CS 839 Systems Verification

Lecture 3: Induction

Learning outcomes

1. Informally reason about disjunction and exists
2. Appreciate the nuances of induction

Rocq demo: Disjunctions

Safe vs unsafe tactics

Recall some tactics:

- `intros`
- `destruct`
- `left`
- `right`
- `reflexivity`
- `simpl`

Which of these are safe?

Define a *safe tactic* as one that if the goal is true, creates only true goals.

Short exercise, just gets them thinking about the semantics of each tactic.

Rocq demo: exists

Exercise: informal exists proof

5-min break

Induction

Transition to digital whiteboard

First example: sum of 1..n

$$1 + 2 + \cdots + n = n(n+1)/2$$

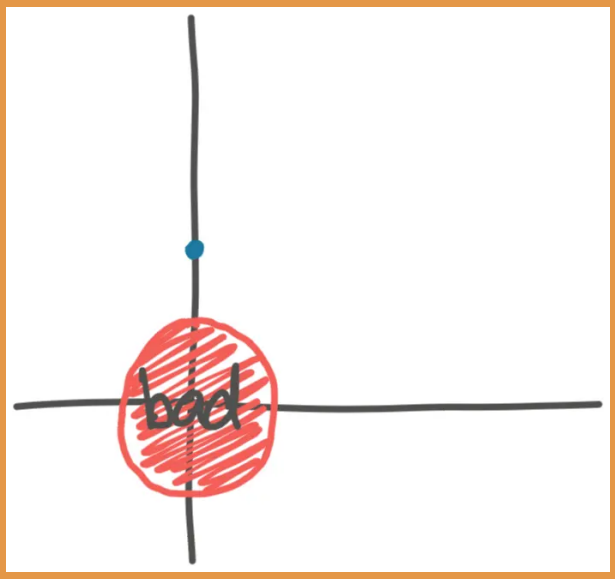
Principle of induction

Have some $P : \mathrm{nat} \to \mathrm{Prop}$

Show $P(0)$

Show $\forall k, P(k) \to P(k+1)$

Derive $\forall n, P(n)$

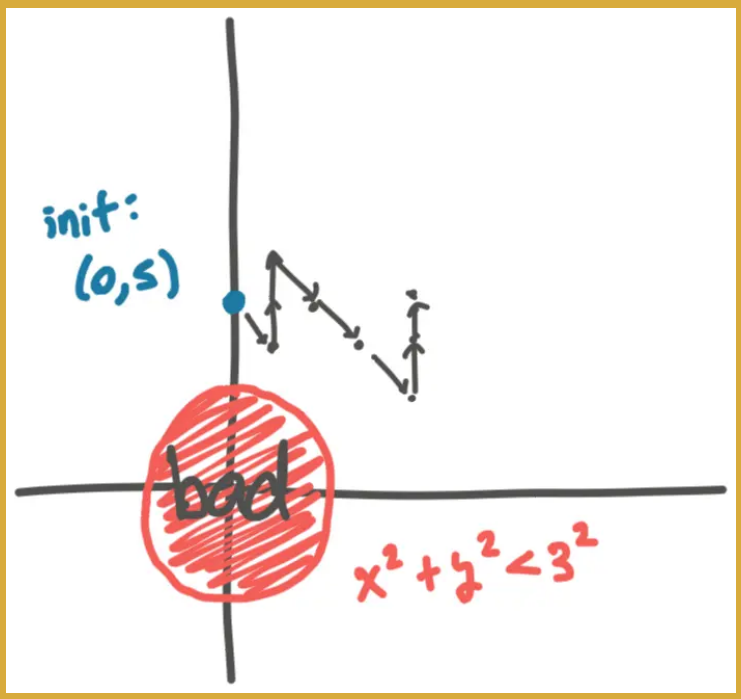


Another example

Imagine a 2D plane

There is a hole of radius 3 at the origin

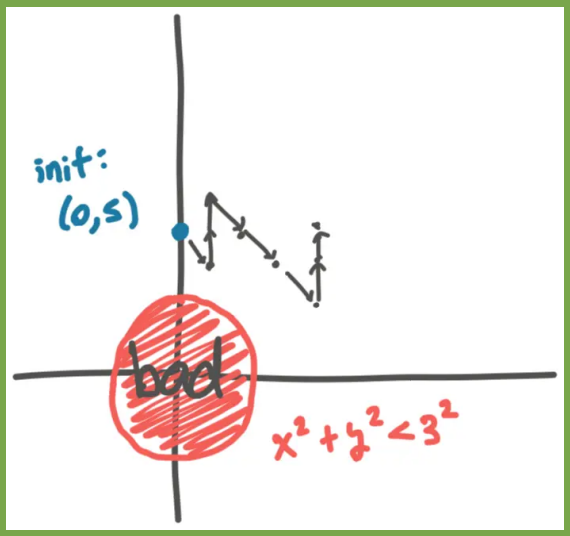
Crawler dynamics



Formalization

We need to formalize this a bit to prove it.
The crawler's behavior can be described by a sequence of states, where a state is just the coordinates. A sequence is good enough because the crawler moves one discrete step at a time.

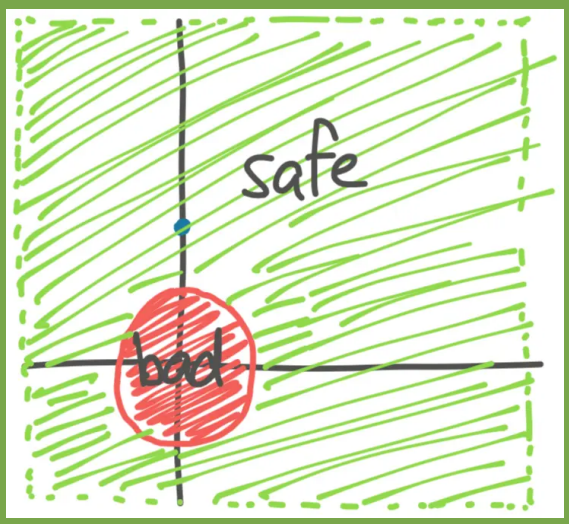
Correctness

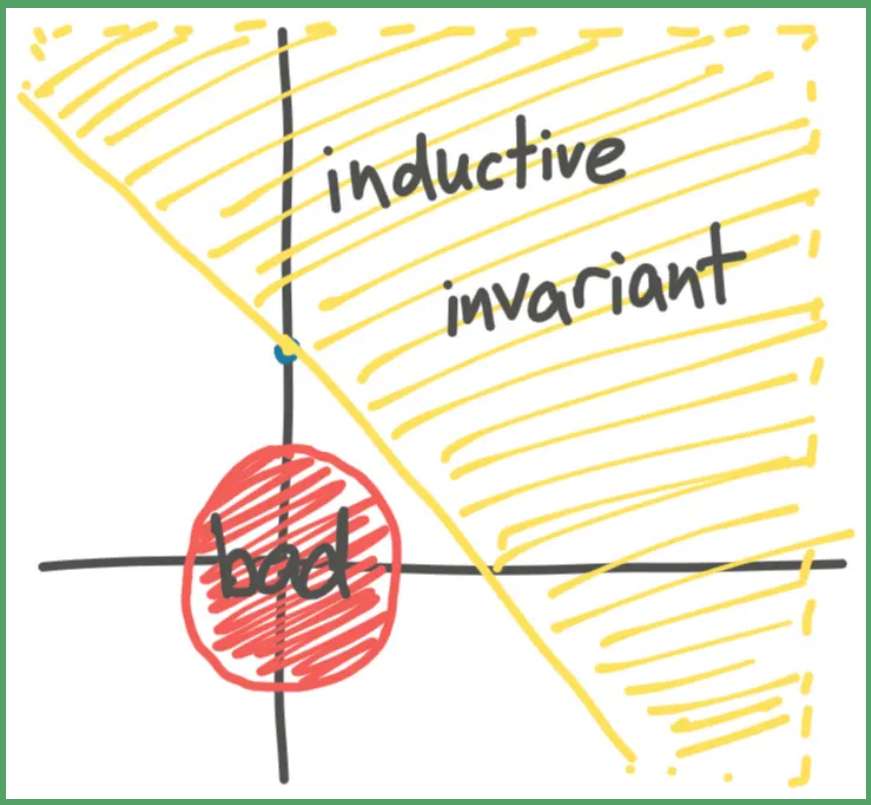


$e = \sigma_0, \sigma_1, \sigma_2, \ldots$

$tr(e(i), e(i+1))$

Want $\forall i, \text{safe}(e(i))$




inductive
invariant
bad

Exercise: finite example

transitions $tr(i, j)$

(e.g., $tr(1, 2) = \text{true}$, $tr(2, 4) = \text{false}$)

To prove: $\forall i, e(i) \neq 6$