\mathrm{refl\_equal}\ \mathrm{true})$$

Example in Coq: primality

Different strategies for the conversion test

Lazy versus Call-by-value

Example of primality proof

- Mersenne numbers: $2^n - 1$
  Lucas test: $2^{216091} - 1$ checked in Coq (31th Mersenne prime, 8 days)
- Pocklington certificate (less than 100 digits)
- Elliptic curves (Laurent Théry) (less than 300 digits)

For Pocklington and Elliptic curves it can be see as result checking

Other examples of proof by computation

- 4-colors theorem (Gontier, Werner)
- Coq tactic for user: ring, field, romega, micromega(linear and little more)

micromega also based on result certification.

See homepage of F Besson, B Grégoire, A Mahboudi, L Théry.

Result checking

Theorem (Pocklington)

For all N, such that $N - 1 = F * R$ and if exists a such that:

- $F = p_1 \ldots p_n$
- $N < F^2$
- $a^{N-1} \mod N = 1$
- $\forall p \in \{p_1, \ldots, p_n\}.\ \gcd(a^{\frac{N-1}{p}} - 1, N) = 1$
- $\forall p \in \{p_1, \ldots, p_n\}.\ \textit{prime } p$

then N is prime

Advantages of proof by computation

- Small proof
- Efficient checking

The semi-decision procedure (or the checker) has to be proved but have not to generate a proof.

Application to PCC

- Reducing the TCB: certified VCgen
- Reducing the TCB and small certificate: certified analysis
- We can mix the two

Coq demo: A certified VCgen for bytecode