Proof Obligations in Event-B (Refinement)

Proof obligation (PO)

- A Proof obligation (PO) is a formal property to be proved of an Event-B model

- A PO is a sequent of the form Hypotheses $\vdash$ Goal

- This means we should prove the goal while assuming that the hypotheses are true.

- The prover uses properties in the Hypotheses, applies rules and tactics, to prove the Goal

- Example

  $x < MAX \vdash x+1 \leq MAX$

  Prove that $x+1 \leq MAX$ assuming that $x < MAX$

Proof obligations in Event-B

(POs for refinement)

- Simulation (SIM)
  - update of abstract variable correctly simulated by update of concrete variable
- Guard strengthening (GRD)
  - Refined event only possible when abstract event possible
- Convergence (VAR)
  - Ensure convergence of new events using a variant
    - i.e. new events eventually become disabled and allow an old event to occur

Simulation

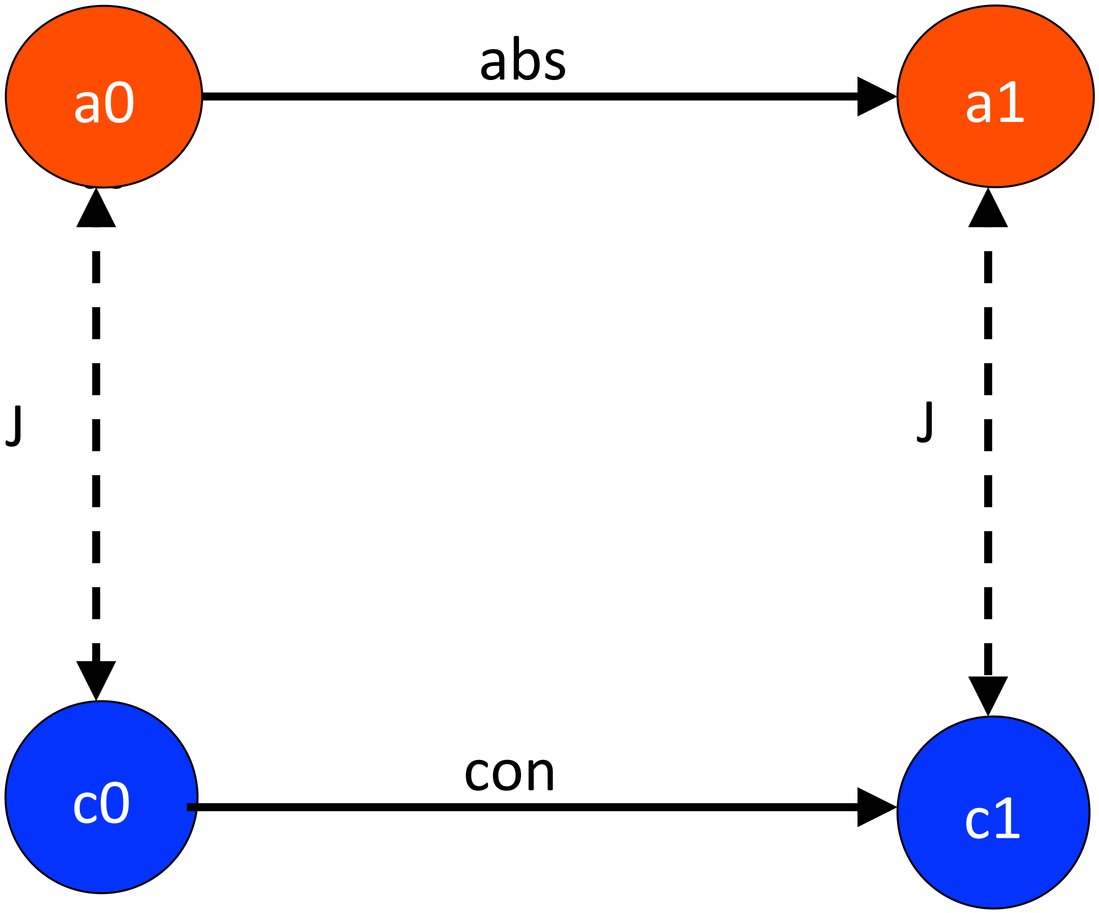
- Refinement according to the gluing relation

(The gluing invariant links the new variables to the old ones)

GRD: $I(v), J(v,w), \ldots, \quad G_r(w)$

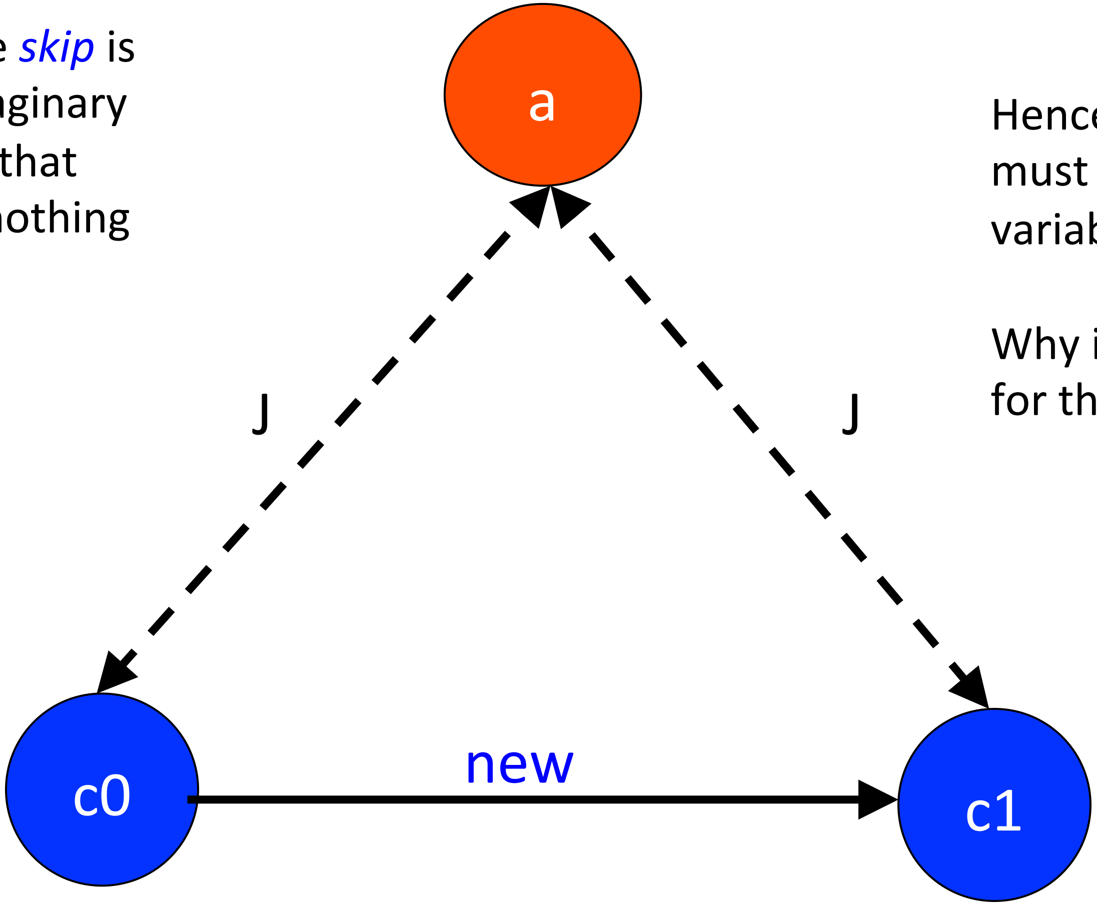
$$\vdash \quad J\,(\, exp_a(v)\,,\, exp_r(w)\,)$$

Simulation: maintaining a gluing relation



New concrete events refine *skip* (stuttering step)

Where *skip* is an imaginary event that does nothing



Hence new events must not alter old variables.

Why is there no PO for for this?

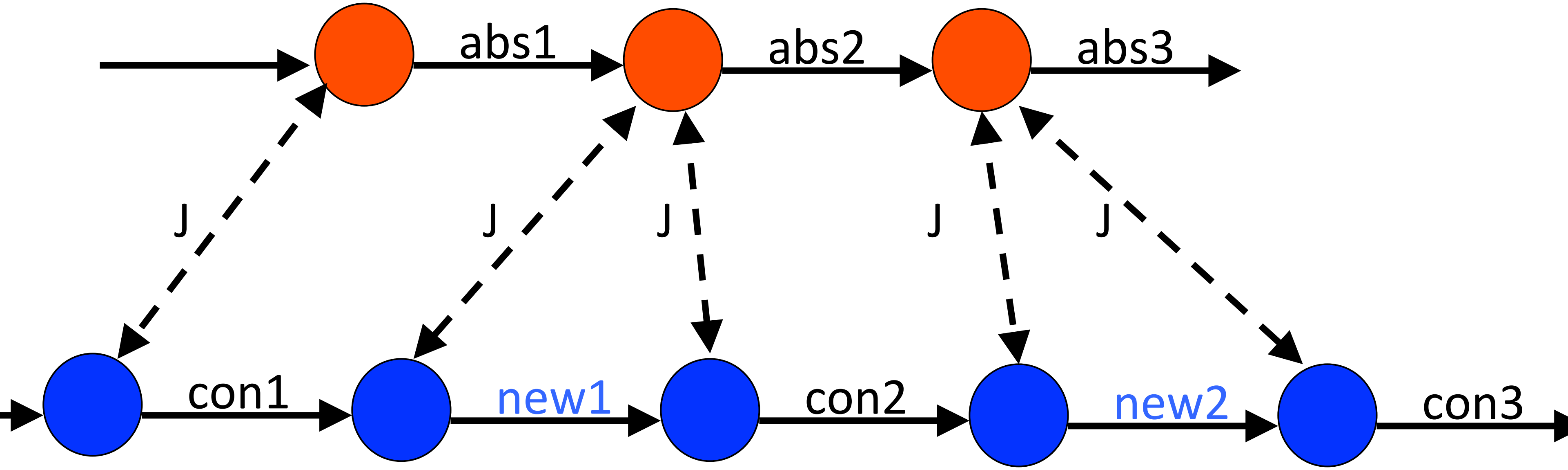
Guard Strengthening

- We need to prove that the guard of a refined event is not weaker than the guard of the abstract event.

GRD: $I(v), J(v,w), G_r(w) \vdash G_a(v)$

- Why can't guards be weakened?

Refining traces



A concrete trace must correspond to an abstract trace (omitting new events).

Hence guards must not be weakened otherwise new traces are introduced