

# CS 472 – Provably Correct Programming

William Mansky

## Questions

Nobody has responded yet.

Hang tight! Responses are coming in.

# Interactive Theorem Provers

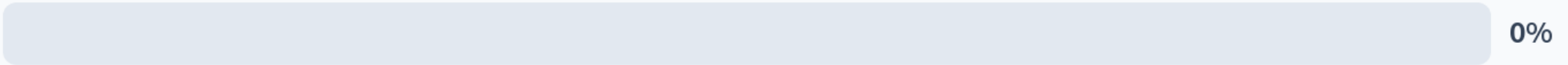
- In the theorem prover, we can:
  1. Write **definitions**, in a math-like programming language
  2. Write **proofs** about those definitions, using logic “tactics”
  3. See the **proof state** at each point in a proof (what do we know? what do we still need to show?)
  4. Automatically **check** that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

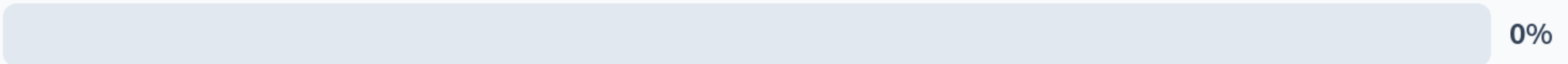
Yes



No



Not sure



# Inductive Definitions

Inductive day :=	Types are sets!	
monday	{monday, tuesday, ..., saturday, sunday}	
tuesday		
wednesday	day is a type	day is a set
thursday	monday : day	monday ∈ day
friday	tuesday : day	tuesday ∈ day
saturday	...	...
sunday.	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 1/10 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

Nobody has responded yet.

Hang tight! Responses are coming in.

# 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; there's also an autograder on Gradescope, though it checks more problems than were assigned
- Due Sunday 1/21 at 11:59 PM
- Submit via Gradescope