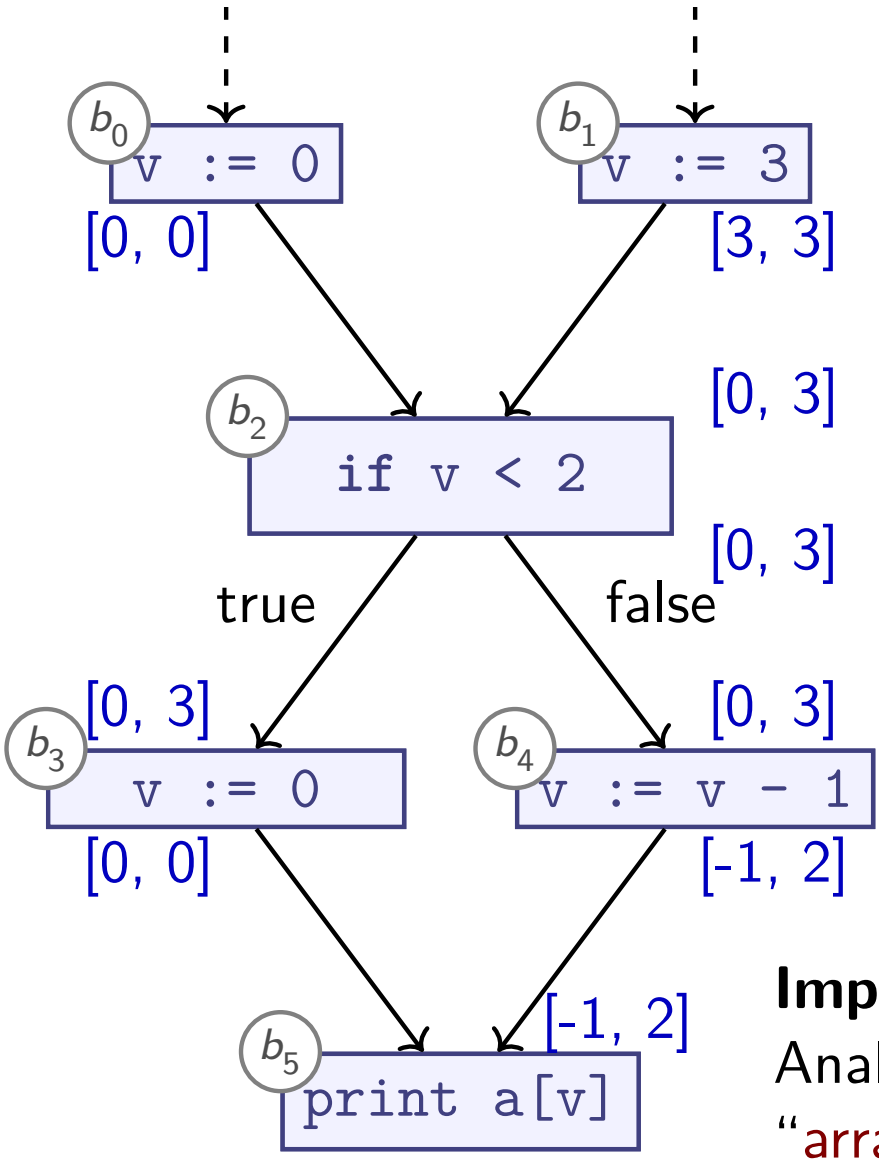
LUND UNIVERSITY

EDAP15: Program Analysis

DATAFLOW: CONTROL SENSITIVITY

Christoph Reichenbach

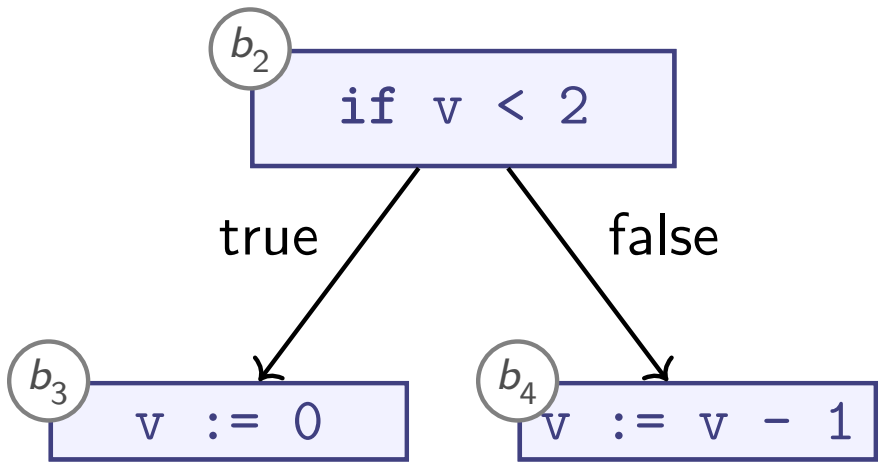
Conditionals



Imprecision can yield false positive
Analysis concludes:
"array index may be negative"

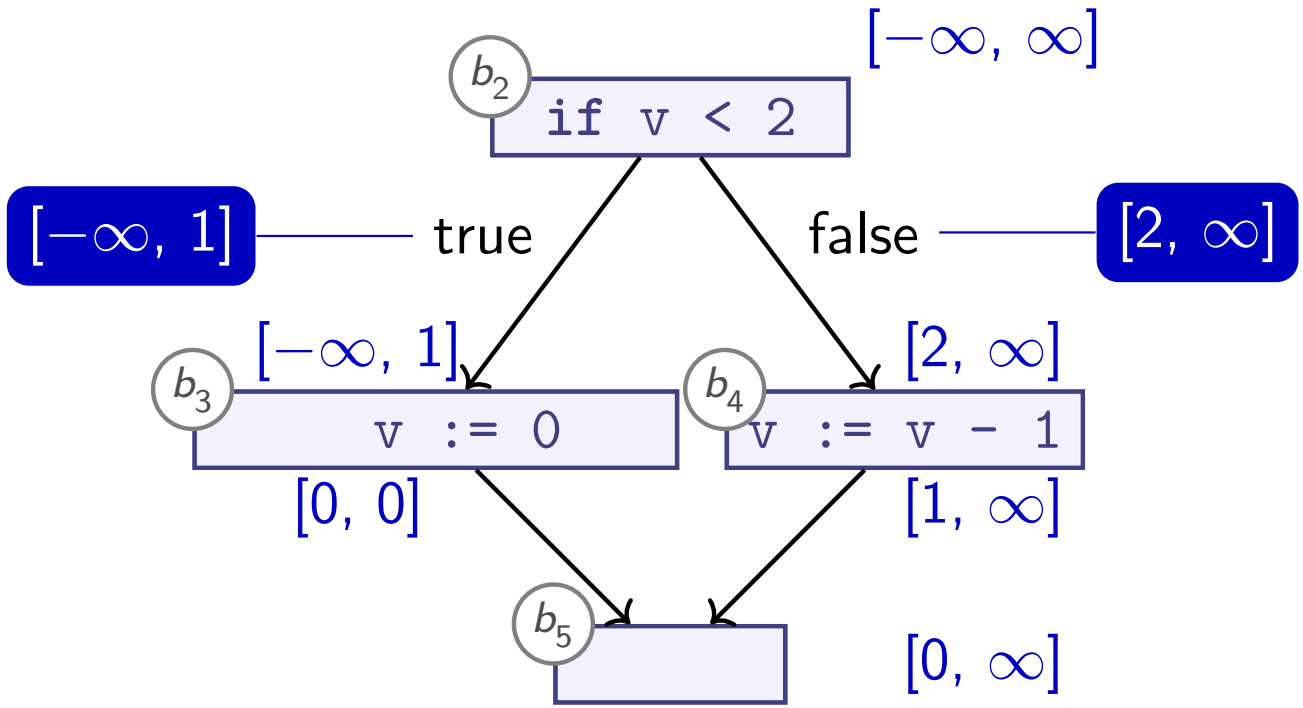
Handling Conditionals (1/2)

- So far: Did not make use of conditional predicate
  - `true` branch: only if `v < 2`
    $v \in [-\infty, 1]$
  - `false` branch: only if $\neg$`(v < 2)`
    $v \in [2, \infty]$



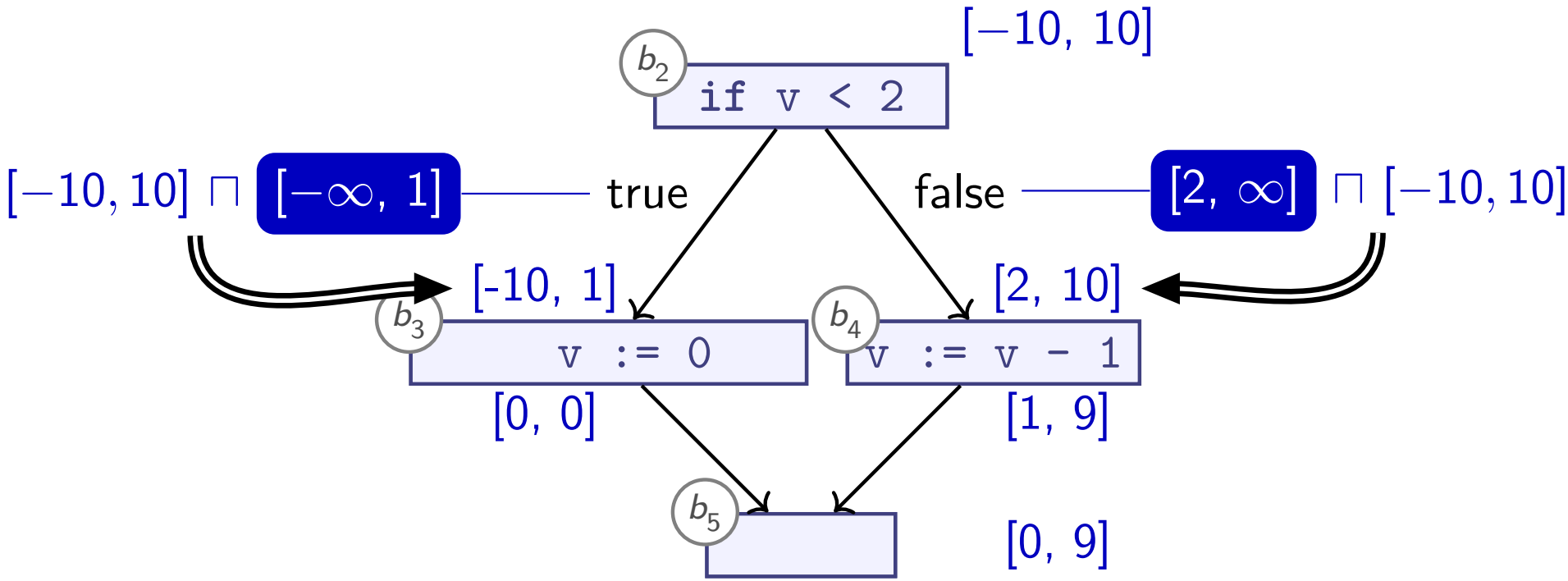
- **Control Sensitive** analysis utilises this information
  - Filter possible values

Handling Conditionals (2/2)



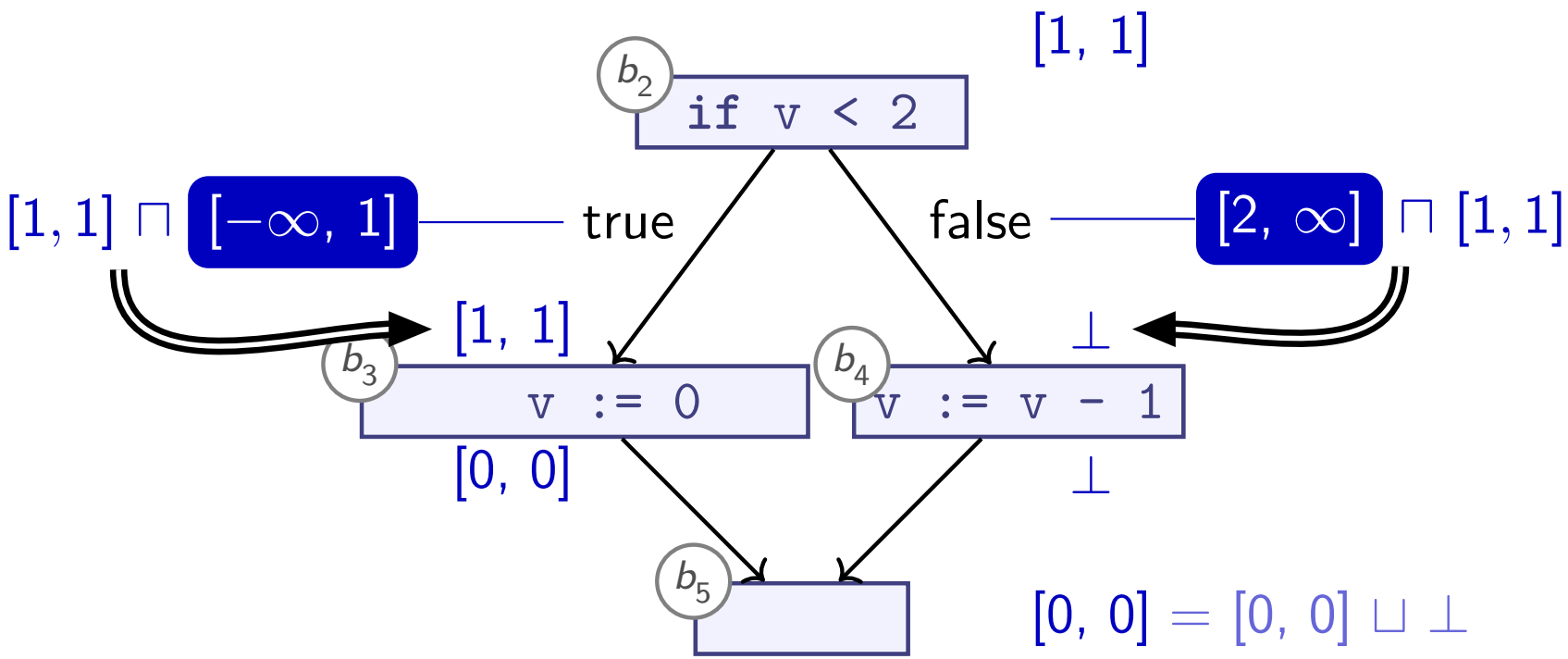
- *Idea*: Split interval for v for true/false branches
  - Analyse each branch with part of original interval
  - "Re-assemble" interval on join afterwards

Handling Conditionals (2/2)



- *Idea*: Split interval for v for true/false branches
  - Analyse each branch with part of original interval
  - "Re-assemble" interval on join afterwards
- If not $v \mapsto \top$:
  - **Filter** with lattice *meet*: $\sqcap$

Contradictions



Summary

- **Control sensitive** analysis considers conditionals:
  - May propagate different information along different edges:
    - **if** P:
    - Special transfer function for '**assert** P' on 'true' edge
    - Special transfer function for '**assert** `not` P' on 'false' edge
- More precise than **control insensitive** analysis
- Utilises *Lattice Meet* operation $\sqcap$

  Intuition: $a \sqcap b$ "satisfy a **and** b"
  $a \sqcup b$ "satisfy a **or** b"
- $a \sqcap b = \bot$ can happen: *branch will never execute*