Usability Issues in Formal Methods

Topics

- Tooling
- Pen-and-paper proofs
- Publishability
- Training
- Verifiability
- Others?

Tooling

Tools for producing mechanical proofs can be a limiting factor in our ability to produce proofs.
Tool developers often prefer to work on fancy new features over UI/UX improvements.

Pen-and-Paper Proofs

Pen-and-paper proofs can be easier to produce than mechanised ones.
However as they become longer it becomes harder to be sure they are correct.

Publishability

A successful analysis may find no issues, i.e. that the protocol meets its goals.
Such results are very hard to get published because they are not “novel”, even though they may be valuable to the community.

Training

People report finding the learning curve for formal methods tools too steep.
There are limited intermediate level training materials.

Verifiability

Verifying a mechanical proof is correct can take many hours and cost hundreds or even thousands of dollars.

Verifying a pen-and-paper proof can take weeks or months of expert time.

Often these are far beyond the resources of peer-review.

Others?

Reusability, Composability, Understandability, Mathematical limits, ...