

"For mathematicians
there is no ..b..us"

D. Hilbert

Burden of Proof

- We aim to make writing proofs by computer easier through better automation.
- This will be achieved by exploiting the combined strengths of specialised tools.

Challenges

- Balancing soundness and efficiency.
- Choosing suitable source and target logics or fragments.
- Optimisation and other techniques for some logics are not yet well-developed.
- Understanding how different approaches relate to one another.

Benefits

- Proofs discovered by external tools are re-checked in the host system. This provides a high level of assurance of their correctness.
- Compared to the monolithic approach, building tools by combining simpler tools is sensible and safe.

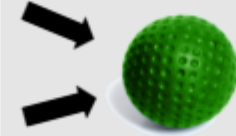
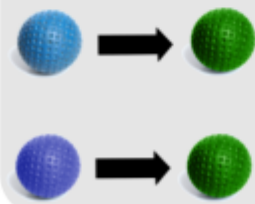
Method

Start with a problem which has been encoded into an expressive logic, then:

1 Break problem down into simpler ones which are expressible in simpler logics.

2 Dispatch subproblems to automatic tools.

3 Compose the proofs back into a proof for the original problem, in the original logic.



Background

Mathematics relies on proofs, which can be made precise using a logic. Doing mathematics requires **creativity** and **calculation**. A computer can do calculations with far greater speed than we can. Creativity, so far, is mostly left up to us to provide. Computers have been successfully employed in **checking** our mathematics, and there have been encouraging results in automating the **proof-search** process too.

Having improved automation would help increase the scope of interactive theorem-provers such as Isabelle:

```
Proof: thy "isabelle/isar"
theorem "( $\sum_{i=1}^n (2 * i + 1) = n^2$ )"
  (is "P n" is "S n = n^2")
proof (induct n)
  show "P 0" by step
next
  fix n
  have "P (Suc n) = S (2 * n + 1) + P n" by step
  also assume "S n = n^2"
  also have "... + 2 * n + 1 = (n+1)^2"
    by (step add power2_eq_square)
  finally show "P (Suc n)" by step
qed
-----
Mkmc: Proof: thy "clear script 33 Isabelle/Isar/Scripting
proof (state): step 2
Fixed variables: n, n = n
this:
( $\sum_{i=1}^{n+1} (2 * i + 1) = (\sum_{i=1}^n (2 * i + 1) + 2 * n + 1$ )
goal (cheer, 1 output):
1.  $\forall n. (\sum_{i=1}^n (2 * i + 1) = n^2) \Rightarrow (\sum_{i=1}^{n+1} (2 * i + 1) = (n+1)^2$ 
-----
Mkmc: "isabelle/isar-goals" (Group:state) --- All
Display the current context
```

(More on Isabelle at www.cl.cam.ac.uk/research/hvg/Isabelle)

