Safety Control

EECS 20

Lecture 36 (April 23, 2001)

Tom Henzinger

Revised by Matteo Zavatteri and Tiziano Villa, Fall 2020

The Control Problem

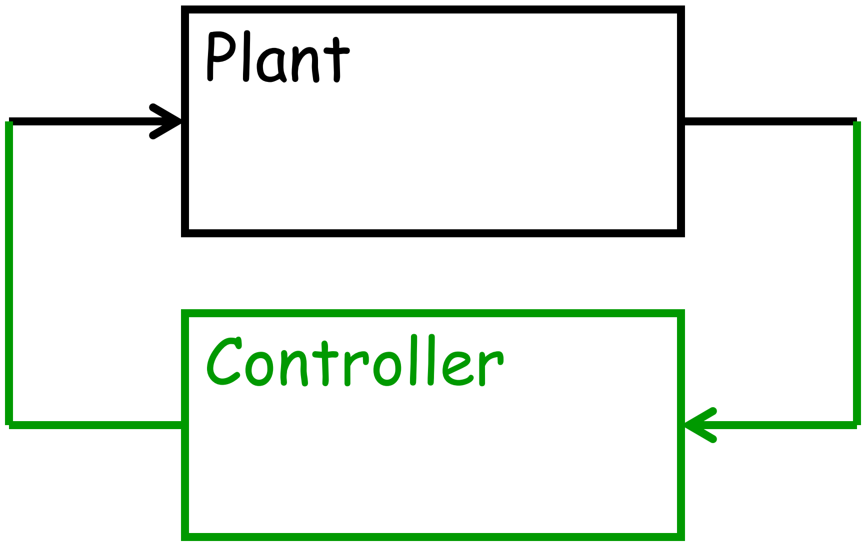
Given

1.

2. Objective

The Control Problem

Find



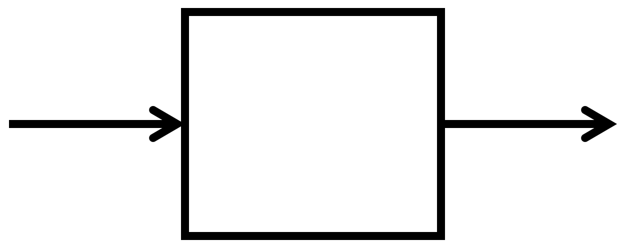
such that the composite ("closed-loop") system satisfies the Objective

Simple Control Problems

1. LTI Plant
2. Finite-State Plant

Even Simple Linear Systems are Not Finite-State

$x: Nats_0 \to Reals$

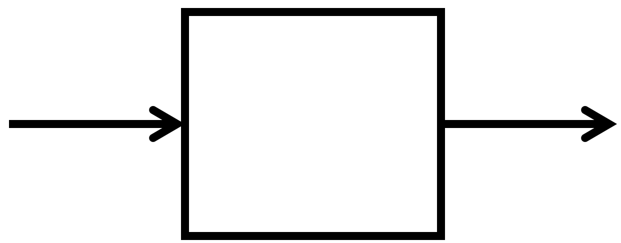


$y: Nats_0 \to Reals$

$$\forall\ z \in Nats_0,\ \ y(z) = \begin{cases} 0 & \text{if } z=0 \\ \frac{1}{2} \cdot (x(z-1) + x(z)) & \text{if } z>0 \end{cases}$$

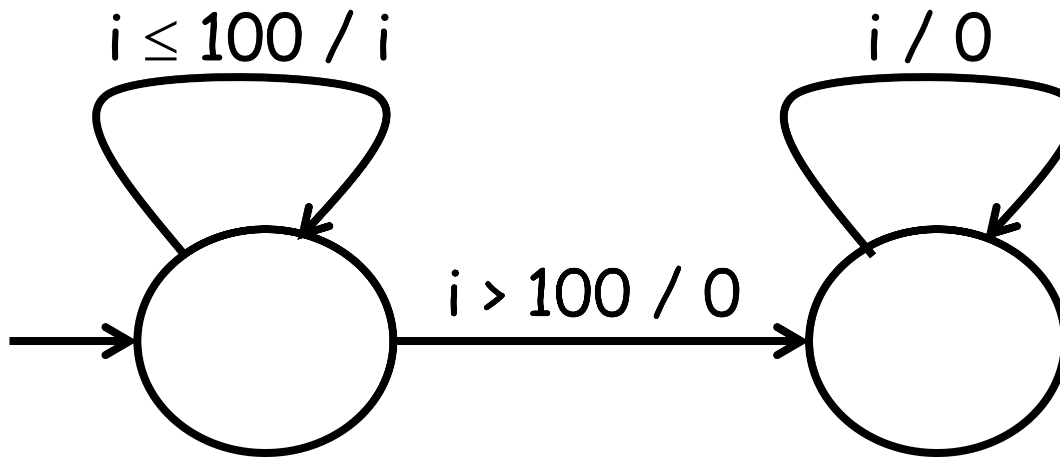
Even Simple Finite-State Systems are Not Linear

$x: \text{Nats}_0 \to \text{Reals}$



$y: \text{Nats}_0 \to \text{Reals}$

$$\forall\, z \in \text{Nats}_0,\ \ y(z) = \begin{cases} x(z) & \text{if } \forall\, z' \le z,\ \ x(z') \le 100 \\ 0 & \text{if } \exists\, z' \le z,\ \ x(z') > 100 \end{cases}$$



("i" stands for any input value)

Simplest Finite-State Control Objective:

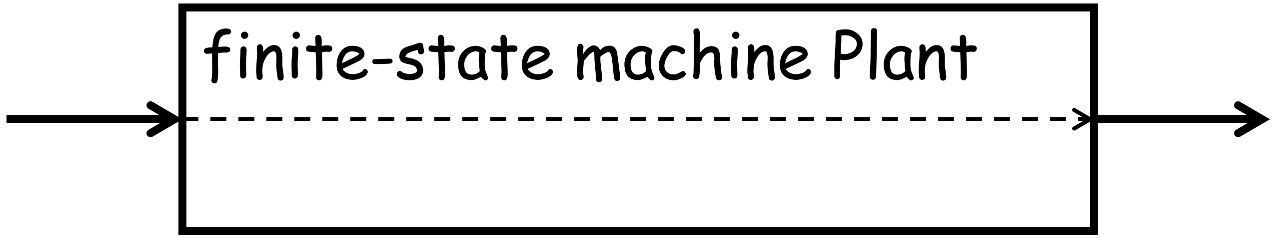
SAFETY

stay out of a set of undesirable plant states
(the “error” states)

The Finite-State Safety Control Problem

Given

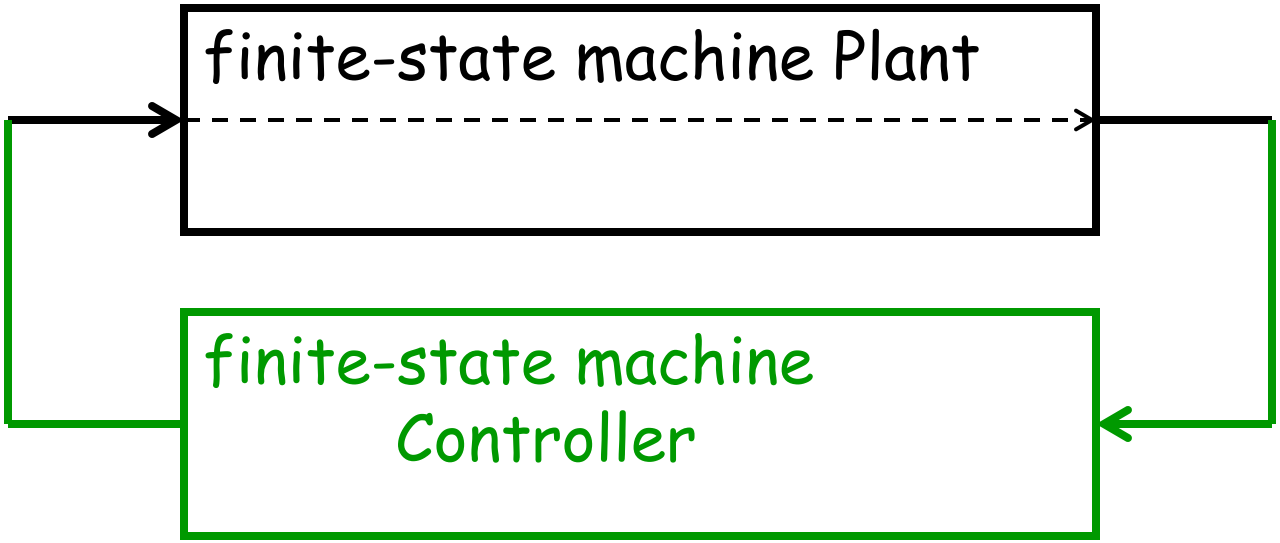
1.



2. set Error of states of Plant

The Finite-State Safety Control Problem

Find



such that the composite system never enters a state in Error

Step 1:

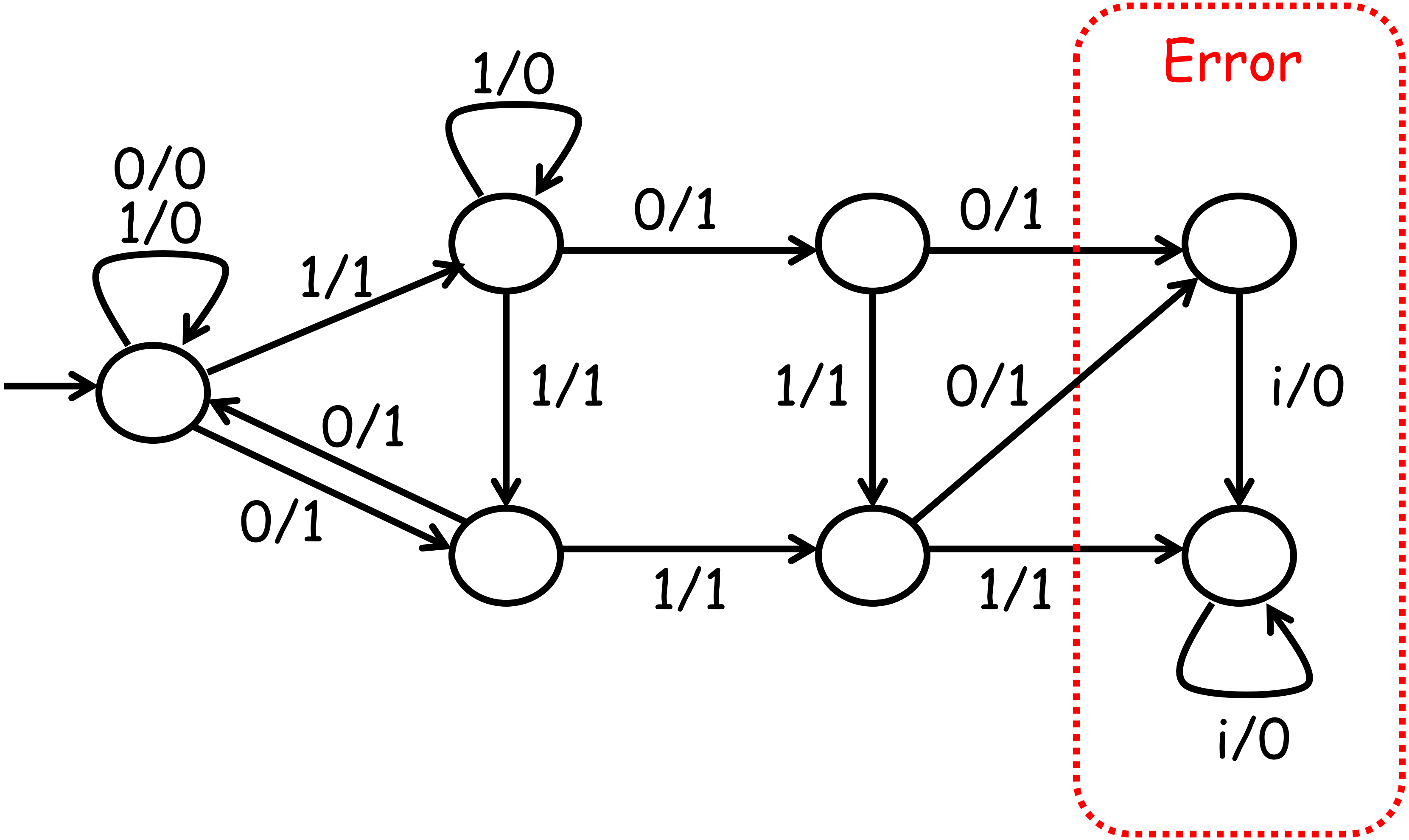
Compute the "uncontrollable" states of Plant

1. Every state in Error is uncontrollable.
2. For all states s,

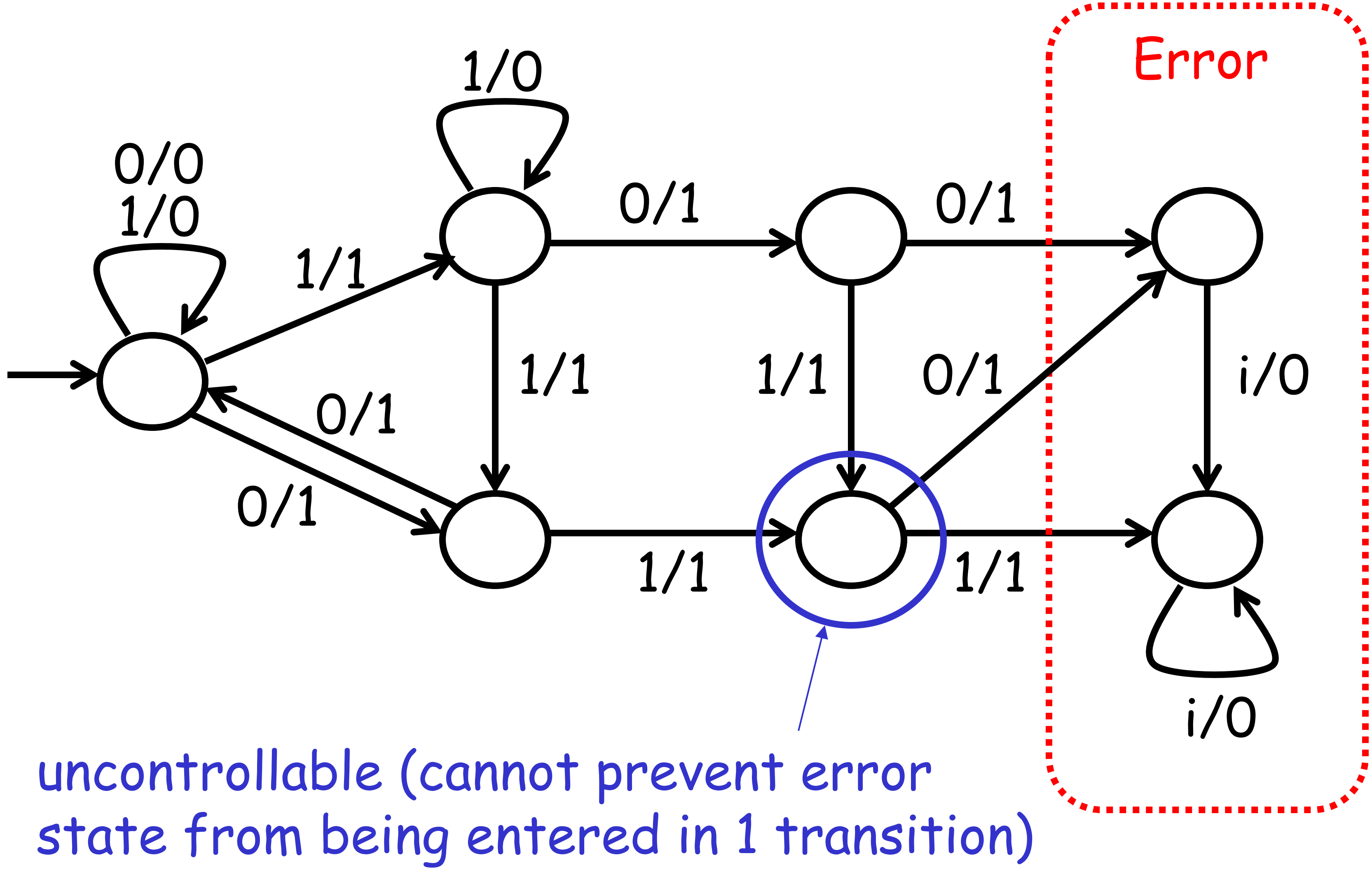
   if for all inputs i
   there exist an uncontrollable state s'
   and an output o
   such that (s',o) ∈ possibleUpdates (s,i)

   then s is uncontrollable.

Plant

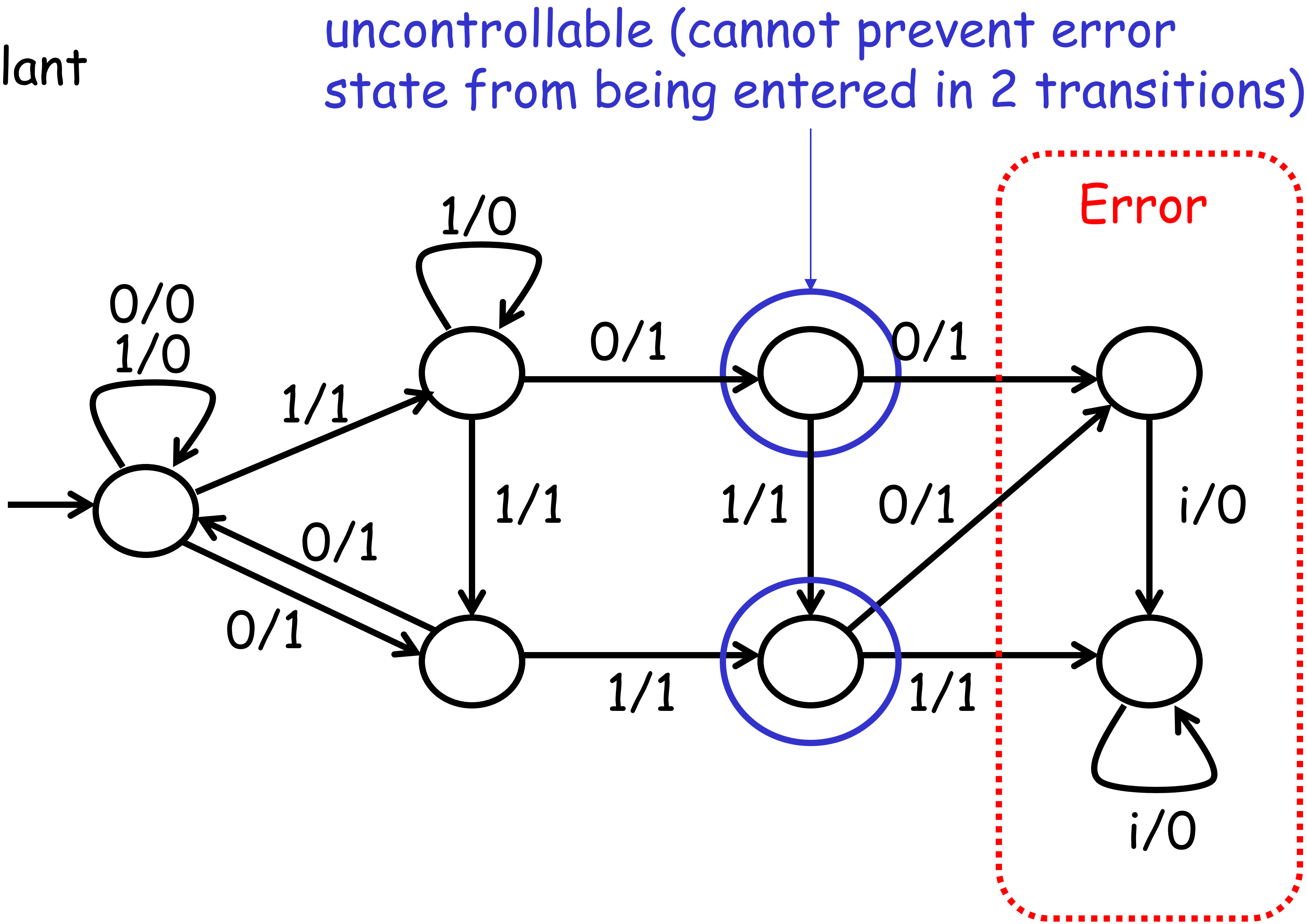


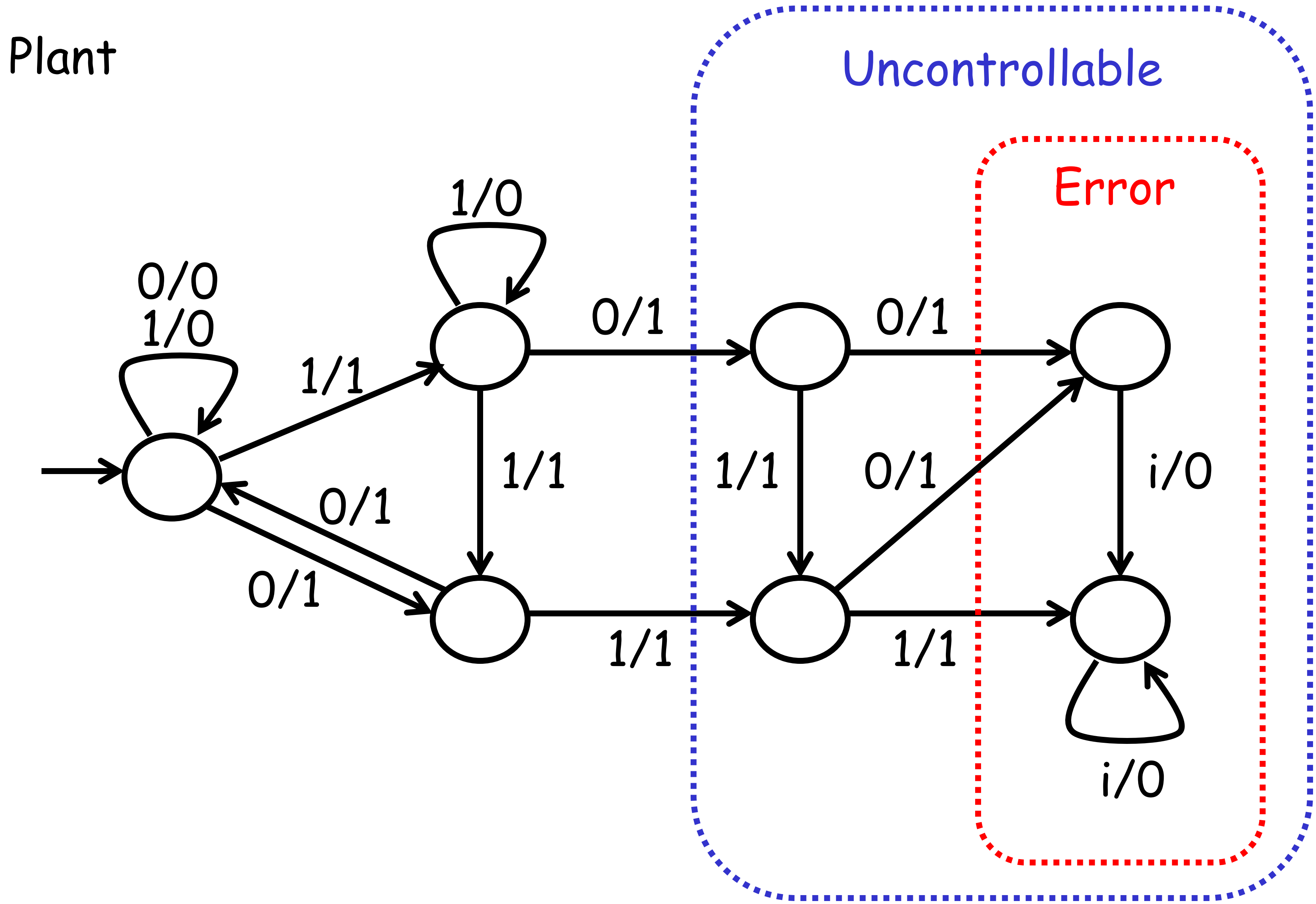
Plant

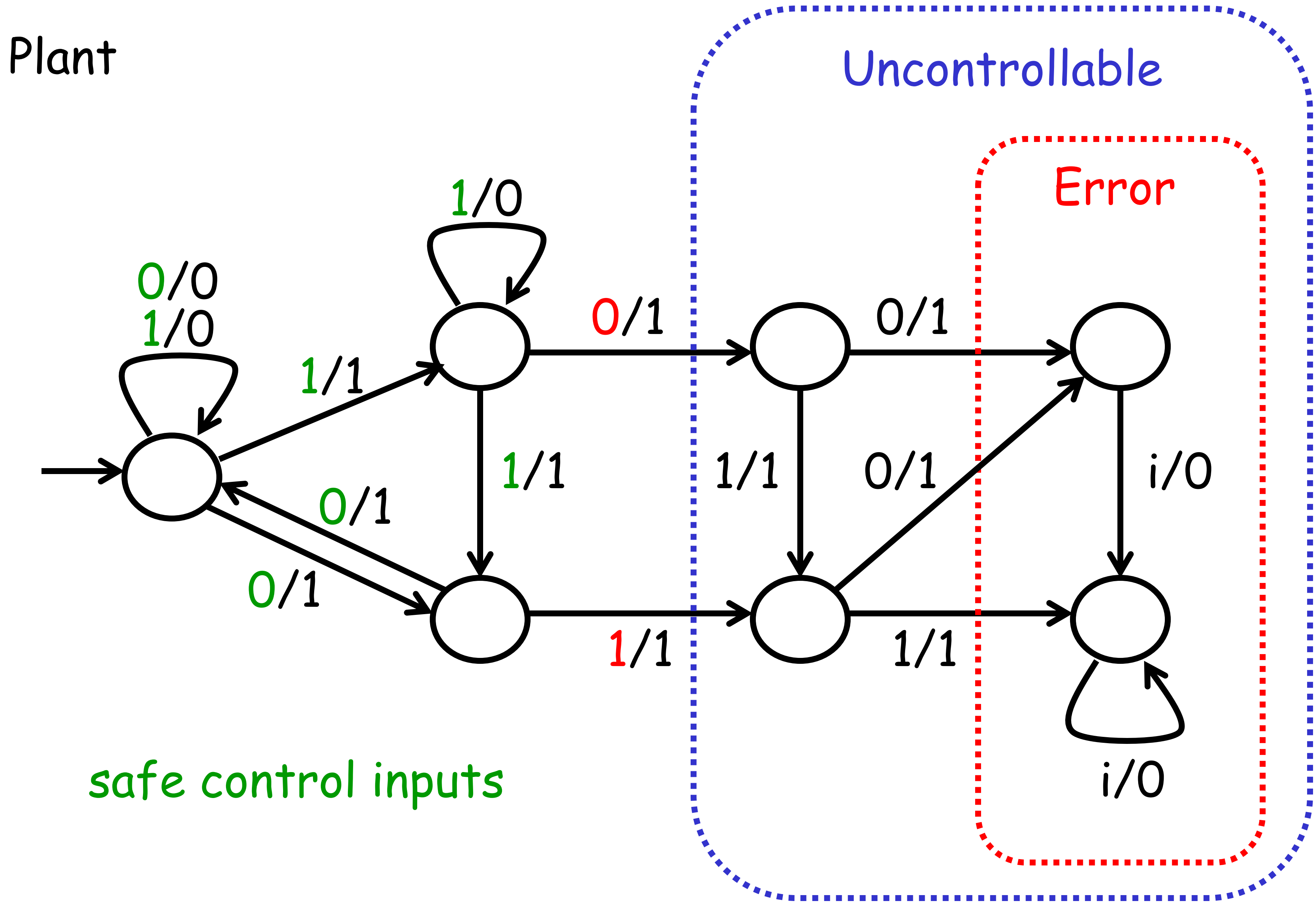


Error
0/0
1/0
1/0
1/1
0/1
0/1
0/1
0/1
1/1
1/1
0/1
i/0
1/1
1/1
i/0
uncontrollable (cannot prevent error state from being entered in 1 transition)

Plant


uncontrollable (cannot prevent error state from being entered in 2 transitions)
Error
0/0
1/0
1/0
1/1
0/1
0/1
0/1
1/1
1/1
1/1
0/1
0/1
1/1
i/0
i/0


Plant
Uncontrollable
Error
1/0
0/0
1/0
1/1
0/1
0/1
1/1
0/1
0/1
1/1
0/1
i/0
1/1
1/1
i/0

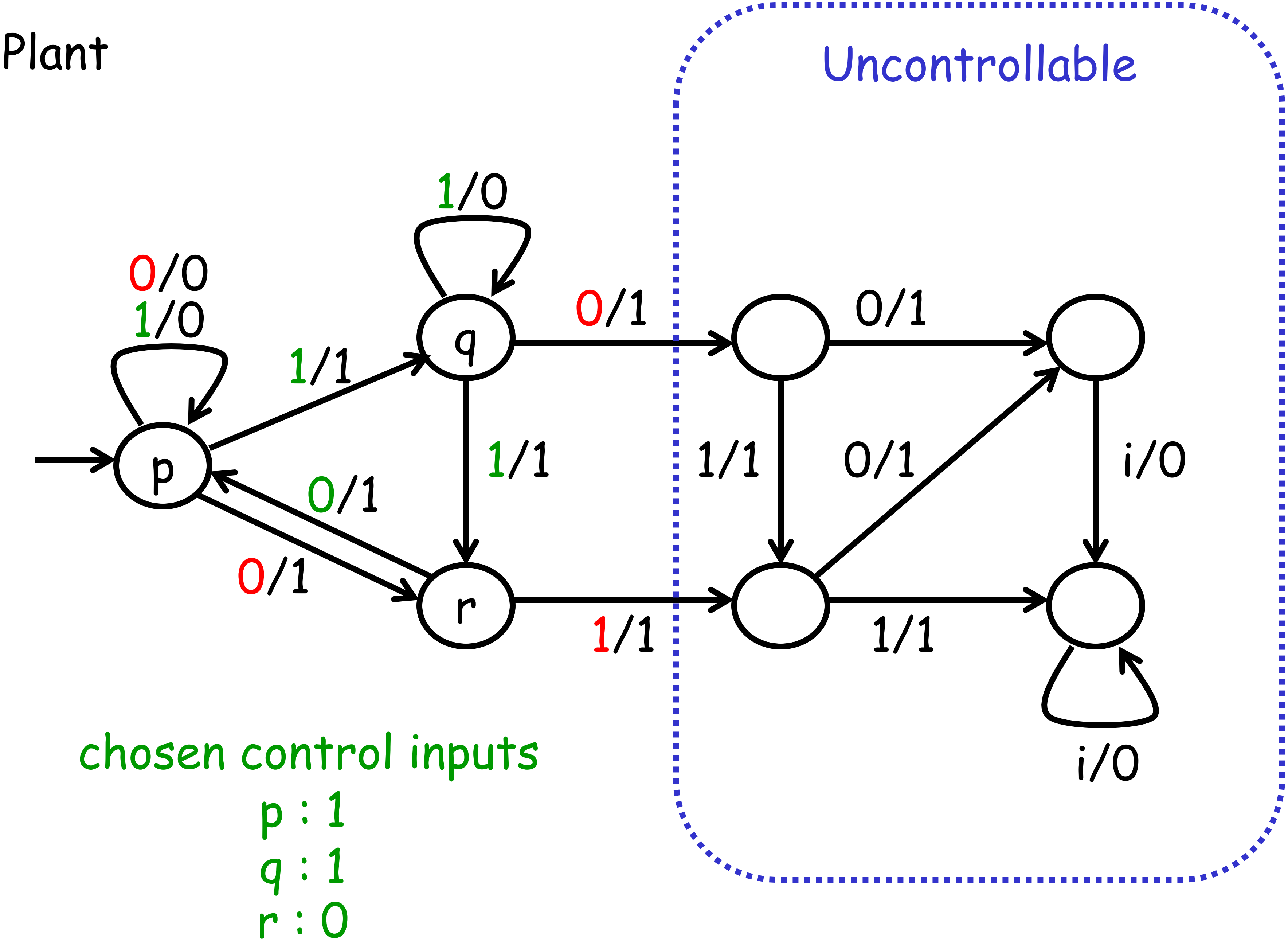


Plant
Uncontrollable
Error
0/0
1/0
1/0
1/1
0/1
0/1
0/1
1/1
1/1
0/1
1/1
0/1
1/1
i/0
i/0
safe control inputs

Step 2:

Design the Controller

1. For each controllable state s of the plant, choose one input i so that possibleUpdates (s,i) contains only controllable states.



Plant
Uncontrollable
0/0
1/0
1/0
1/1
0/1
0/1
1/1
0/1
1/1
0/1
1/1
0/1
i/0
1/1
i/0
p
q
r
chosen control inputs
p : 1
q : 1
r : 0

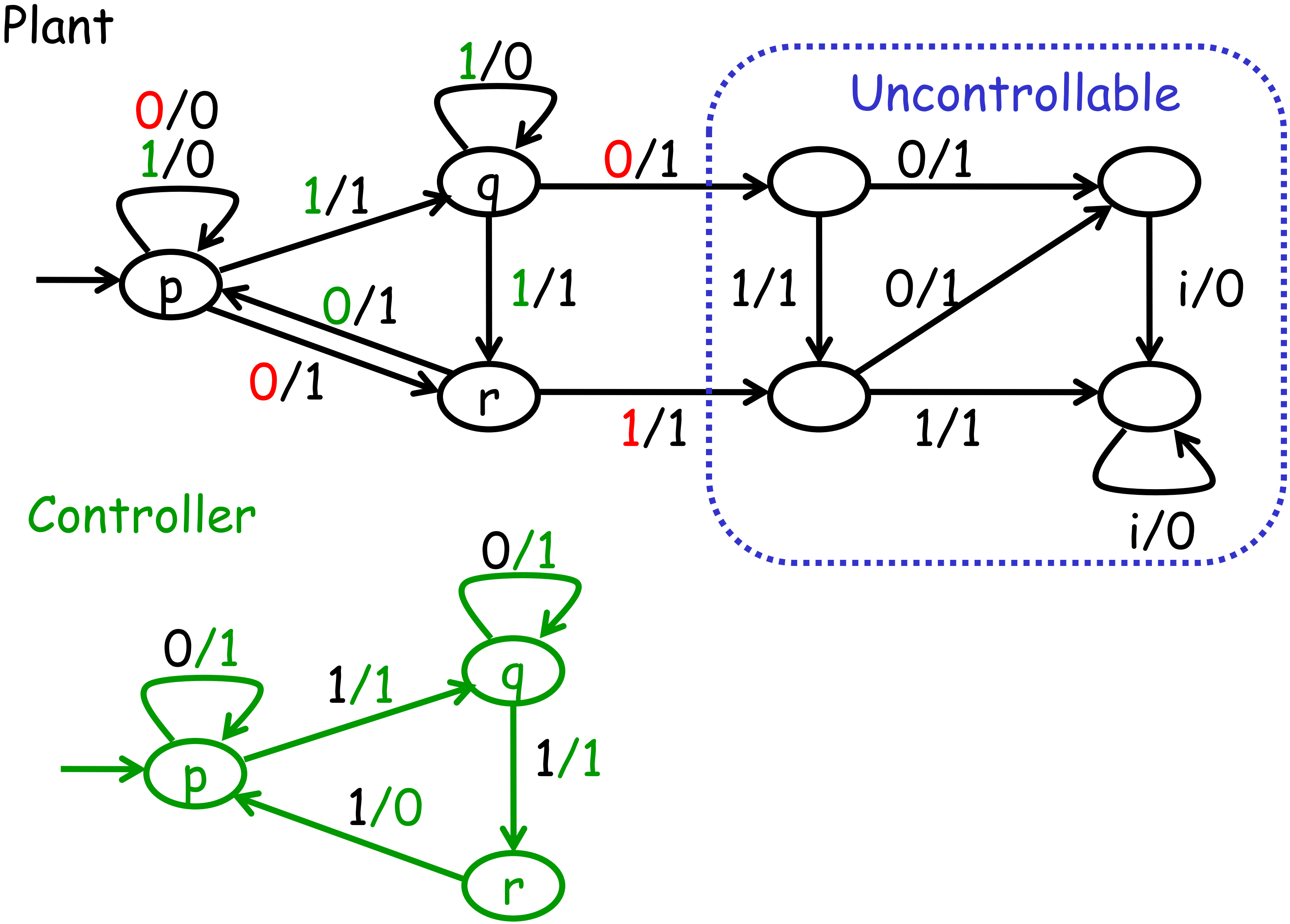
Step 2:

Design the Controller

1. For each controllable state s of the plant, choose one input i so that possibleUpdates (s,i) contains only controllable states.

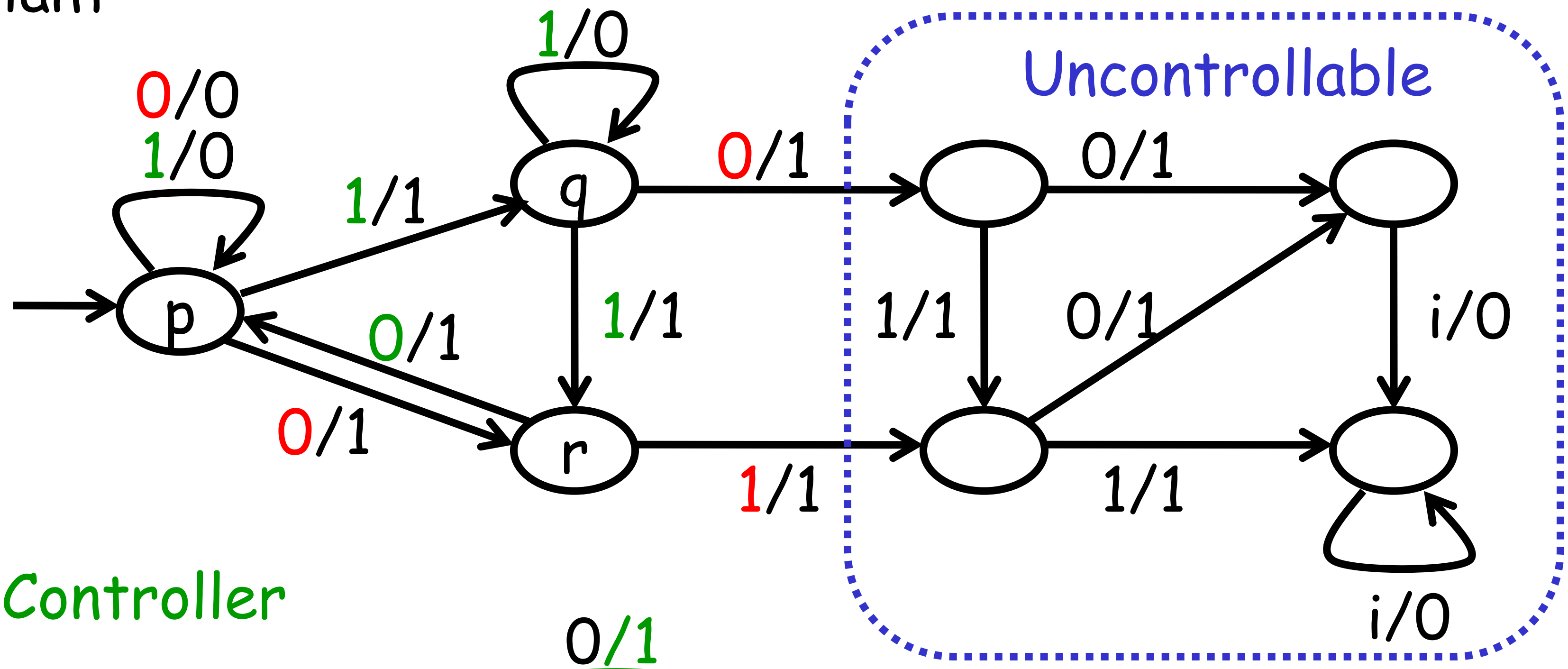
2. Have the Controller keep track of the state of the Plant:

   If Plant is output-deterministic,
   then Controller looks exactly like the controllable part of Plant, with inputs and outputs swapped.

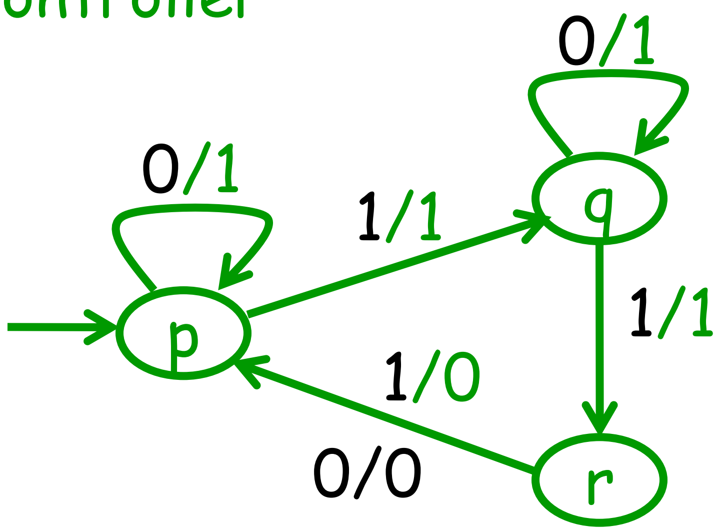


Plant
Uncontrollable
0/0
1/0
1/1
1/0
0/1
1/1
0/1
0/1
0/1
1/1
1/1
0/1
i/0
1/1
1/1
i/0
Controller
0/1
0/1
1/1
1/1
1/0
p
q
r
p
q
r

Plant



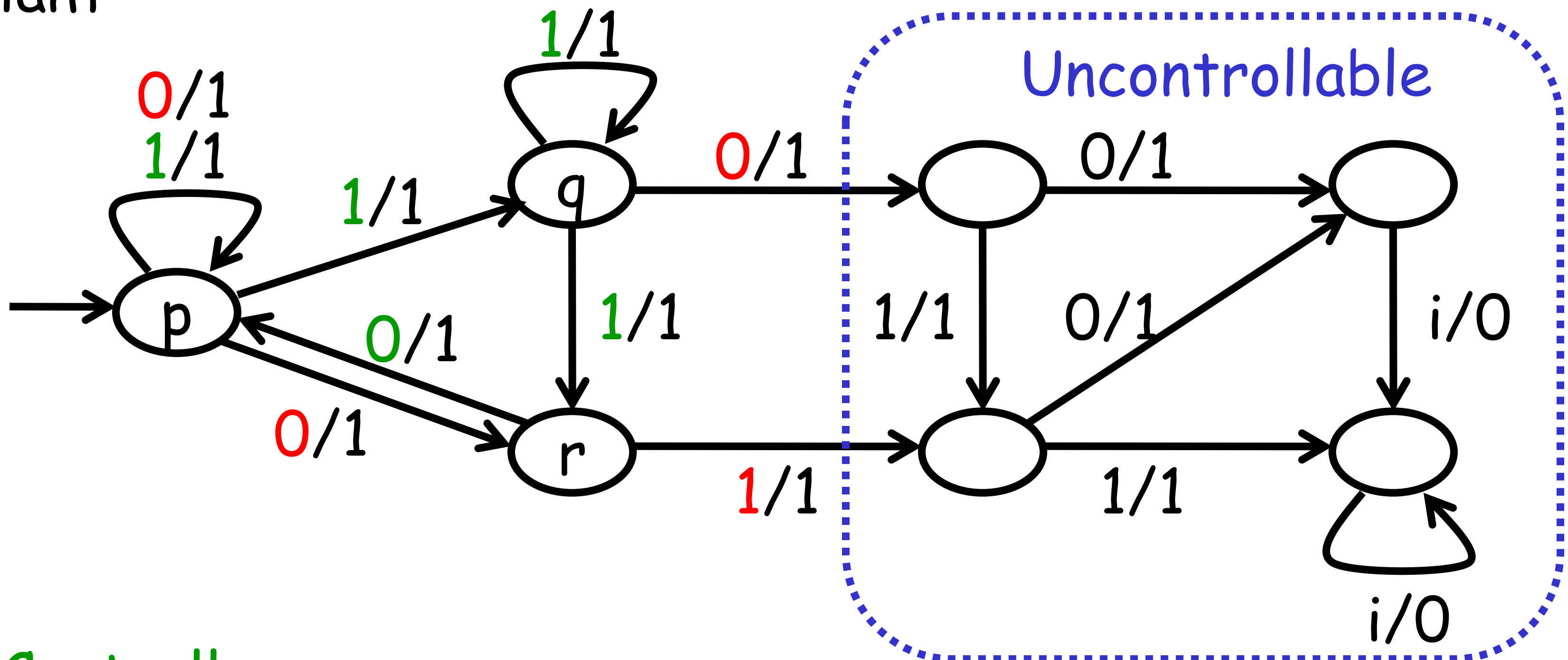
Controller



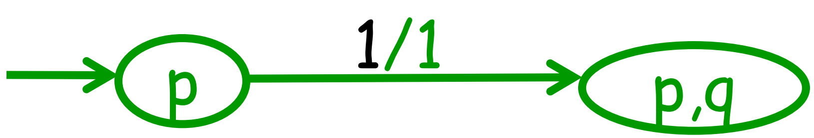
(the Controller can be made receptive in any way)

What if the Plant is not output-deterministic?

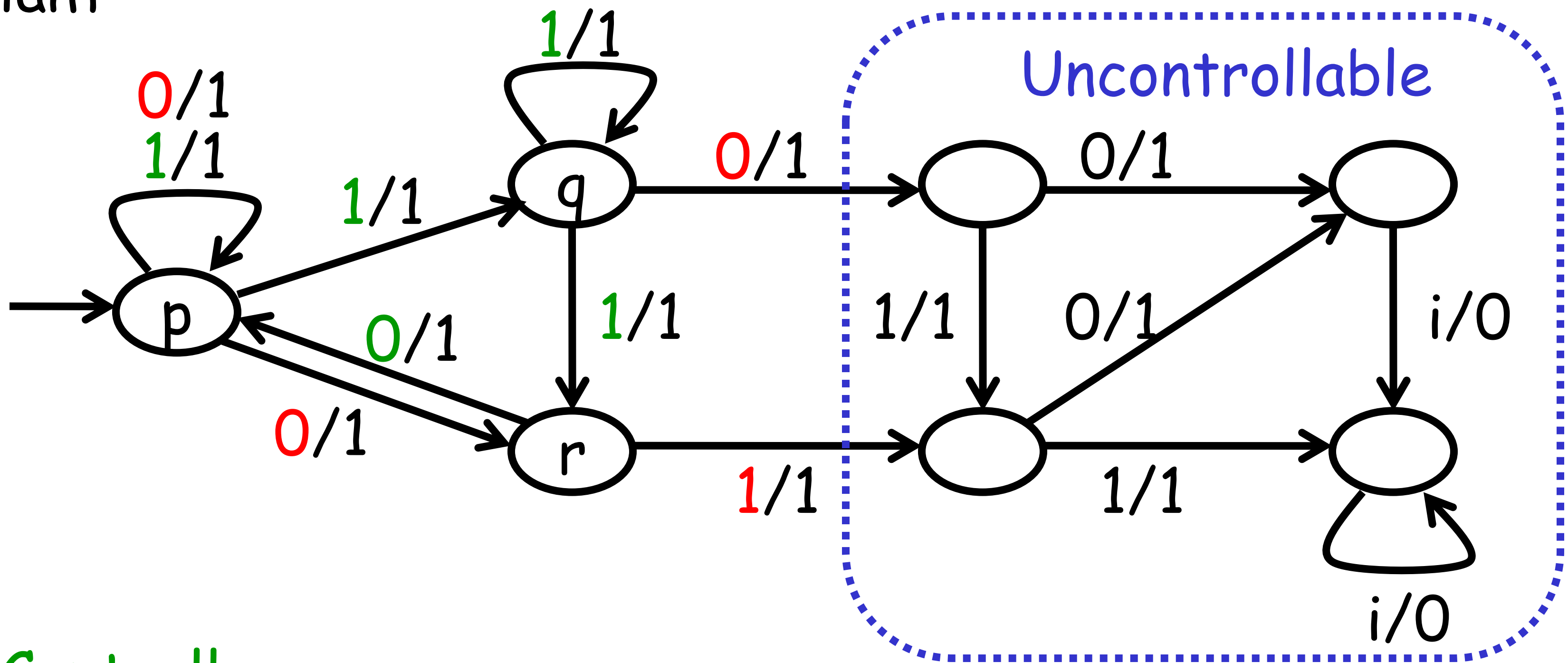
Plant



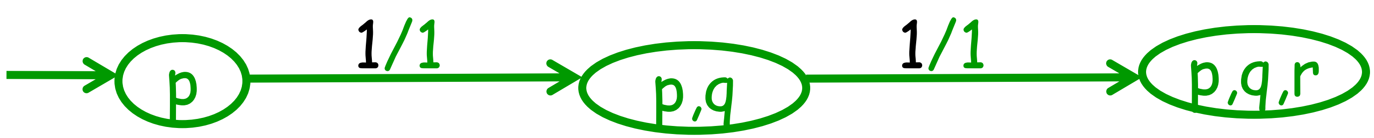
Controller



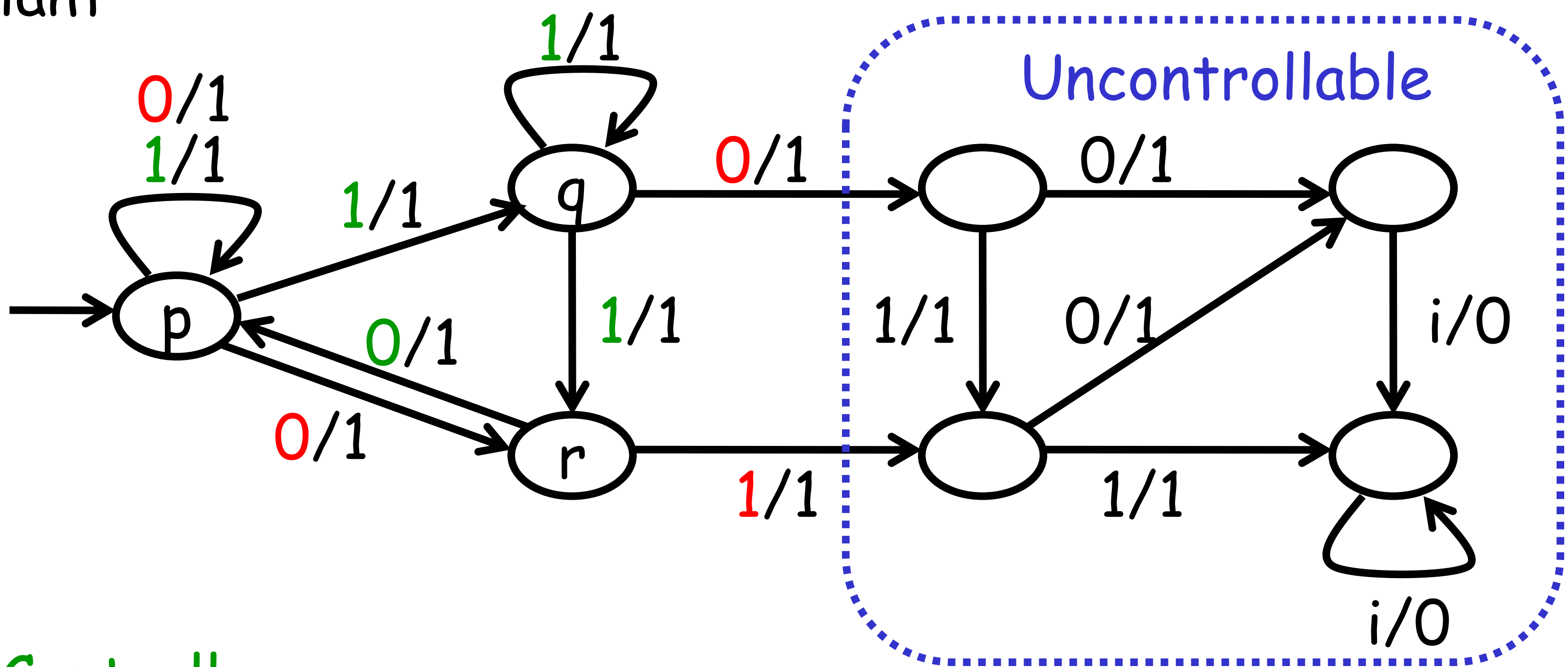
Plant



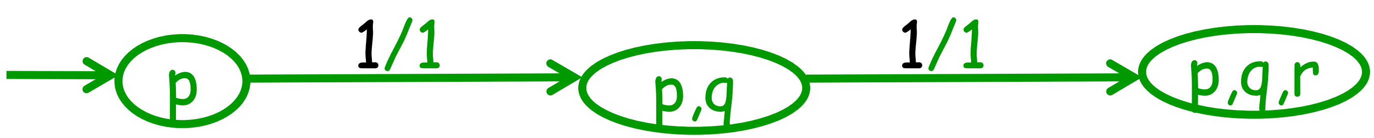
Controller



Plant

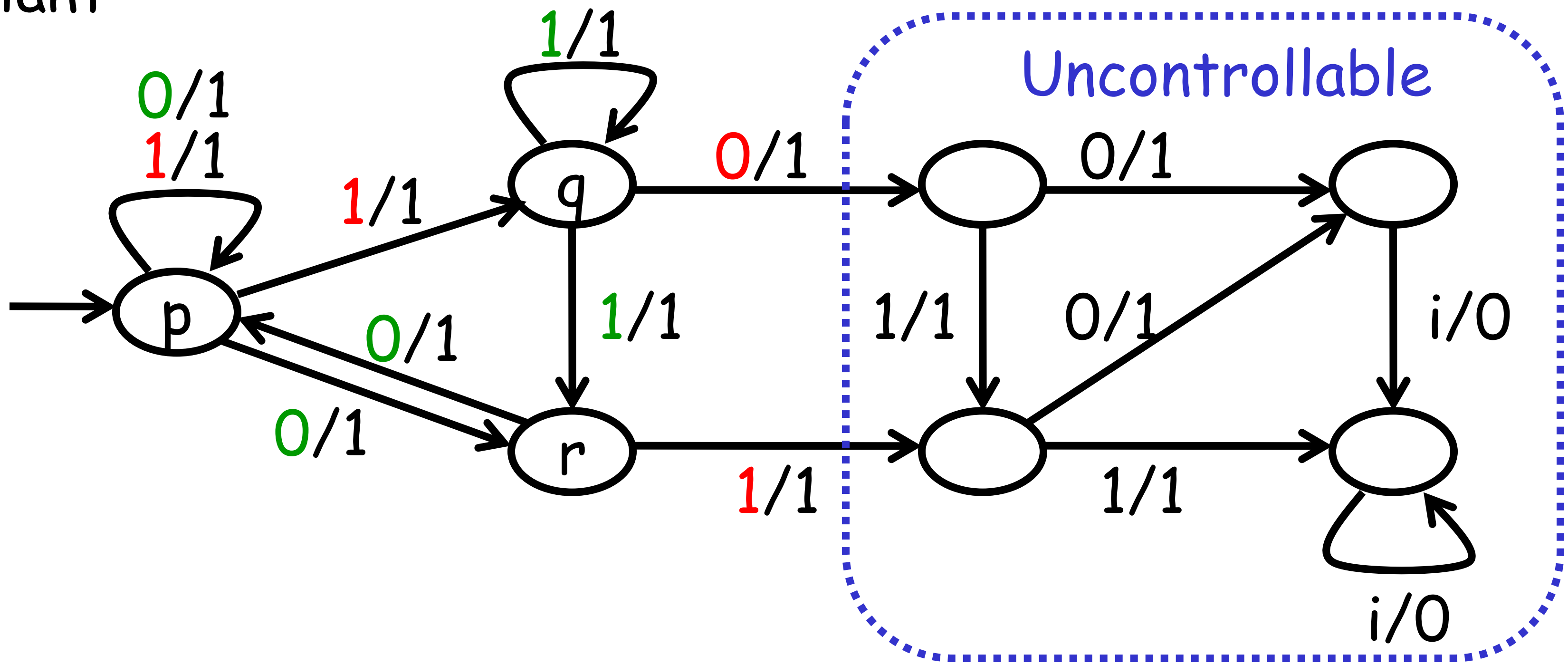


Controller

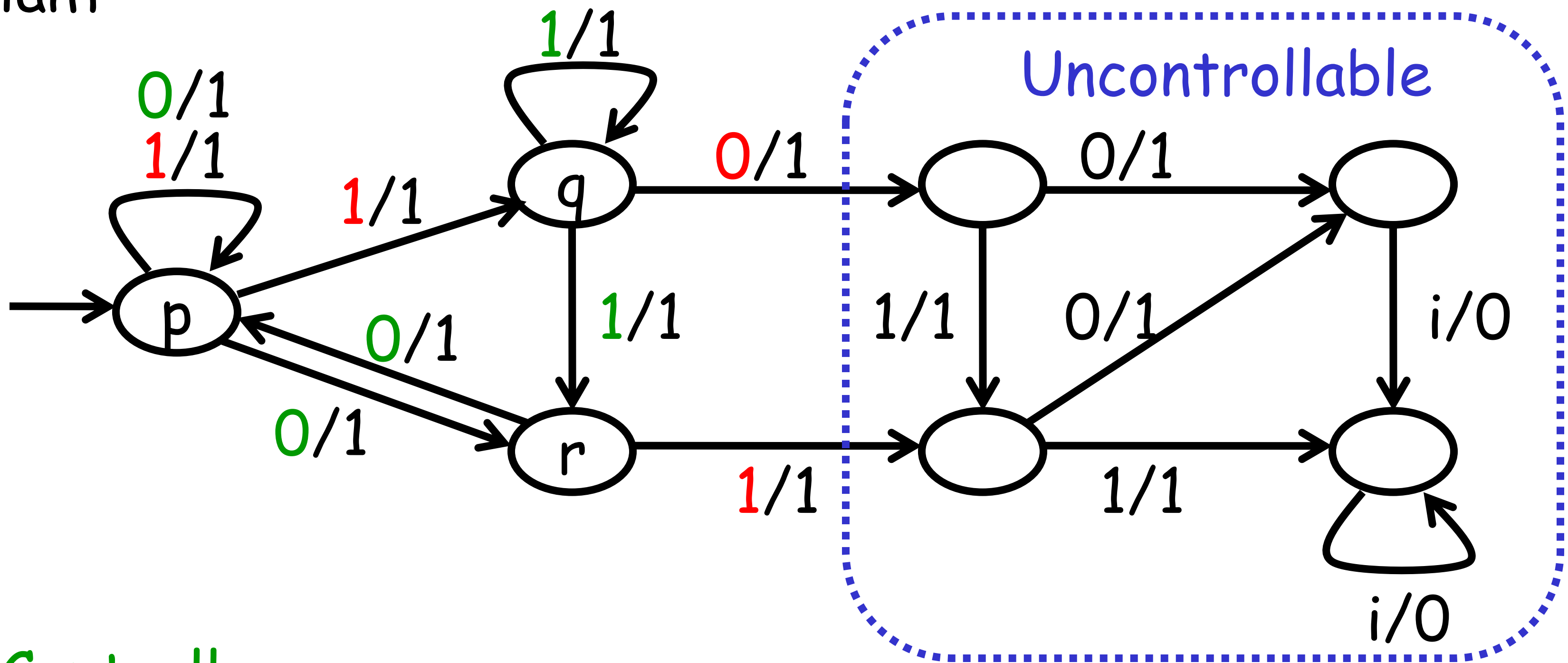


Neither 0 nor 1 is safe !

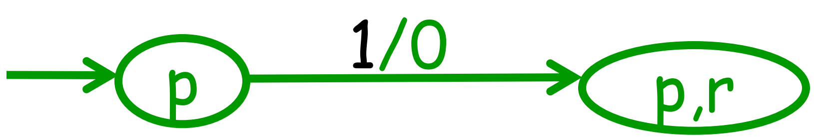
Plant



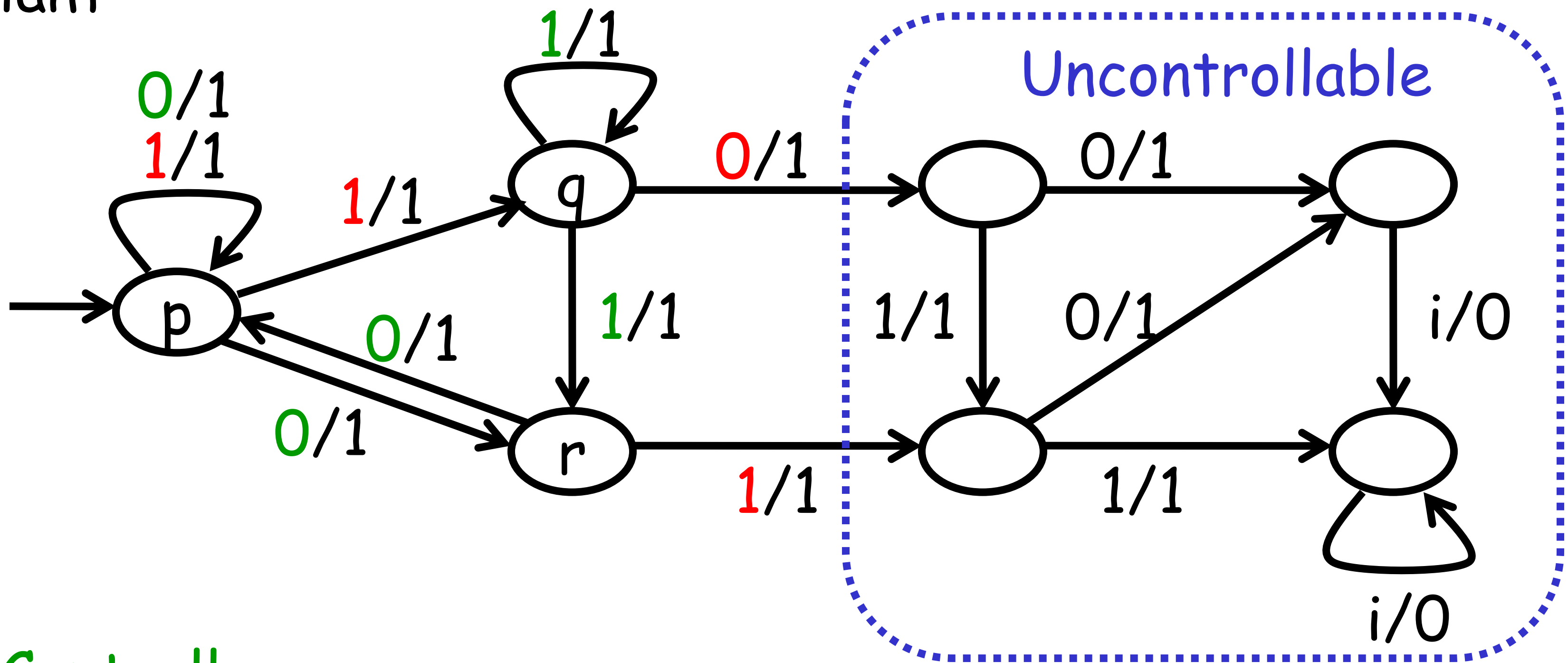
Plant



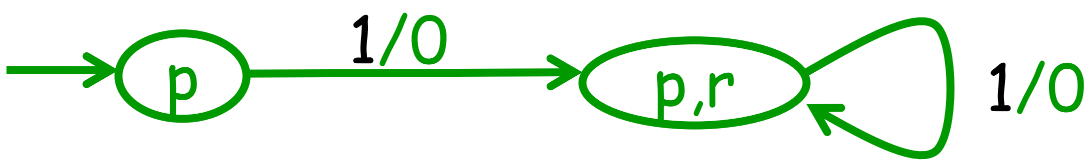
Controller



Plant



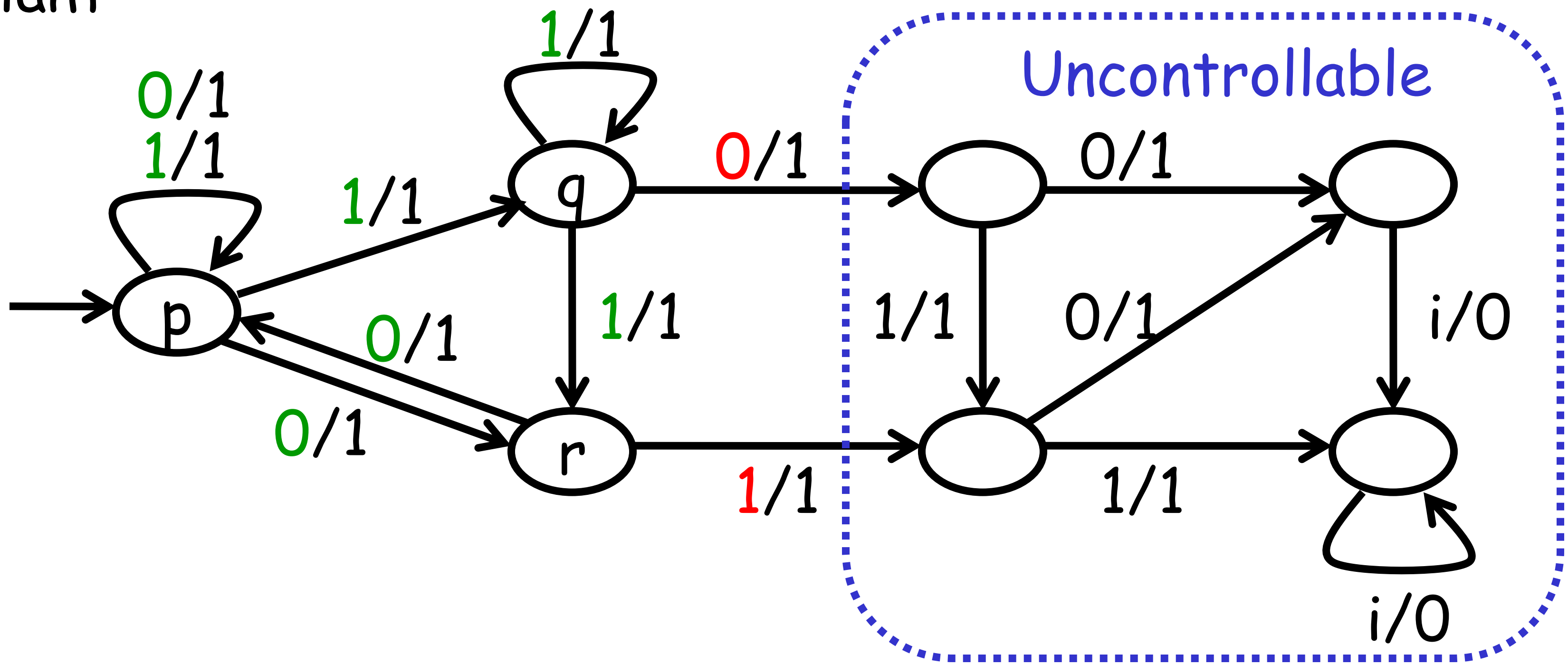
Controller



Step 2: Design the Controller

1. Let Controllable be the controllable states of the Plant. A subset $S \subseteq$ Controllable is consistent if there is an input i such that for all states $s \in S$, all states in possibleUpdates (s,i) are controllable.
2. Let M be the state machine whose states are the consistent subsets of Controllable. Prune from M the states that have no successor, until no more states can be pruned.
3. If the result contains possibleInitialStates (of the plant) as a state, then it is the desired Controller. Otherwise, no controller exists.

Plant

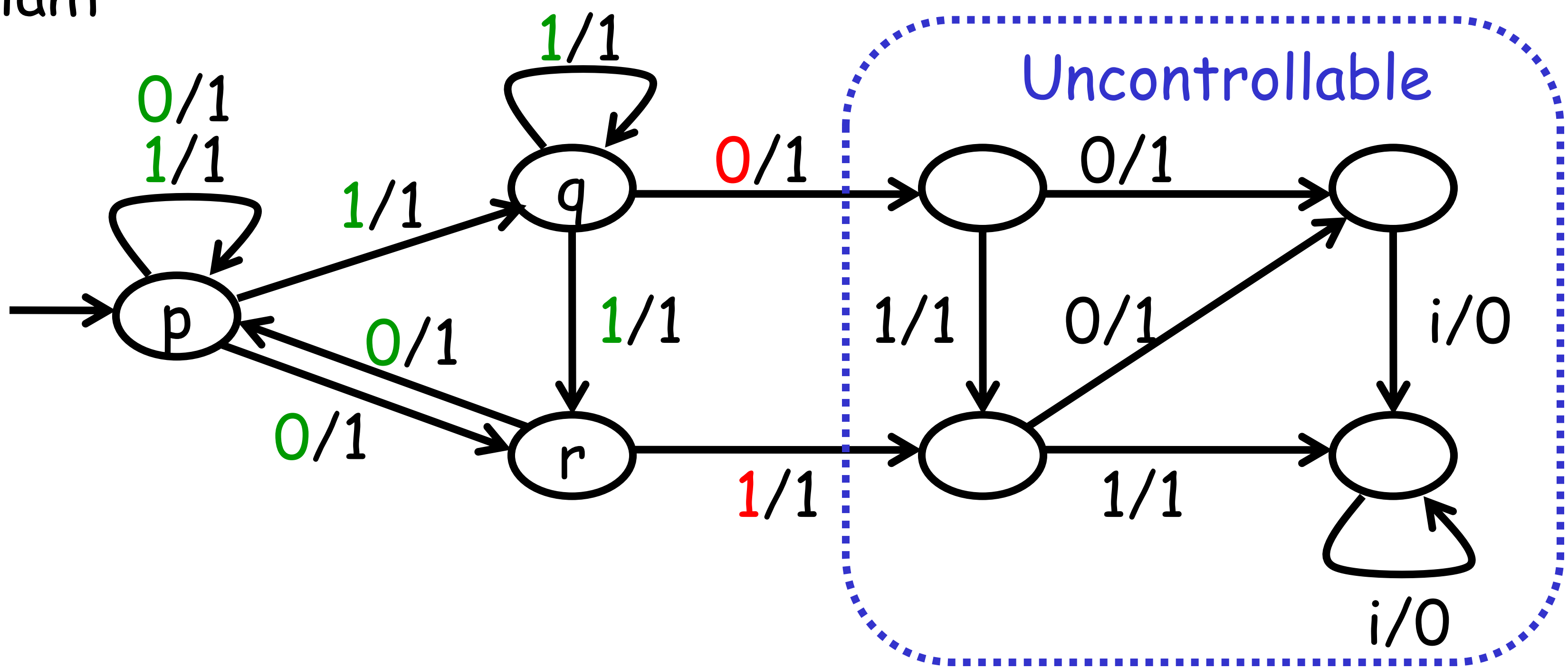


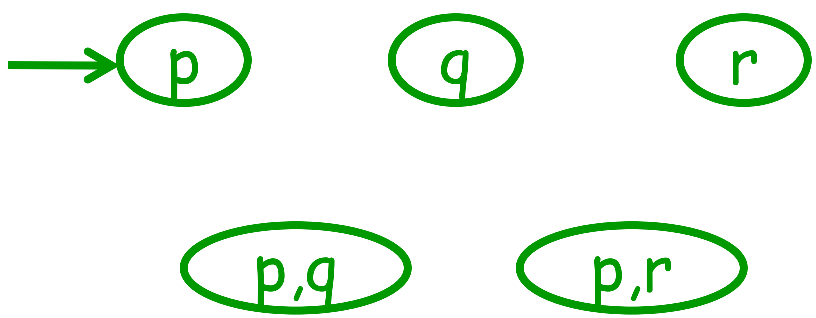
Consistent subsets

{p} : 0, 1
{q} : 1
{r} : 0

{p,q} : 1
{p,r} : 0
{q,r}, {p,q,r} not consistent

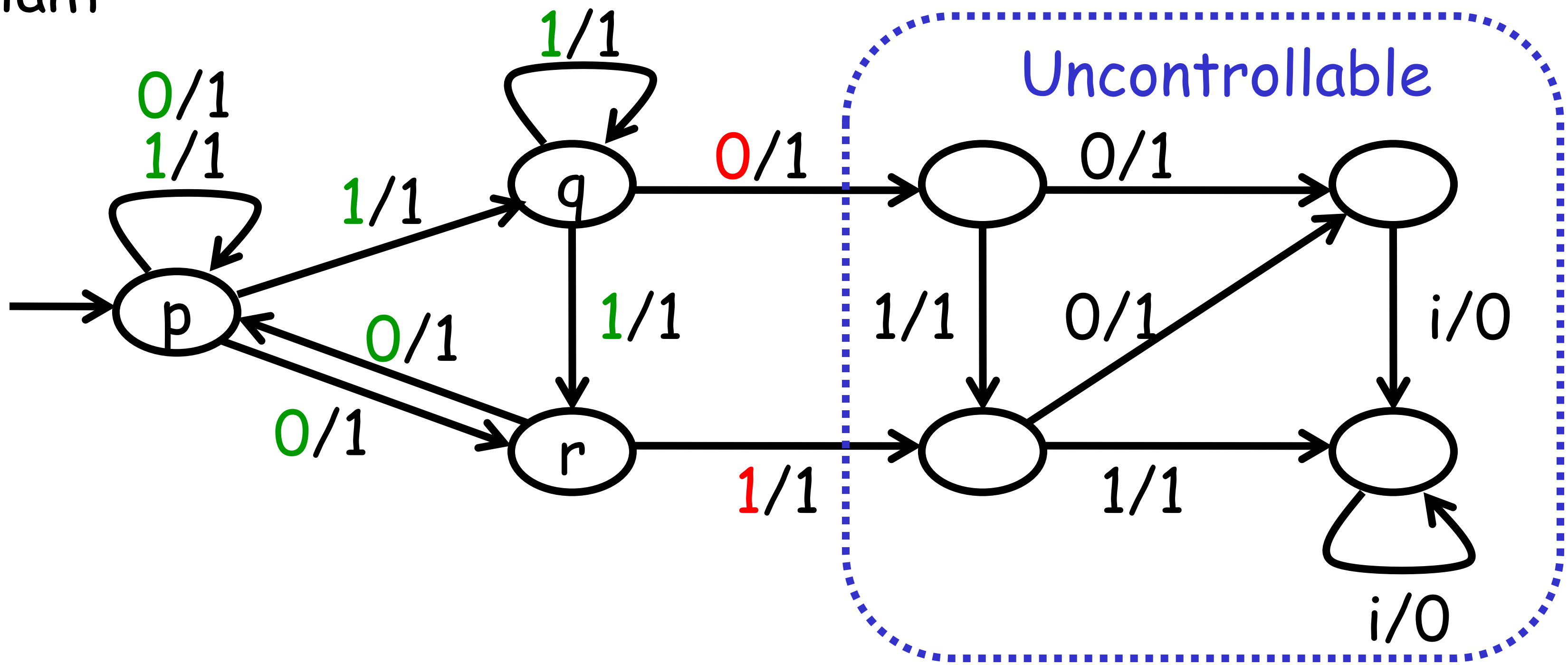
Plant

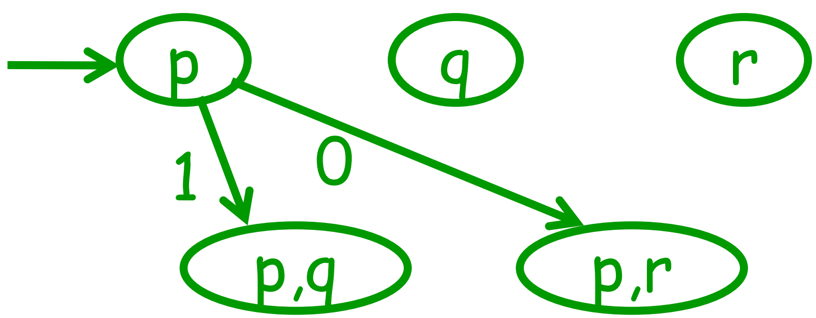




{p} : 0, 1
{q} : 1
{r} : 0
{p,q} : 1
{p,r} : 0

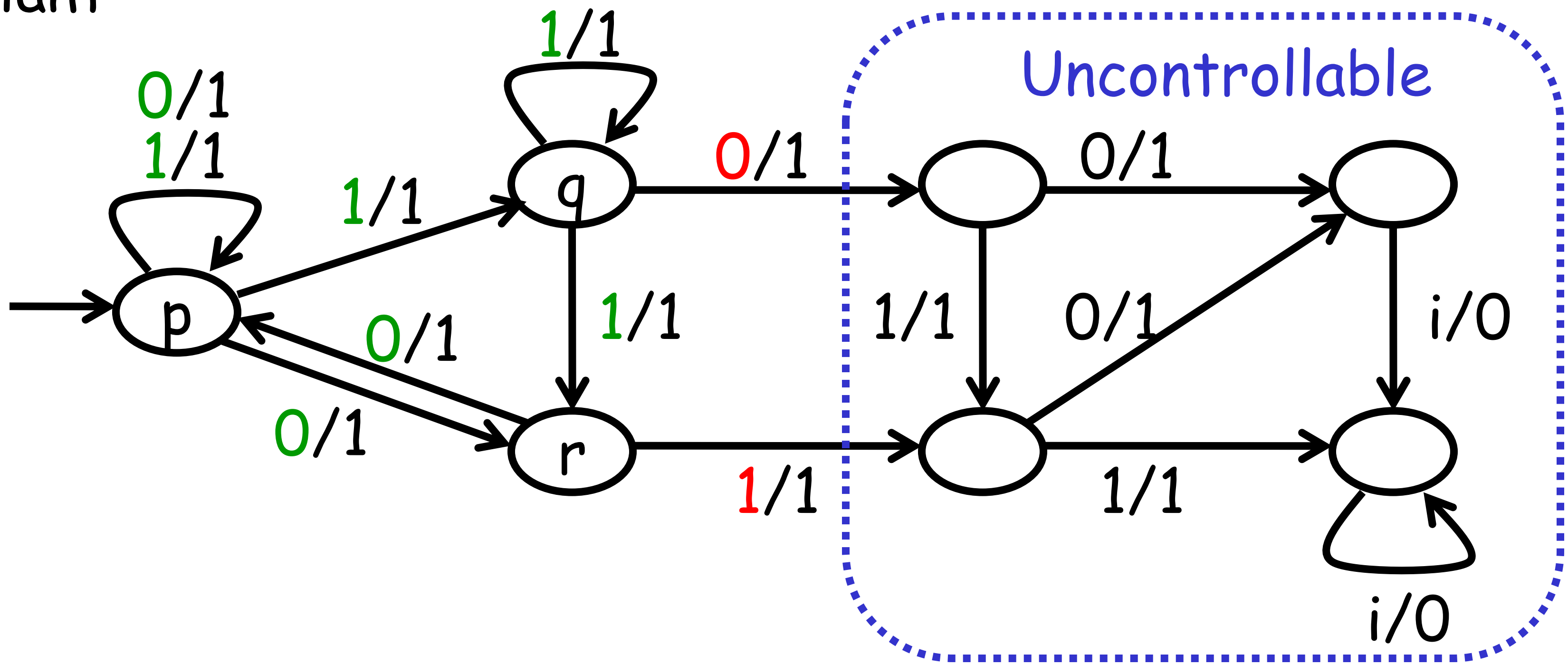
Plant

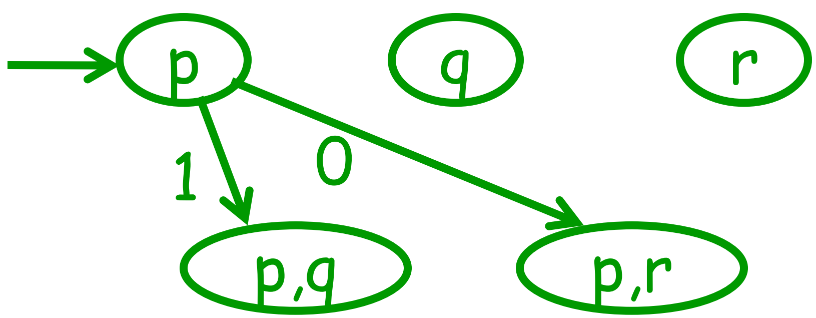




{q} : 1
{r} : 0
{p,q} : 1
{p,r} : 0

Plant



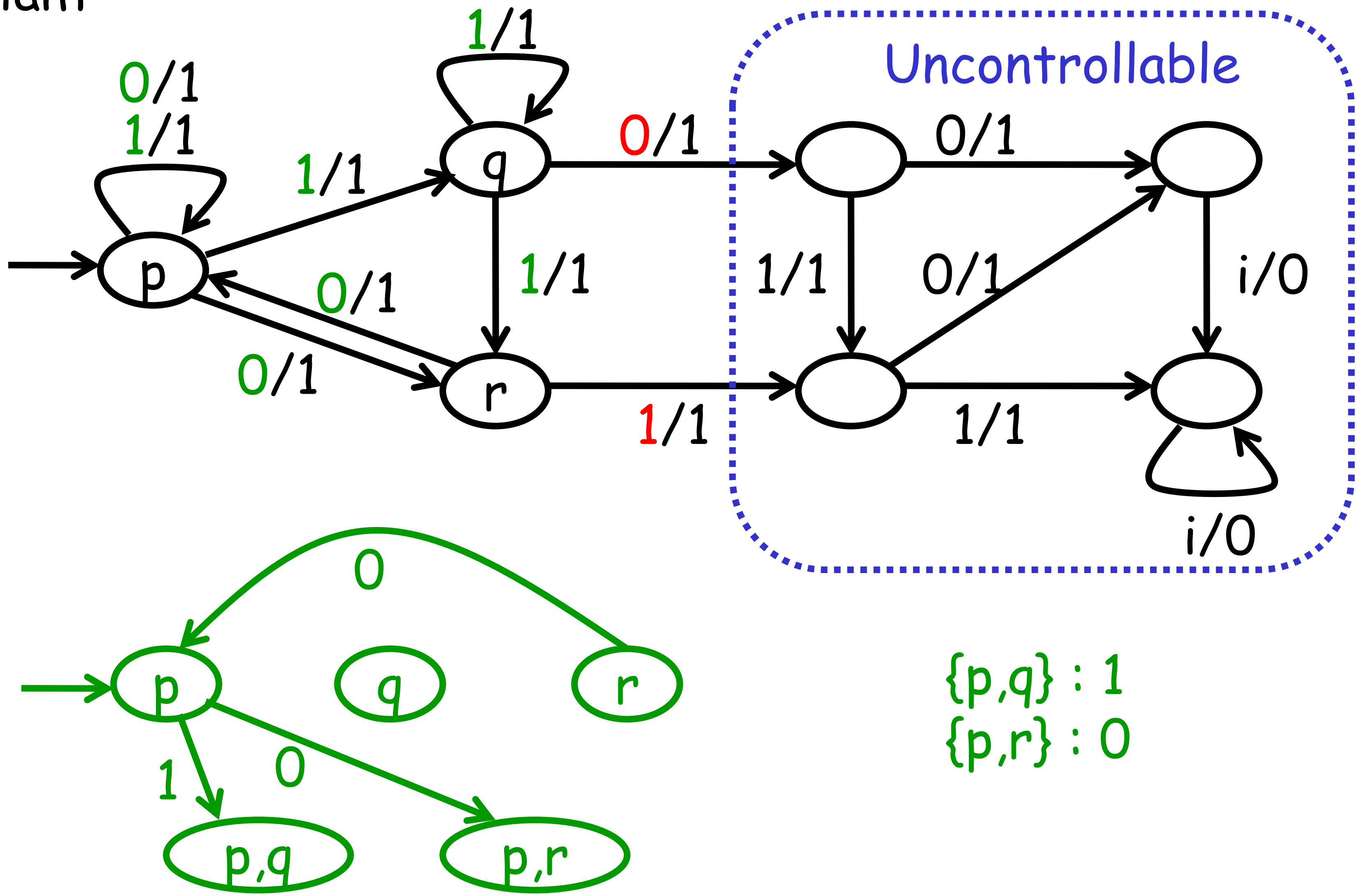


{r} : 0

{p,q} : 1

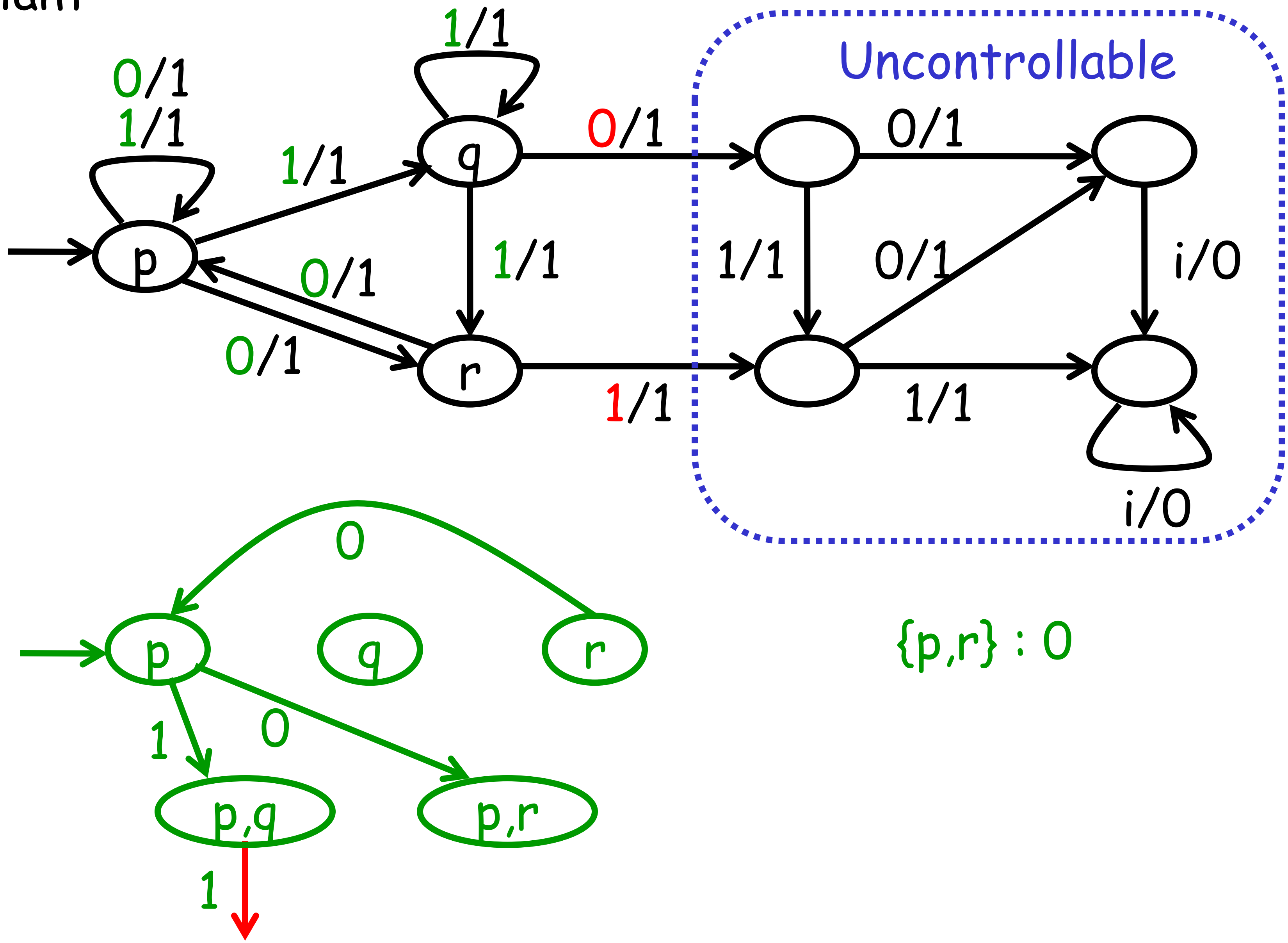
{p,r} : 0

Plant

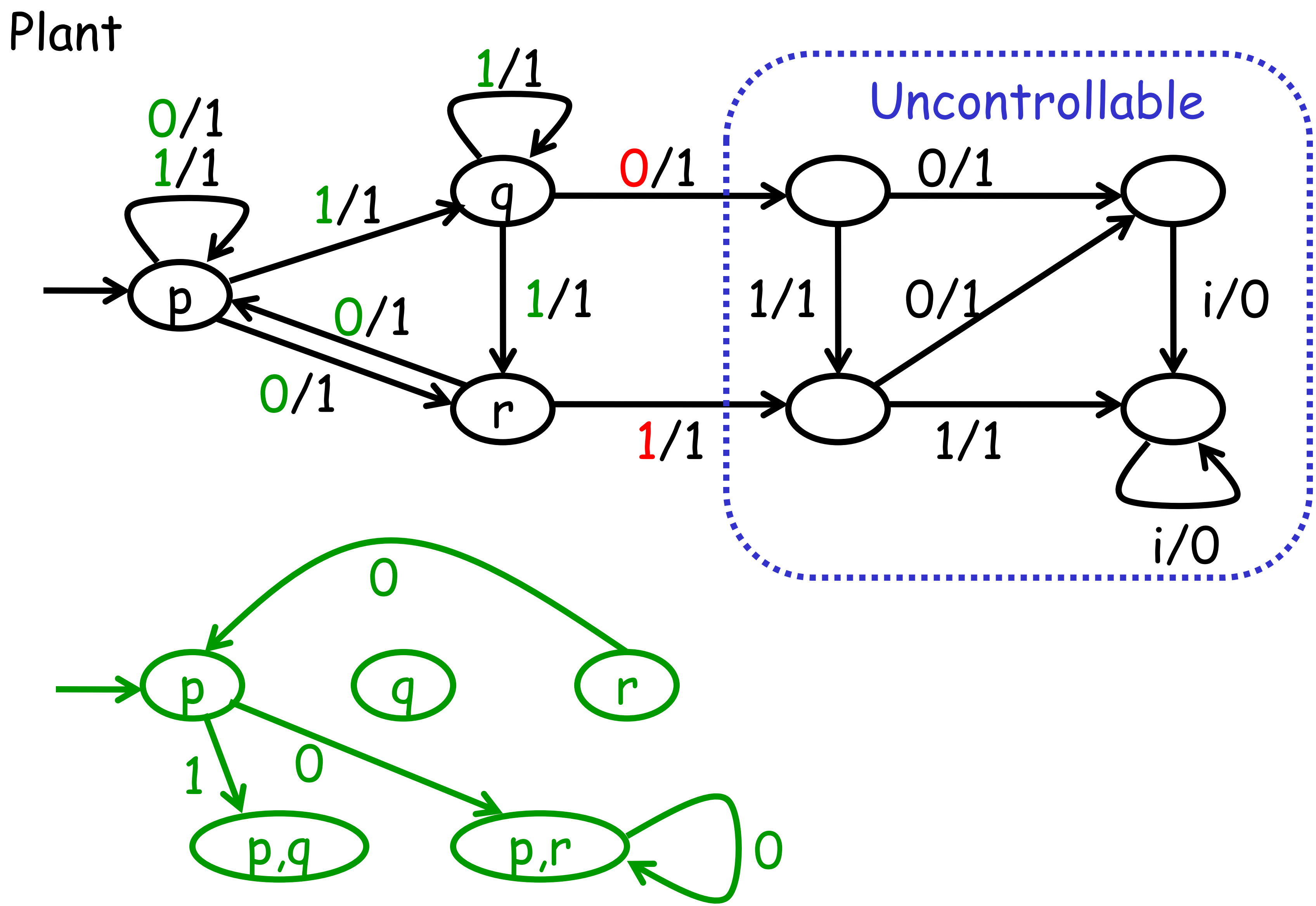


{p,q} : 1
{p,r} : 0

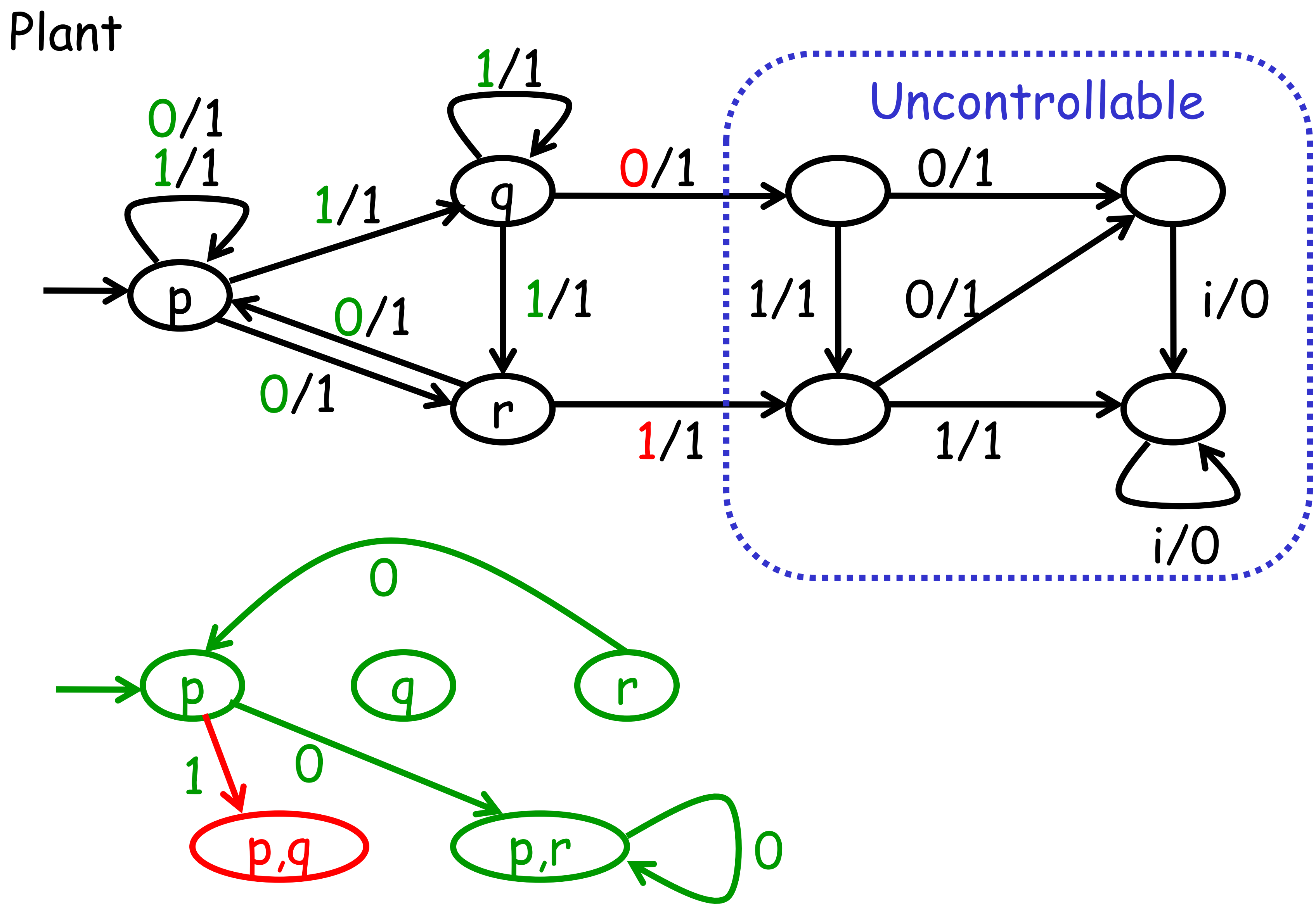
Plant



Uncontrollable
p
q
r
0/1
1/1
1/1
1/1
0/1
0/1
1/1
0/1
1/1
0/1
1/1
0/1
i/0
1/1
i/0
0
1
0
p,q
p,r
1
{p,r} : 0

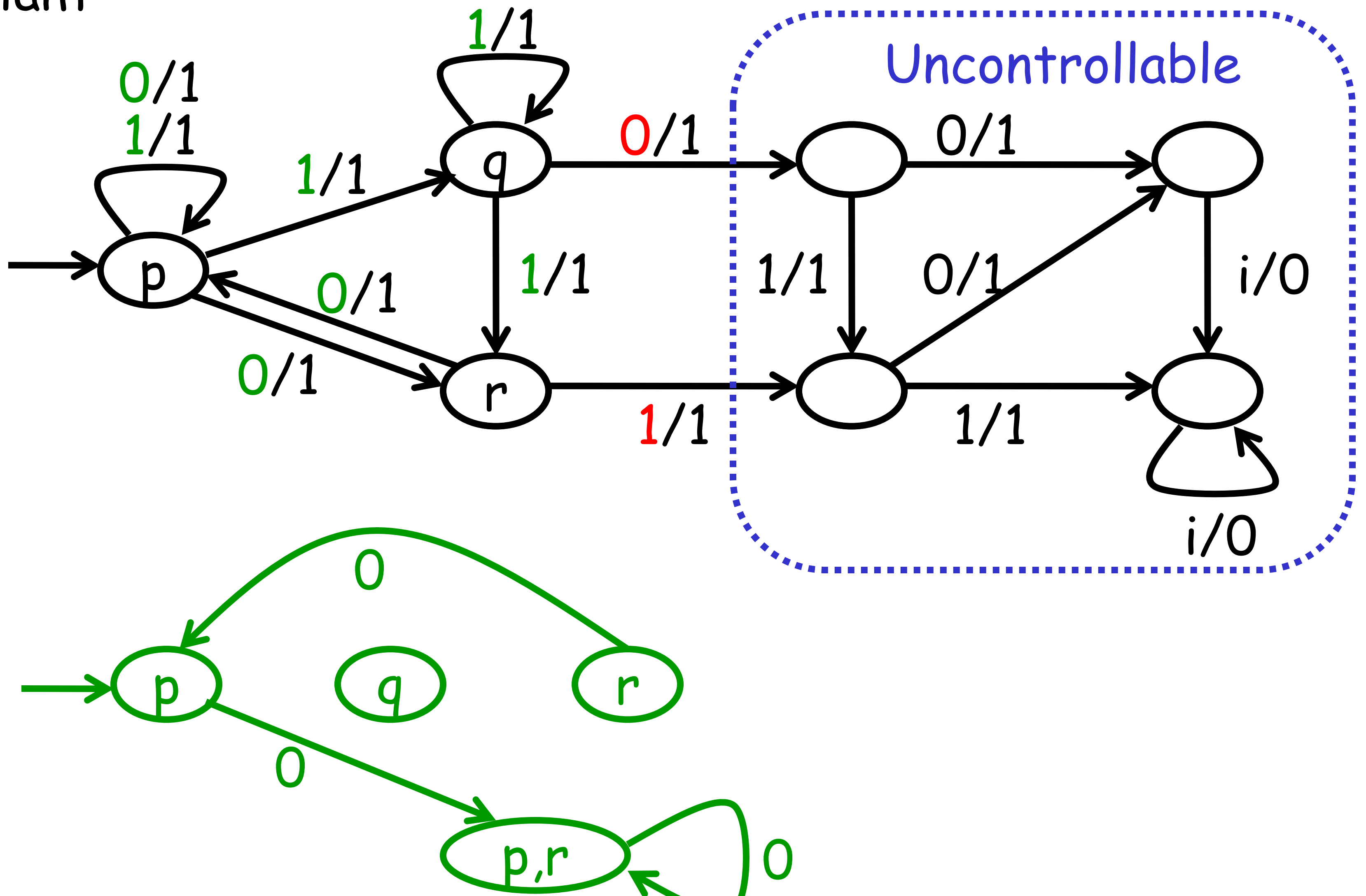


Plant
Uncontrollable
p
q
r
0/1
1/1
i/0
p,q
p,r
0
1

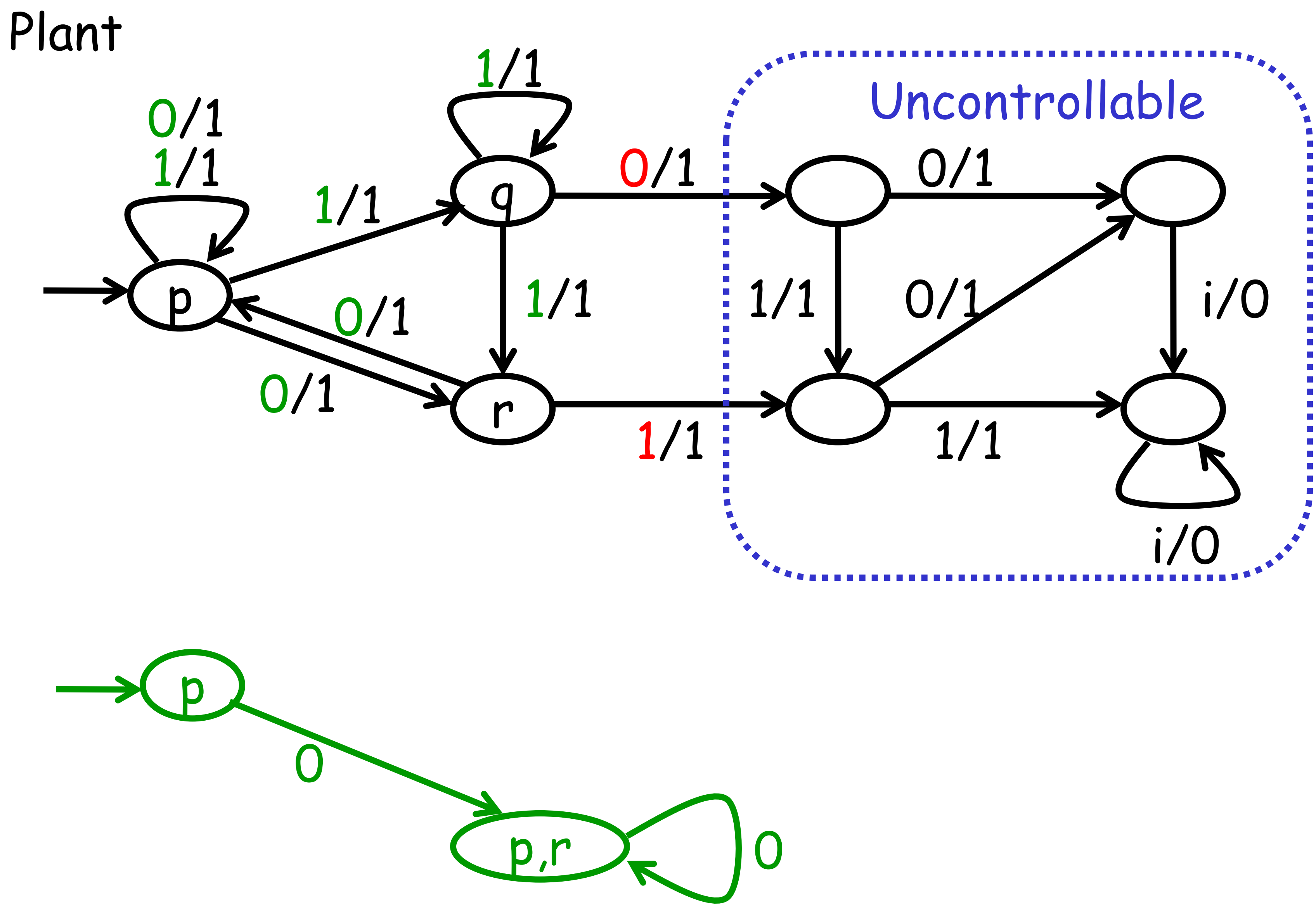


Plant
Uncontrollable
0/1
1/1
1/1
1/1
0/1
0/1
0/1
1/1
0/1
0/1
1/1
0/1
i/0
1/1
1/1
i/0
p
q
r
0
1
0
0
p
q
r
p,q
p,r

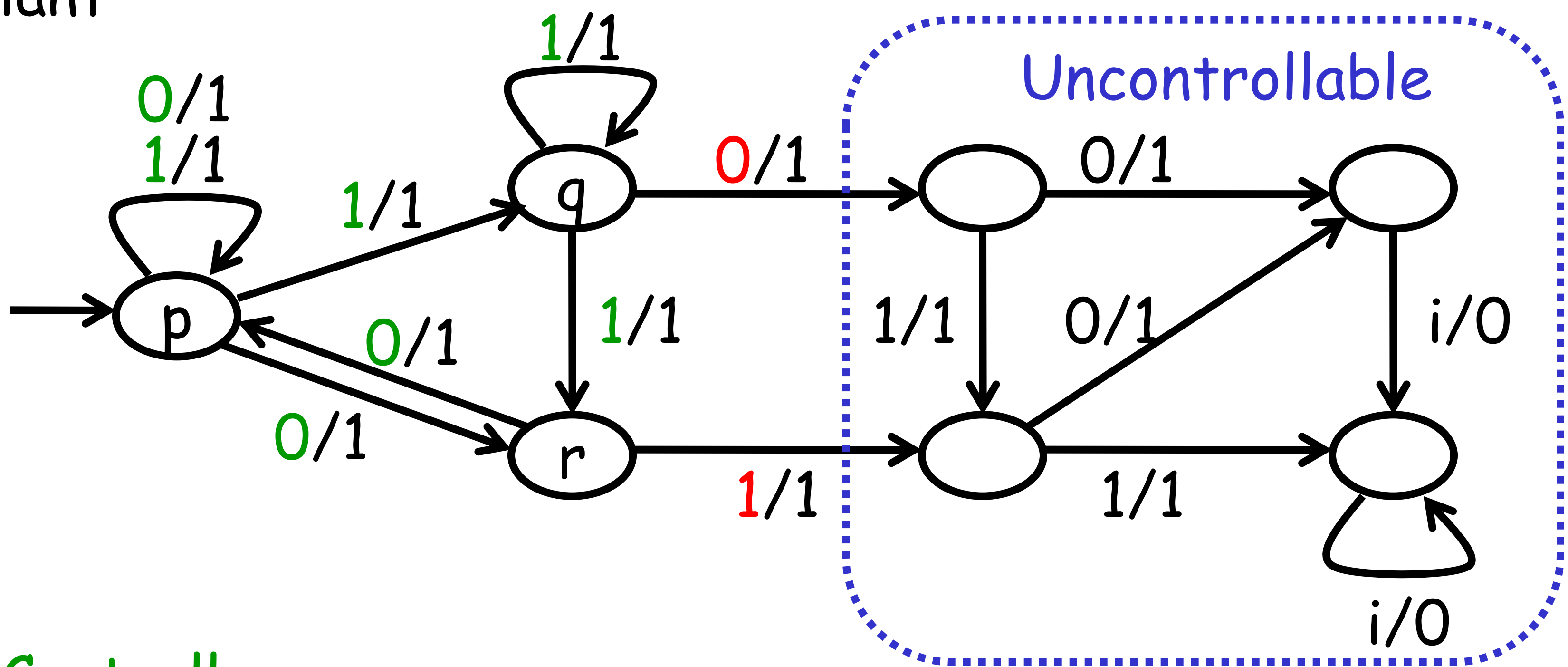
Plant



0/1
1/1
1/1
1/1
0/1
0/1
1/1
0/1
Uncontrollable
0/1
1/1
0/1
i/0
1/1
1/1
i/0
p
q
r
0
p
q
r
0
p,r
0


Plant
Uncontrollable
0/1
1/1
1/1
1/1
0/1
0/1
1/1
0/1
1/1
0/1
1/1
0/1
1/1
i/0
1/1
i/0
p
q
r
p
0
p,r
0

Plant



Controller