CS 494 – Provably Correct Programming

William Mansky

Questions?

Top

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Interactive Theorem Provers

- In the theorem prover, we can:

1. Write **definitions**, in a math-like programming language
2. Write **proofs** about those definitions, using logic “tactics”
3. See the **proof state** at each point in a proof (what do we know? what do we still need to show?)
4. Automatically **check** that each step of our proofs is valid

Writing Definitions in Coq

- The definition language of Coq is an OCaml-like functional programming language, called Gallina
- Key features: inductive types, pattern matching, and recursion
- Purpose is to *define mathematical objects*, not to write programs (though the two are often the same!)

- See Basics.v from the textbook

Have you used a functional language with datatypes and pattern matching before?

Yes
No
Not sure

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Inductive Definitions

```
Inductive day :=
  | monday
  | tuesday
  | wednesday
  | thursday
  | friday
  | saturday
  | sunday.
```

Types are sets!

$$\{\text{monday}, \text{tuesday}, \ldots, \text{saturday}, \text{sunday}\}$$

day is a type	day is a set
monday : day	monday ∈ day
tuesday : day	tuesday ∈ day
…	…
saturday : day	saturday ∈ day
sunday : day	sunday ∈ day

Exercise: nandb

- Complete the exercise “nandb” in Basics.v: fill in the definition of nandb, and prove that the examples work
- Submit your definition and example proofs for Exercise 1/13 on Gradescope

- It may help to refer to the definitions of negb, andb, and orb earlier in the file

Inductive Definitions

How would you define the natural numbers?

Questions?

Top

HW1: Basics.v

- Complete all the exercises in Basics.v (you may skip the one marked optional)
- You can run BasicsTest.v to make sure you’ve gotten all of them
- Due Thursday 1/20 at 2 PM
- Submit via Gradescope