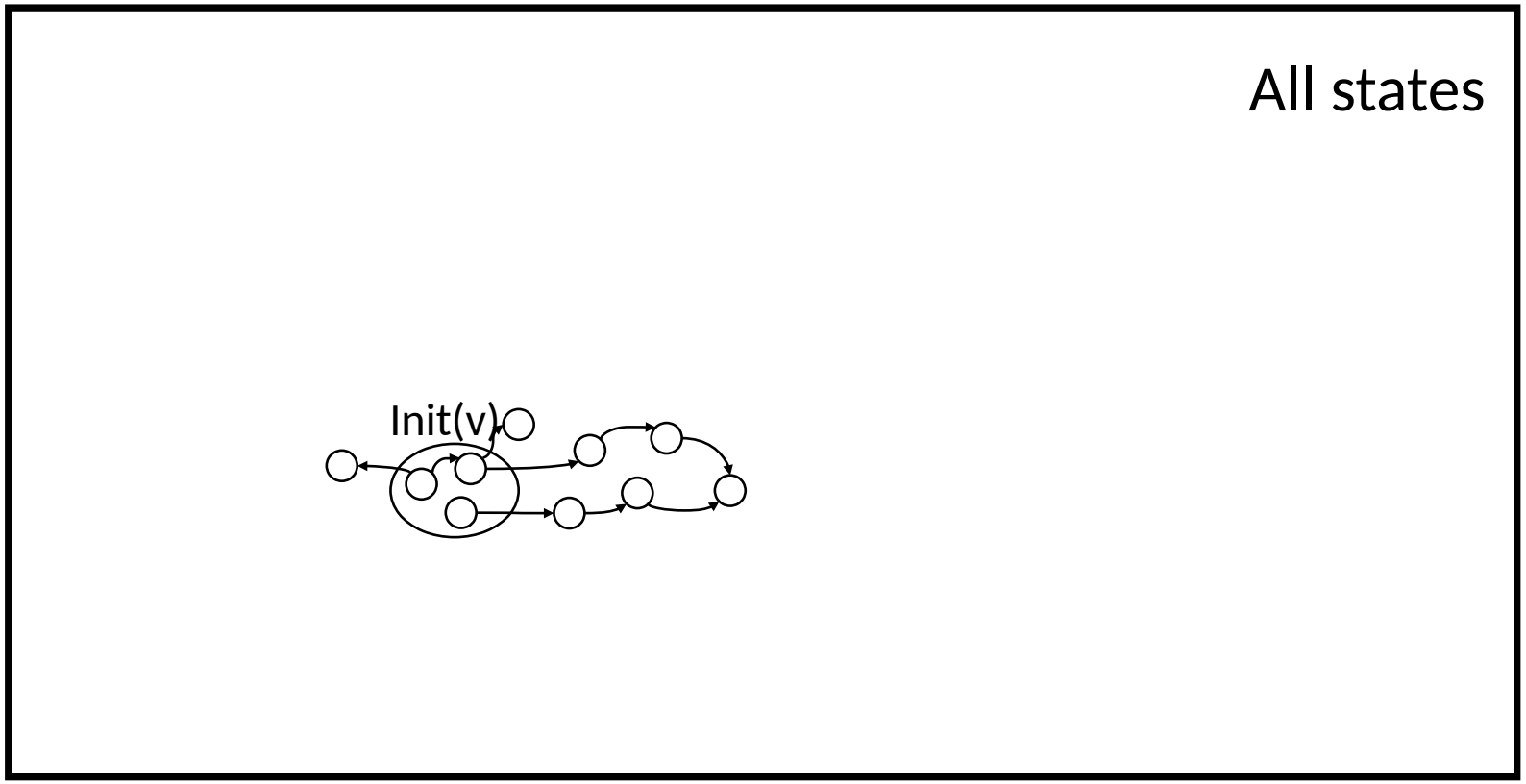
EECS498-003
Formal Verification of Systems Software

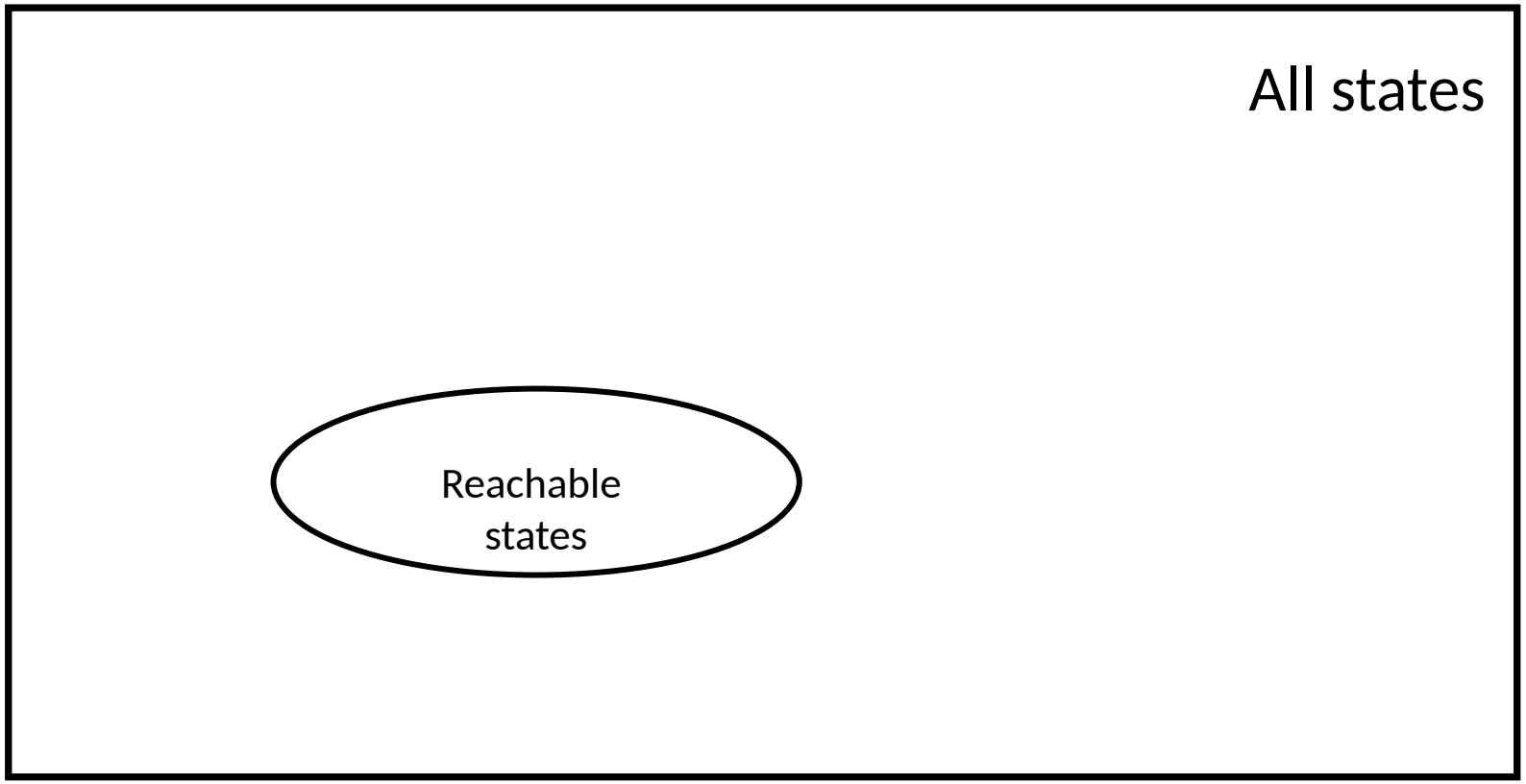
Material and slides created by

Jon Howell and Manos Kapritsos

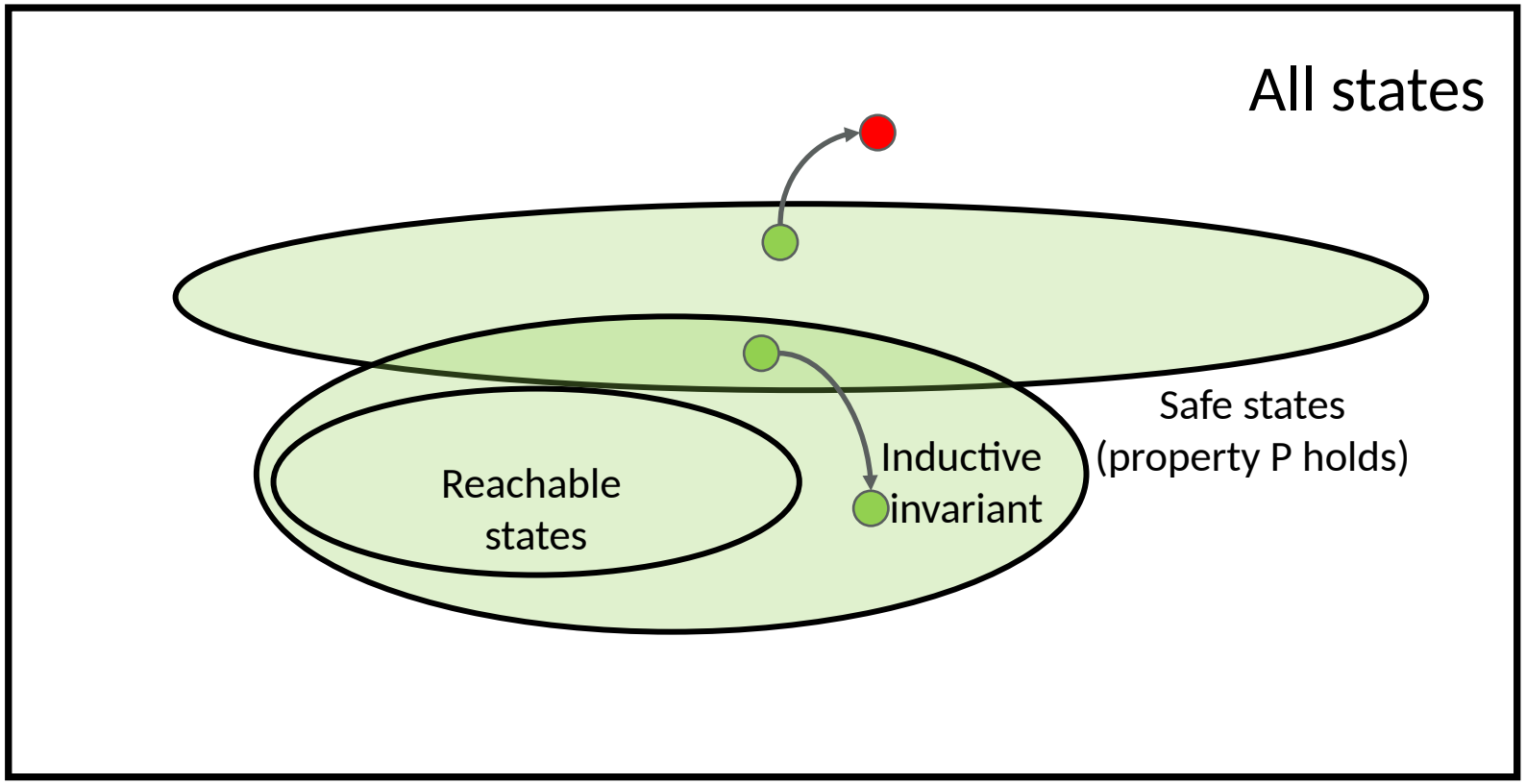
Invariants vs Inductive invariants



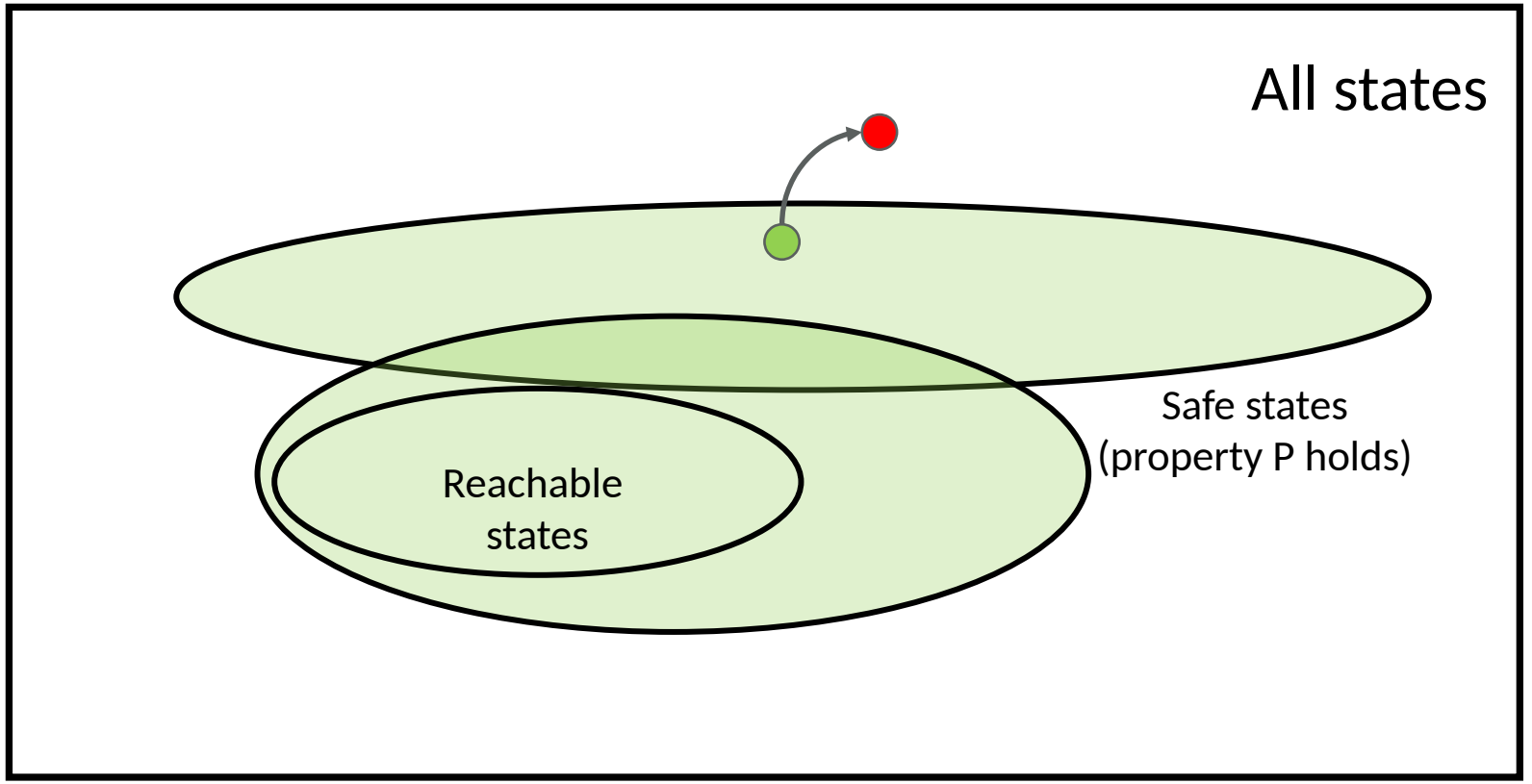
Invariants vs Inductive invariants



Invariants vs Inductive invariants

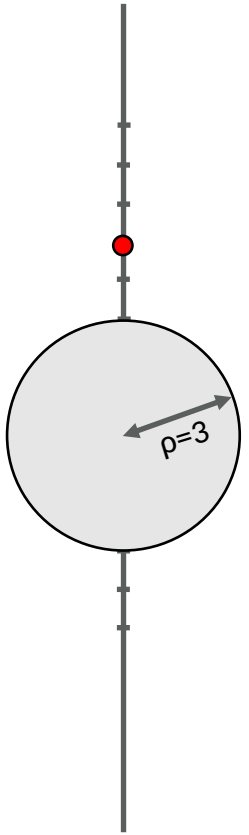


Dangerous states



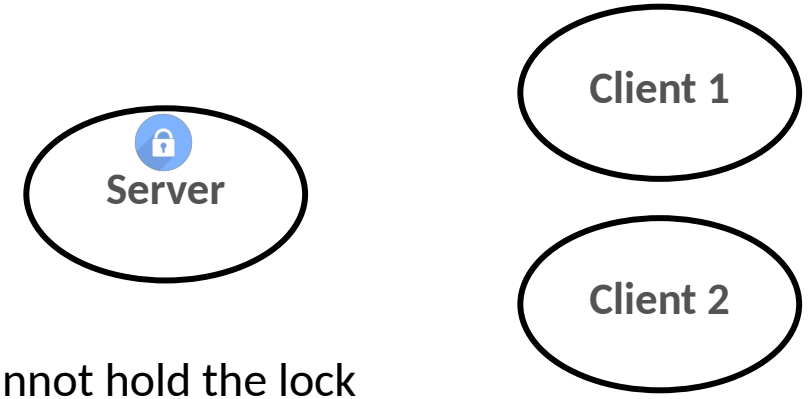
Crawler 2: Revenge of the inductive invariant

- The crawler can now only move North/South
  - Initially it can only move North
- It can also Flip(), teleporting to the symmetric point on the y-axis and changing direction of movement



VSCode transition

Lock server revisited



datatype Variables = Variables(S: bool, C1: bool, C2:bool)

ghost predicate Safety(v) { !(v.C1 && v.C2) }

Both clients cannot hold the lock at the same time

Trivialization #1: A single variable

datatype Variables = Variables(whoHoldsTheLock: int)

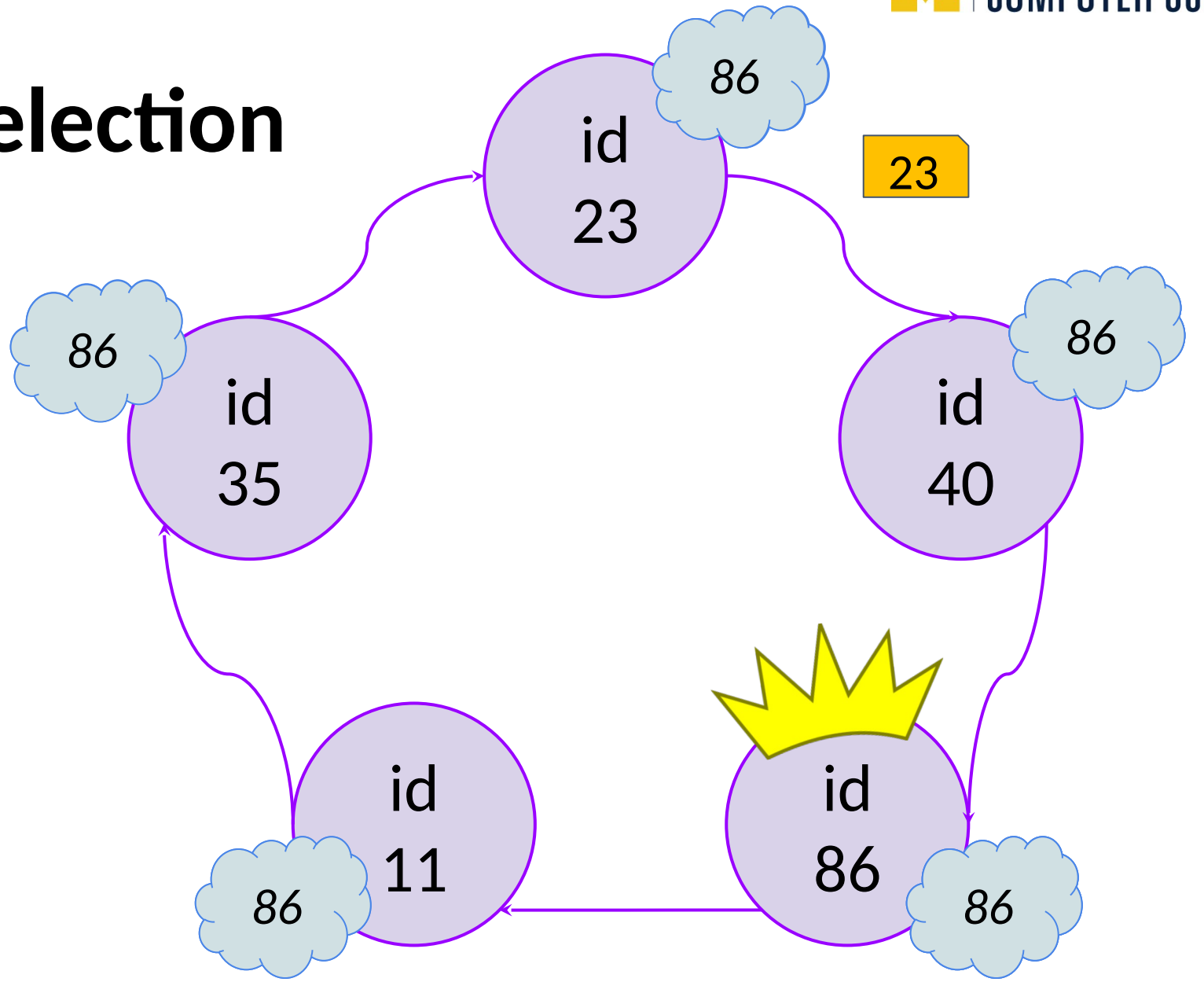
Trivialization #2: Putting Safety/Inv in your transitions

```
predicate ReleaseLock(v) {
  && Safety(v)
  && ...
```

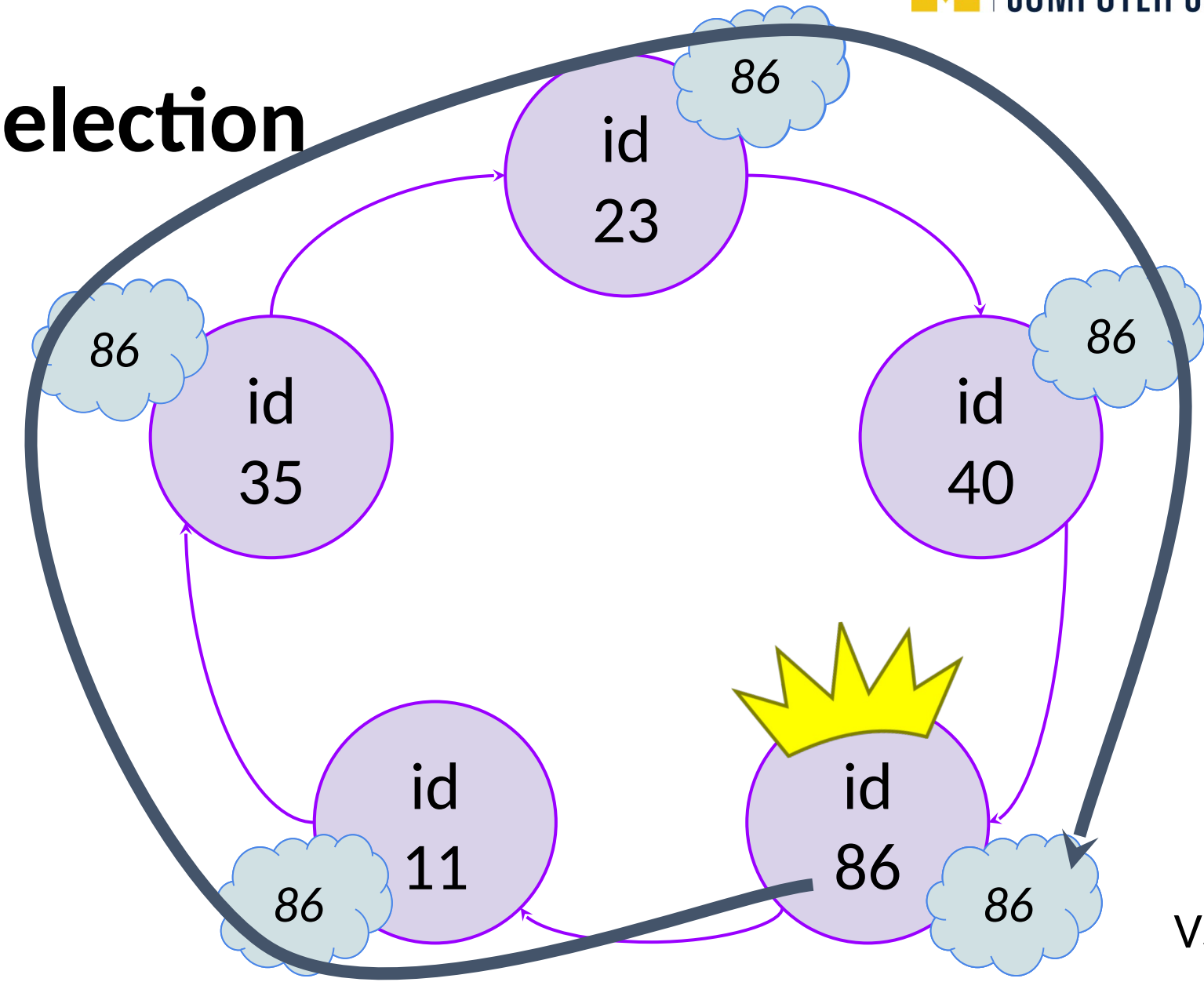
Administrivia

- Keshav is sick, so lab tomorrow is canceled
- PS2 due in one week

Leader election

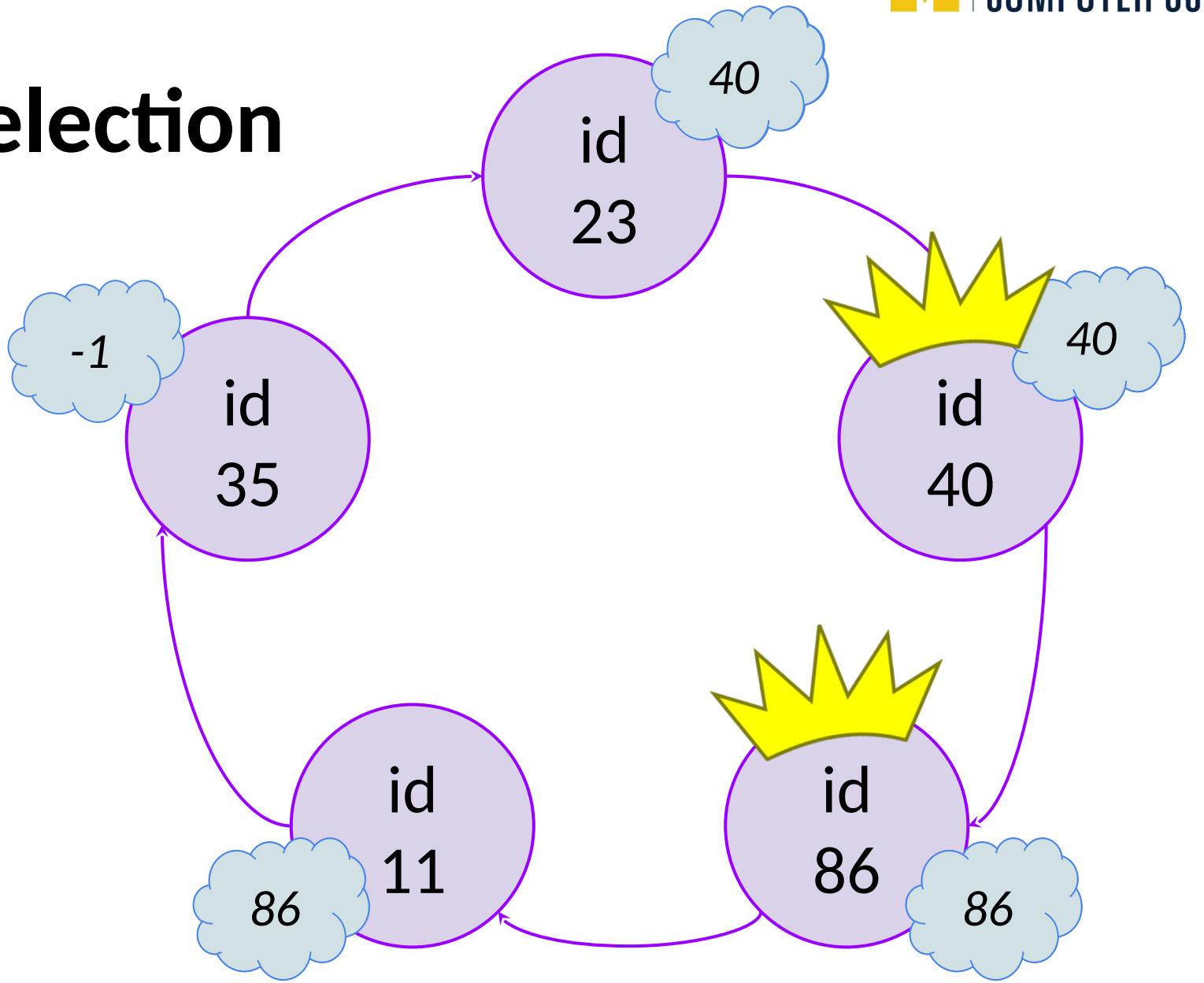


Leader election



VSCode transition

Leader election



Leader election