Correctness through proof

Foundational Proof Certificates

Rob Blanco, Dale Miller et al.
Inria and LIX/École polytechnique

DSSS17 student talk
20 July 2017

Two questions

How to **trust** proofs [*sic*?]

How to **communicate** proofs

One answer

Universal proof system and trusted **proof checkers**

Flexible, independent definition of **proof certificates**

General enough for most paradigms you can think of (Coq?)

- Next: collaborative formats for **theorem prover evidence**

A taste of programmable sequent calculus

Definition side:

$$\dfrac{\texttt{(dlist [}i,j\texttt{])} \vdash \Gamma \Uparrow C_k \qquad \dfrac{\texttt{(rlist R)} \vdash \Gamma, \texttt{(idx k)} : \neg C_k \Uparrow}{\texttt{(rlisti R } k\texttt{)} \vdash \Gamma \Uparrow \neg C_k}\ store}{\texttt{(start } (n+1)\texttt{) (resol } i\ j\ k\texttt{::R)} \vdash \Gamma \Uparrow}\ cut$$

```
cut_ke (start C Resol) C1 C2 Cut :- cut_ke (rlist Resol) C1 C2 Cut.
cut_ke (rlist (resol I J K::Rs)) (dlist [I,J]) (rlisti K Rs) Cut :-
  lemma K Cut.
```

Certificate side: [resol 2 2 4; resol 4 4 5; resol 1 5 6; resol 6 3 7]

To know more

https://team.inria.fr/parsifal/proofcert/

roberto.blanco@inria.fr

Let's talk :-)