The Challenge of Teaching Proofs

- Concepts like induction are inherently complex.
- Easy to get details wrong, without realizing it.
- Feedback in a typical course may take a week or more to grade.

Wouldn’t it be nice if there were an easy-to-use tool that provides students with immediate feedback on mistakes in their proofs?

Introducing SASyLF: a Second-order Abstract Syntax Logical Framework ("Sassy Elf")

Teaching with SASyLF

We used SASyLF for an assignment reasoning about the dynamic semantics of programs in a Spring 2008 graduate course at CMU. Our findings in a controlled experiment were generally promising:

- 11 of 13 students who used the SASyLF tool found that it helped them find errors in their proofs.
- 12 of 13 said the tool increased their confidence that their proofs were correct.
- In contrast, 14 of 16 members of the control (no tool) group wished they had earlier feedback on their mistakes.

Some students dropped out due to usability issues with the tool, many of which we have since addressed. Still, 7 of 11 surveyed students who completed the study with the tool would use the tool again, and another three would use it if the usability issues were addressed.

Comparing the tool to handwritten proofs, one student said, “I actually did the entire assignment on paper first and then moved over to using the tool. I found the paper approach really easy. But once I started using the tool I started understanding the concepts better.”

SASyLF Definitions

SASyLF Proofs

The Tool: SASyLF supports proving so-called "normal" statements of the form "for all judgments J, there exists a judgment J' that tells us something." When we case-analyze, we give a premise per line above the bar, and the conclusion below it.

Proofs are a sequence of statements of the form:

- name : judgment <justification>

The name is used to refer to the fact later. The judgment is the fact, while the justification is an argument for why the fact holds. Facts are facts that hold due to induction.

Because SASyLF builds in hypothetical judgments, "forall" in proofs for subgoals really means that the judgment holds exactly when the case can be replaced with a judgment showing that some another type J is the case. To have judgment J that tells us something J' in structural induction is enough to show that J" in the body of the induction hypothesis on the assumption that e. We can get it by substituting J' into J. To use the rule in a conclusion lemma is required, although we could prove one for pedagogical purposes if we want.

www.sasylf.org

- Open source release of SASyLF
- Paper(s) describing the tool and our teaching experience
- Documentation and examples
- A solution to part 2A of the POPLmark challenge for mechanized metatheory

Related Work

- Educational Tools for Logic
- Educational Tools for PL Theory
- DrElche

SASyLF Design Goals

- Gentle learning curve. Professors don’t have time to spend teaching tools!
- Familiar syntax. The surface syntax of SASyLF mirrors paper proofs.
- Explicit notation. Making clear what is going on aids the learning process.
- Minimal math context. SASyLF is based exclusively on rule induction — set theory, etc. is omitted.
- Support for variable binding. Encoding variables is difficult and distract-

- Incremental proof development. Can write "unproved" for any statement and the assistant will assume it is true (but will yield a warning).
- Local checking and localized errors. Understanding what went wrong is critical to learning, so all checks are local and errors point to the specific low-level step that failed.