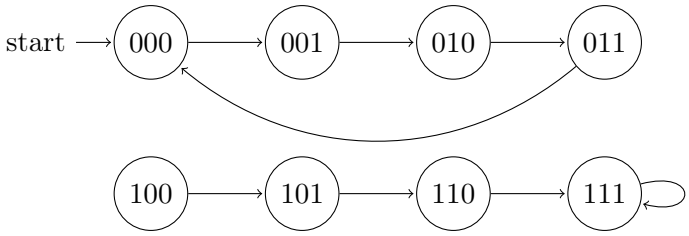
Exercises to the lecture
Semantics
Sheet 4

Prof. Dr. Roland Meyer
Jan Grünke Delivery until 15.05.2025 at 16:15

Exercise 4.1 (IC3)
Consider the following transition system in which states:



Use IC3 to prove that the $Bad := x_1 \wedge x_2 \wedge x_3$ is unreachable. Give at least the sequence of frames and bad states at each iteration. You may apply any generalization to eliminate the counterexample to induction (CTI). If you do so, demonstrate that your generalization is relatively inductive.

Exercise 4.2 (Incremental Proofs)
Let Σ be the set of states in a transitions system. Recall that a set $R \subseteq \Sigma$ is a relative inductive invariant wrt. S if $Init \subseteq R$ and $post(S \cap R) \subseteq R$.

(a) Let I be an inductive invariant and R be relative inductive wrt. to I. Show that $R \cap I$ is an inductive invariant.

(b) Consider the program p, given by

```
1: x := 1
2: y := 1
3: while true do
4:     x := x + y
5:     y := y + 1
6: end while
```

Our goal is to prove that the program p satisfies the safety property $P := x \geq 0$ *incrementally*, assuming the initial states satisfy $Init := x \geq 0 \wedge y \geq 0$.

(b.1) Show that P is not an inductive invariant.

(b.2) Prove that P holds by providing an inducive invariant I_y that involves only the variable y and a relative inductive invariant I_x wrt. I_y that involves only the variable x.

(b.3) Is it still possible to prove P incrementally if you replace line 5 by $y := y + x$? *Hint: Does (a) still holds if I would only be relative inductive to R?*