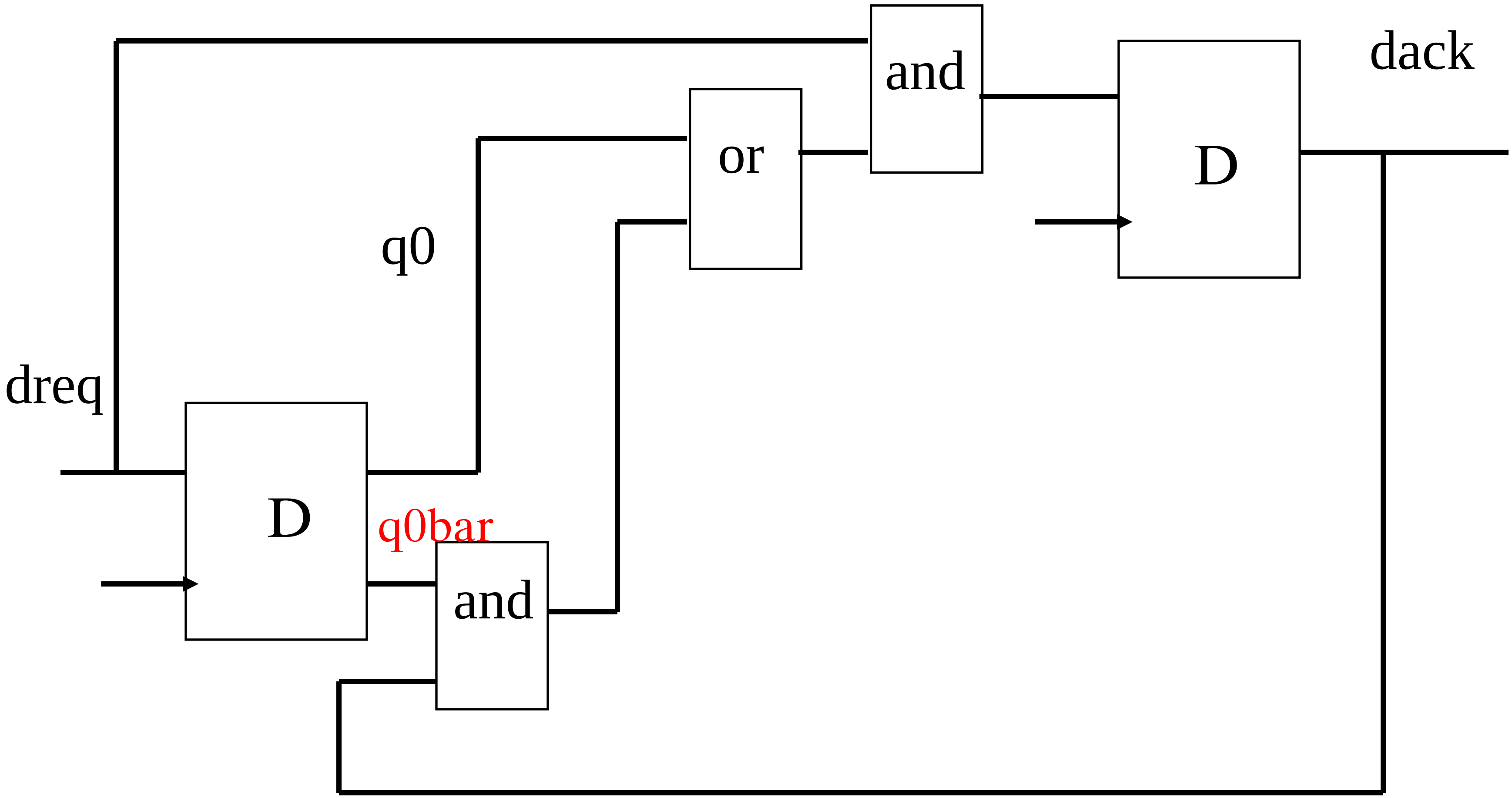
Model Checking I

What are LTL and CTL?



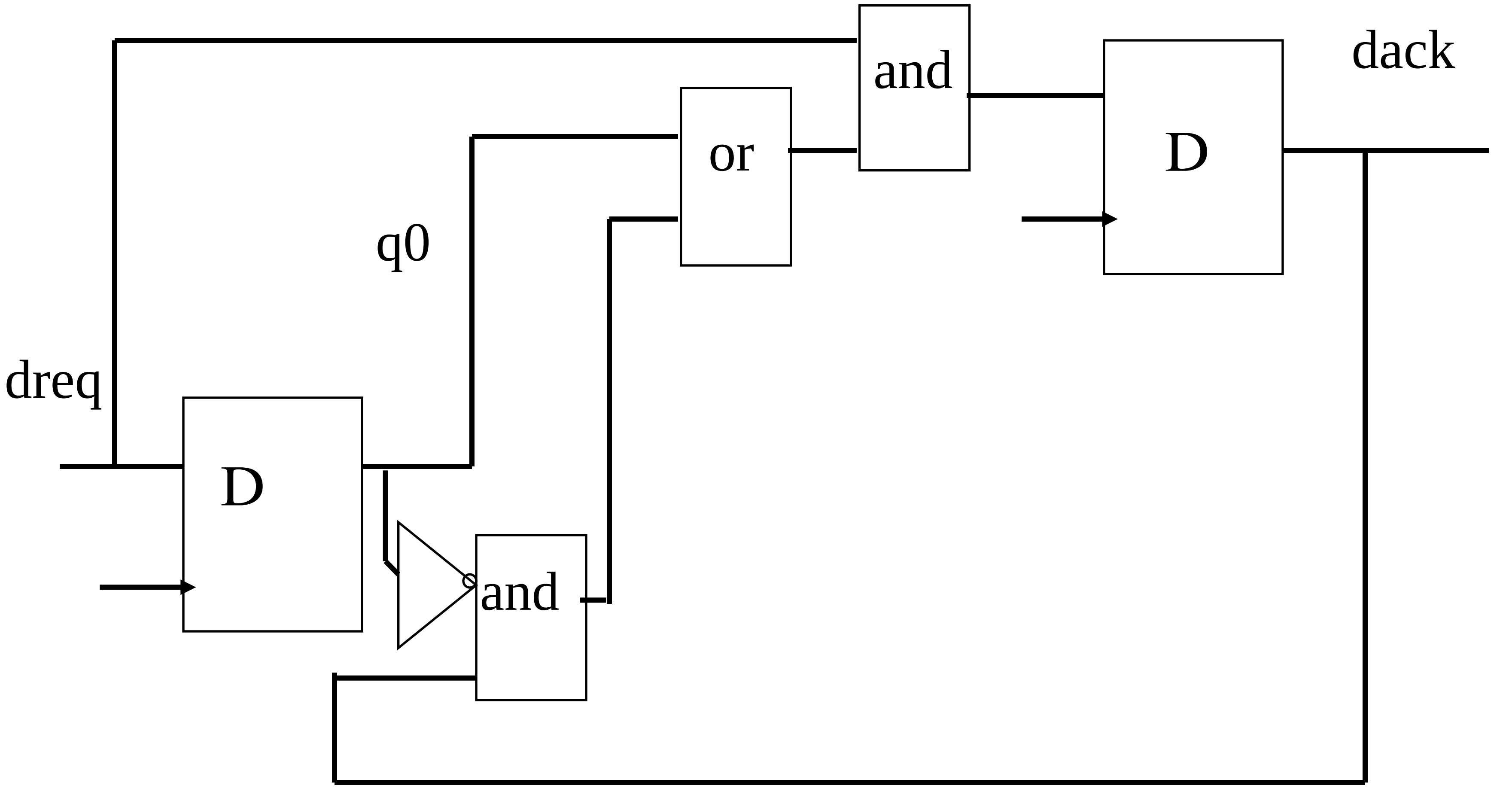
and
dack
or
D
q0
dreq
D
q0bar
and

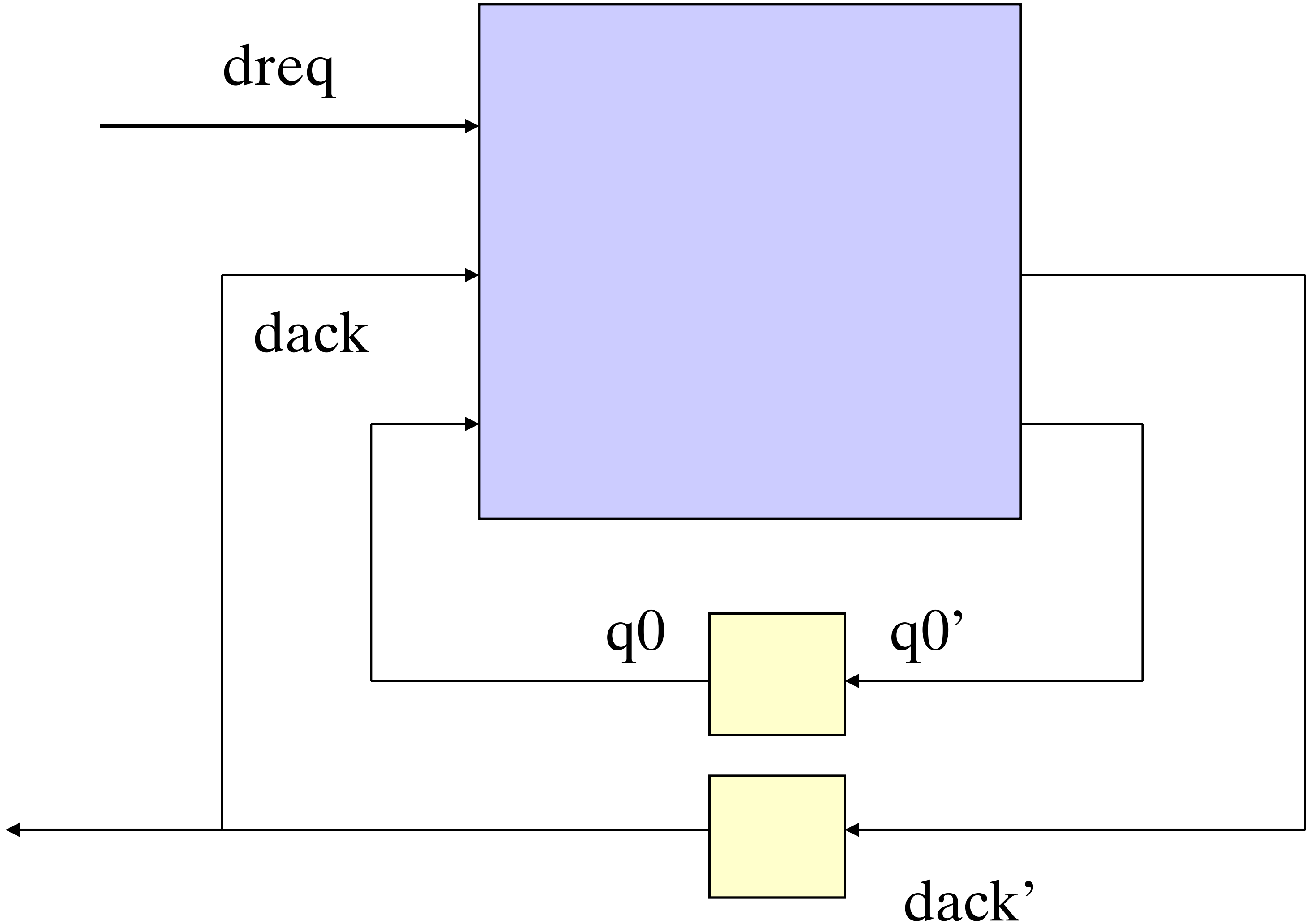
View circuit as a transition system

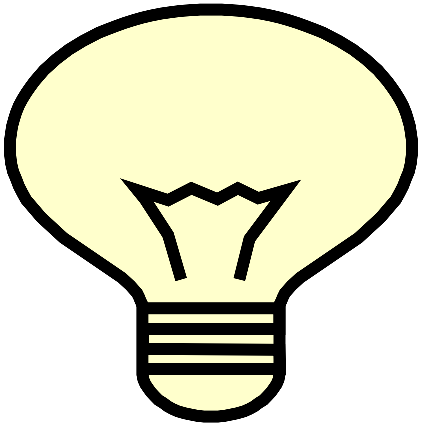
(dreq, q0, dack) → (dreq', q0', dack')

q0' = dreq

dack' = dreq and (q0 or (not q0 and dack))


dack
and
or
D
q0
dreq
D
and


dreq
dack
q0
q0'
dack'



Idea

Transition system

+ special temporal logic

+ automatic checking algorithm

Exercise (from example circuit)

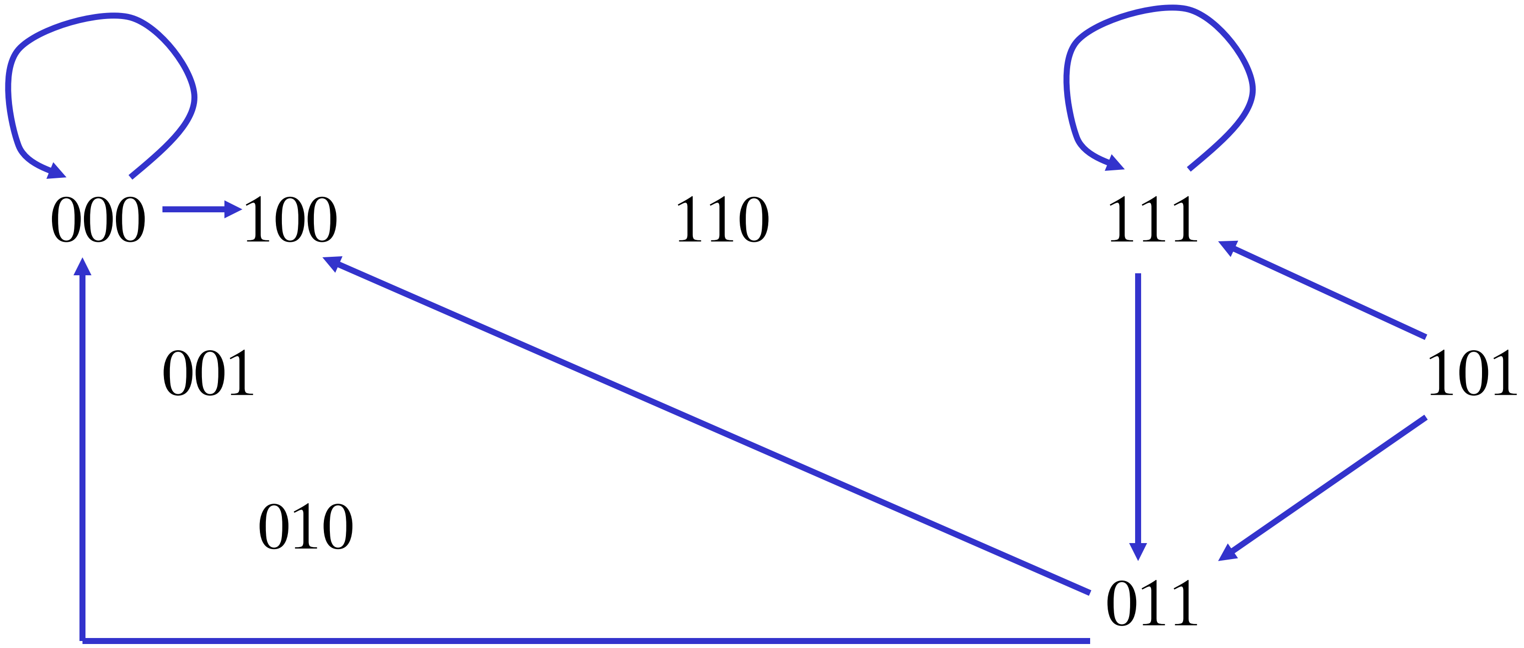
(dreq, q0, dack) $\rightarrow$

(dreq', dreq, dreq and (q0 or (not q0 and dack)))

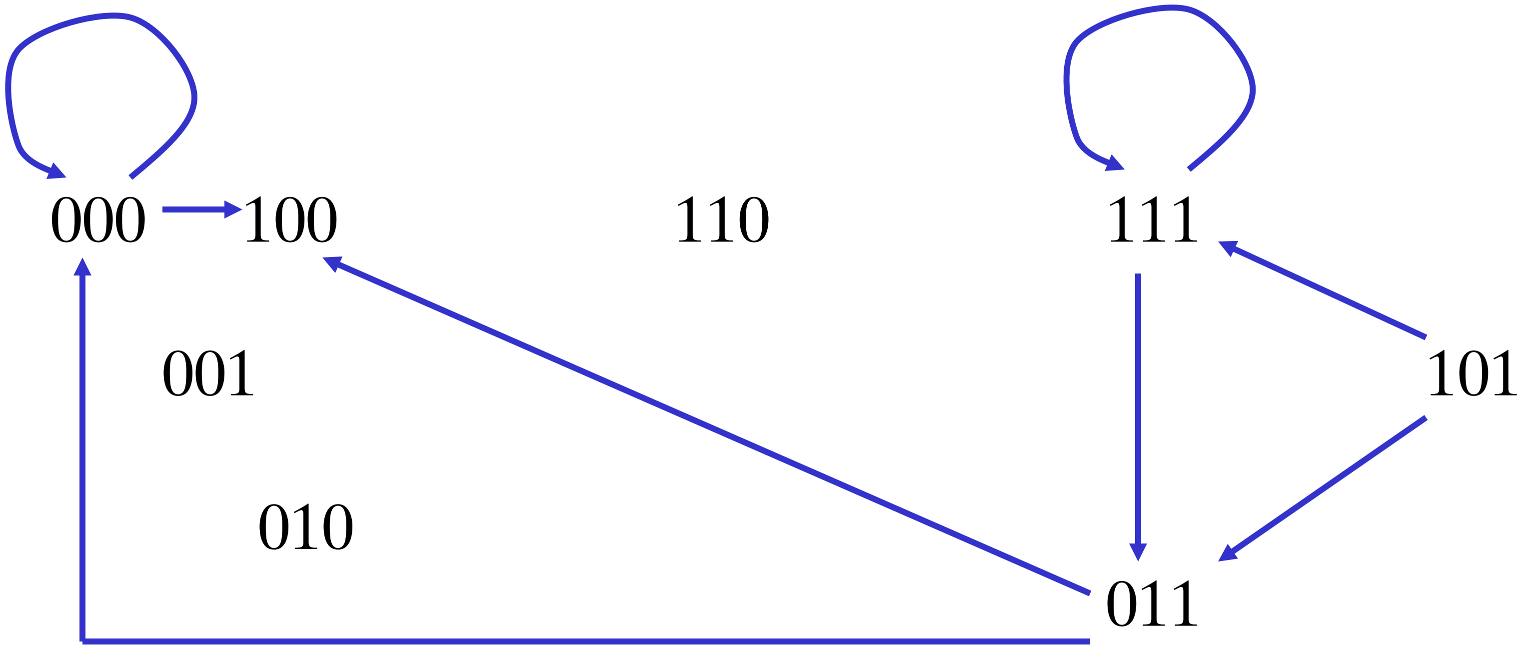
Draw state transition diagram

Q: How many states for a start?

Hint (partial answer)

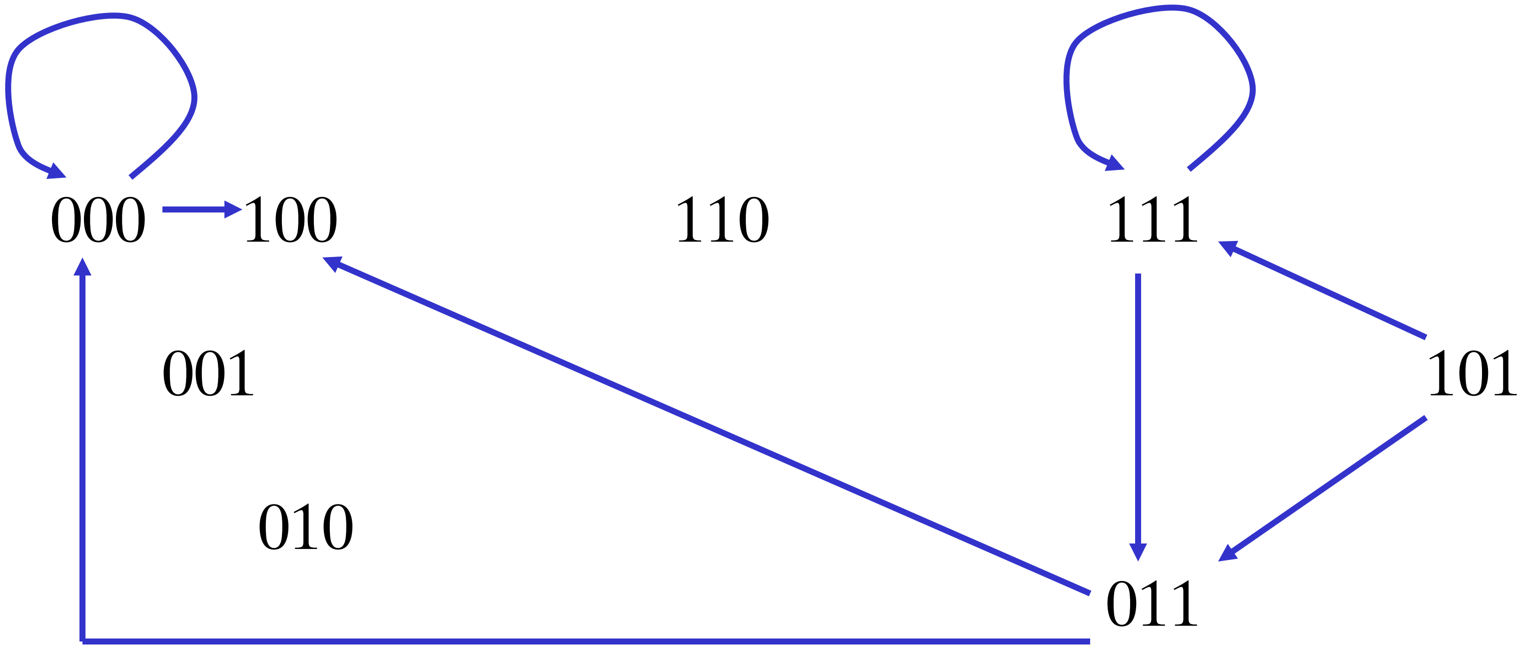


Question



Q: how many arrows should there be out of each state?
Why so?

Exercise

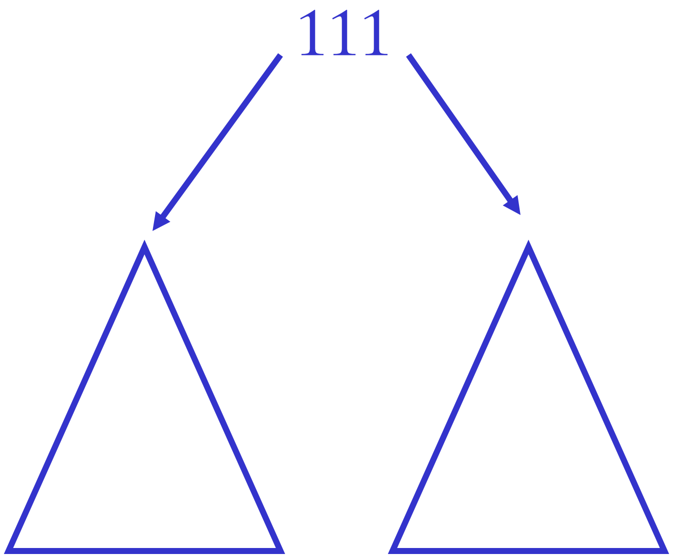


Complete the diagram

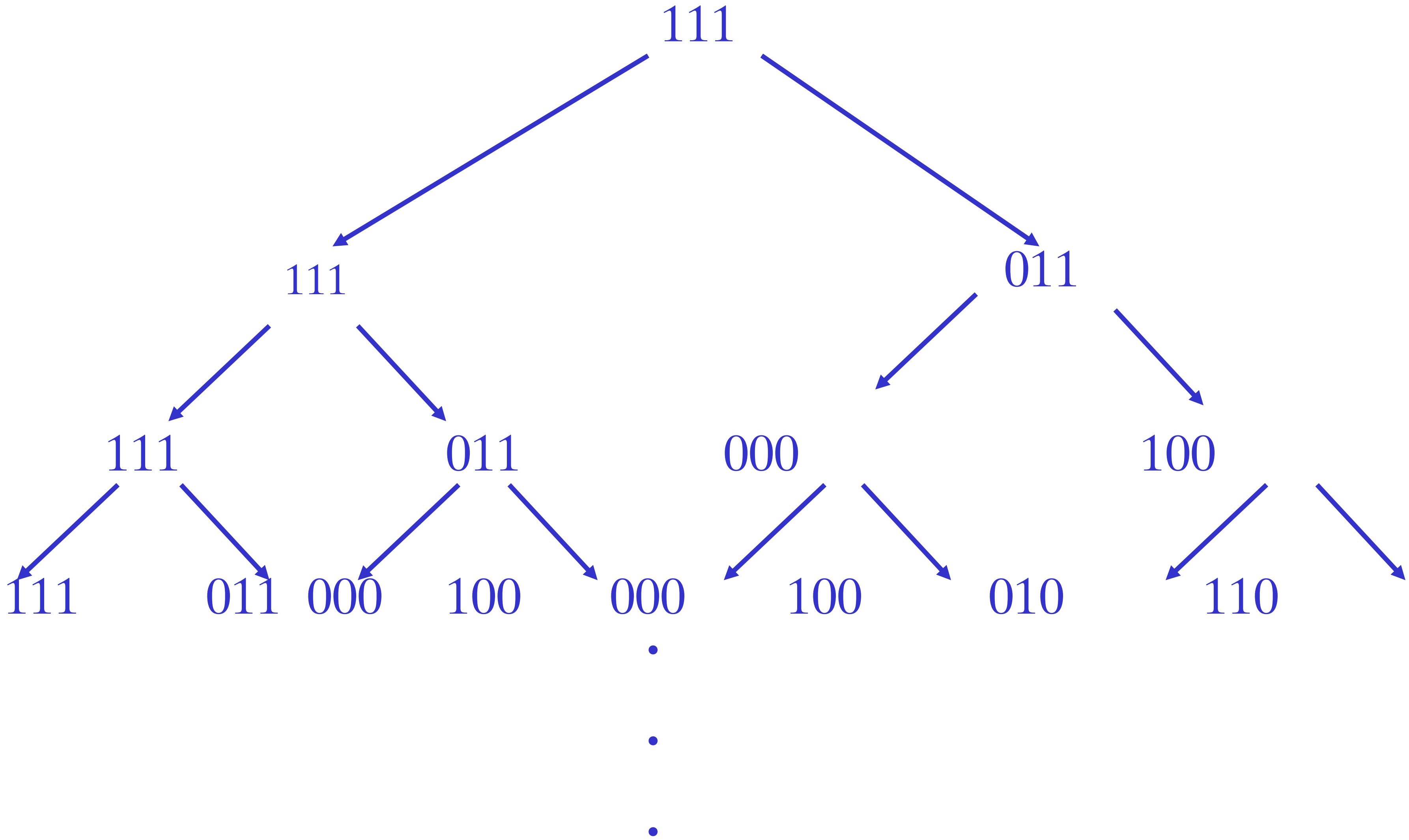
Write down the corresponding binary relation as a set of pairs of states

Another view

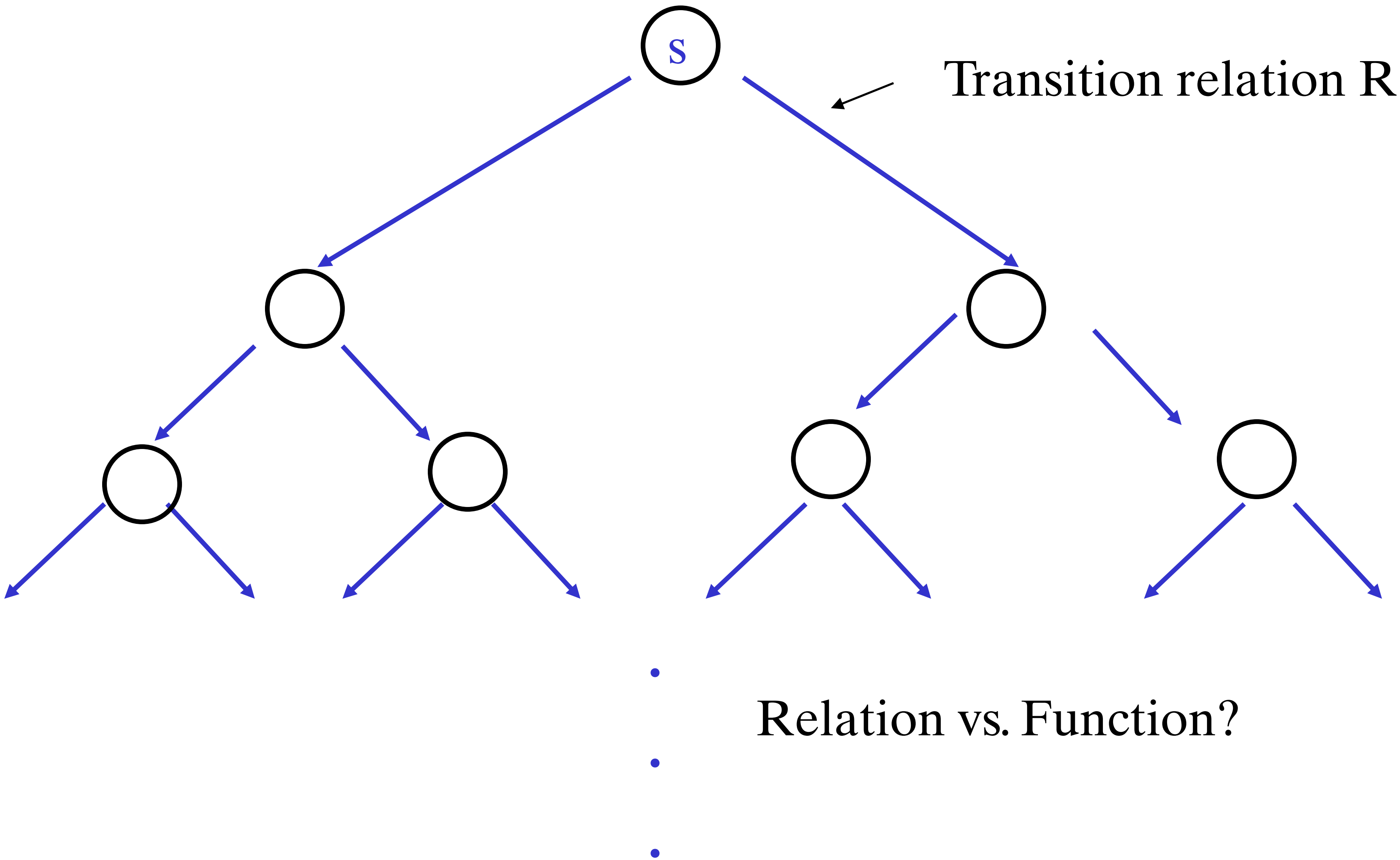
computation tree from a state



Unwinding further

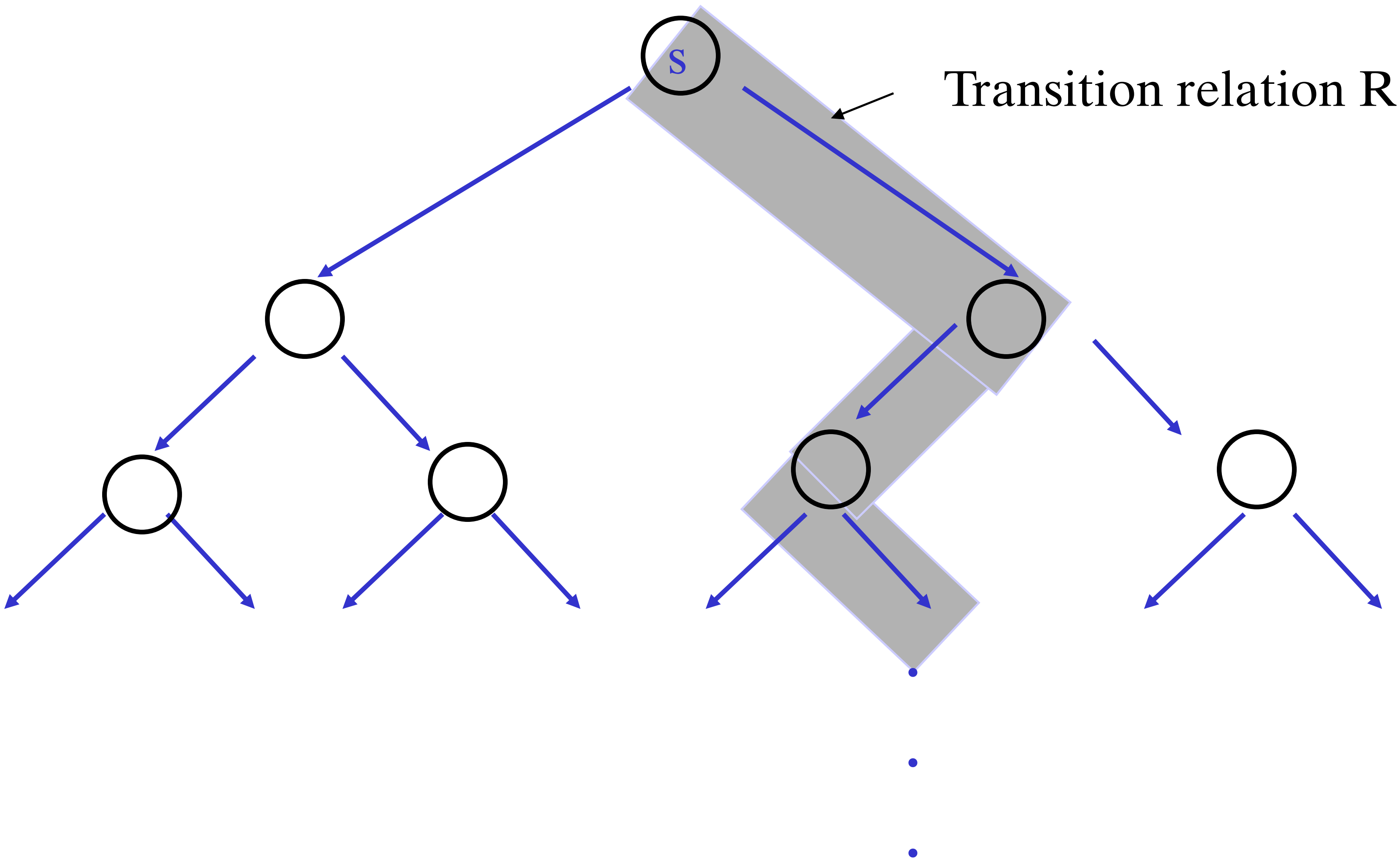


Possible behaviours from state s



Relation vs. Function?

path = possible run of the system



Points to note

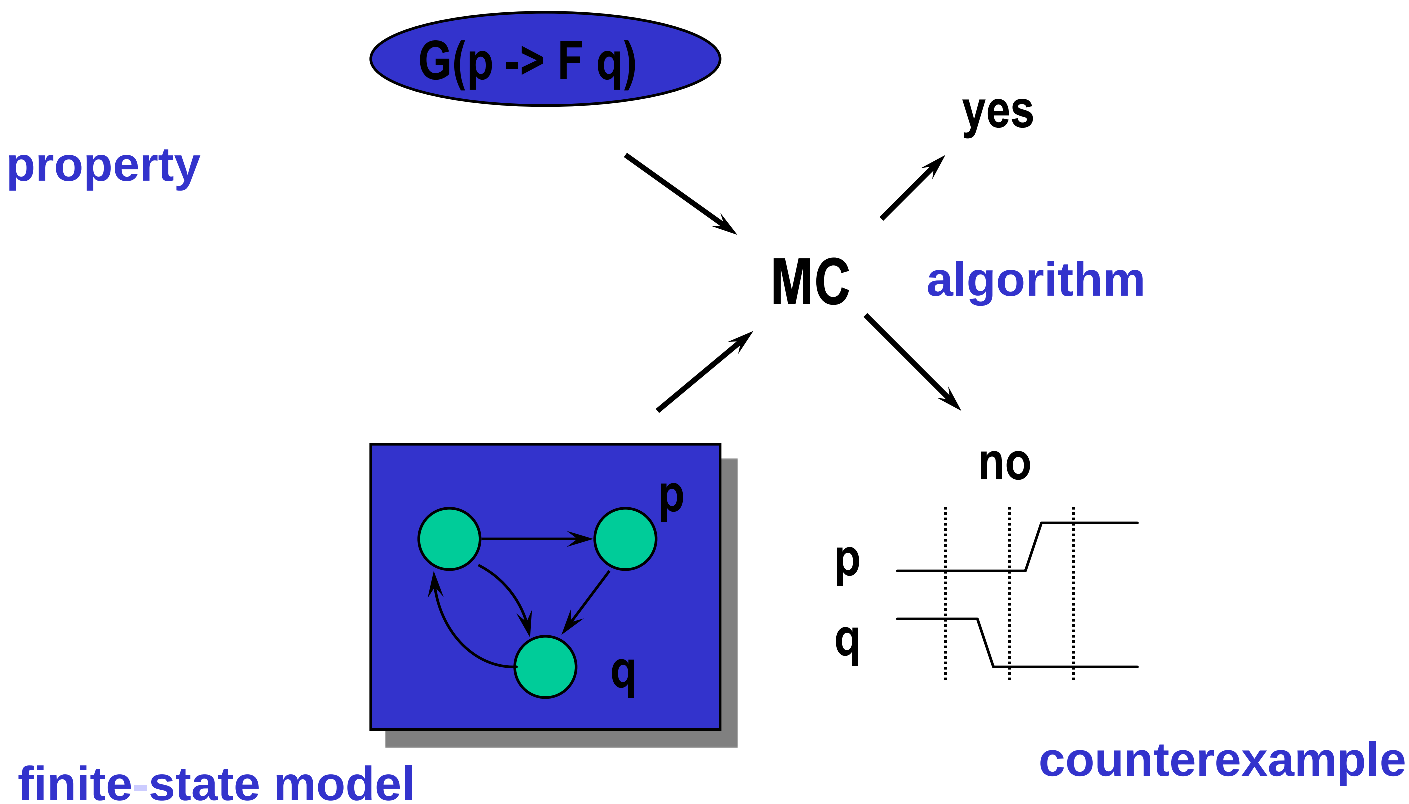
Transition system models circuit behaviour

We chose the tick of the transition system to be the same as one clock cycle. Gates have zero delay – a very standard choice for synchronous circuits

Could have had a finer degree of modelling of time (with delays in gates). Choices here determine what properties can be analysed

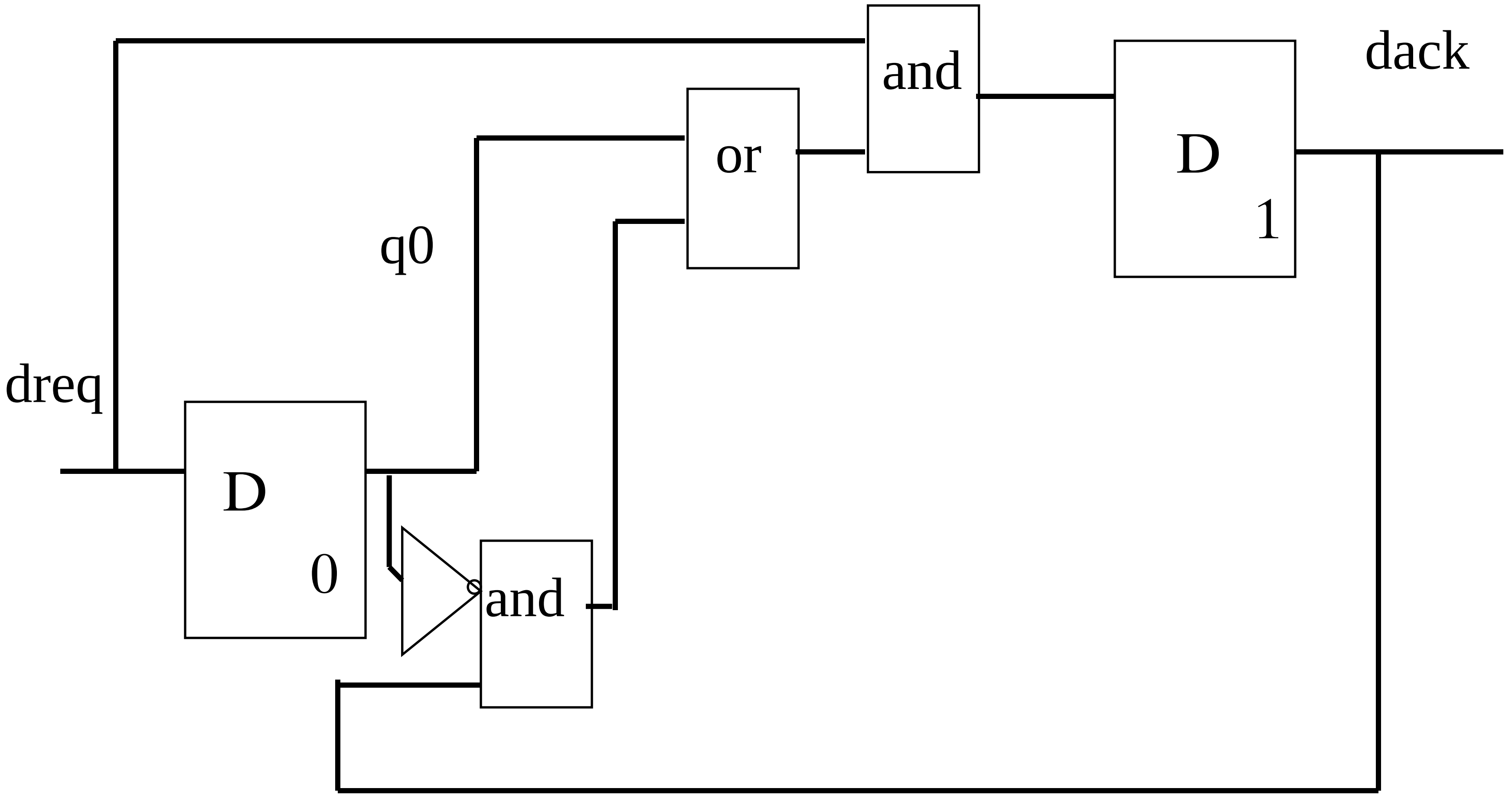
Model checker starts with transition system. It doesn't matter where it came from

Model Checking



(Ken McMillan)

Netlist



input to SMV model checker

```
MODULE main
VAR w1 : boolean;
VAR w2 : boolean;
VAR w3 : boolean;
VAR w4 : boolean;
VAR w5 : boolean;
VAR i0 : boolean;
VAR w6 : boolean;
VAR w7 : boolean;
VAR w8 : boolean;
VAR w9 : boolean;
VAR w10 : boolean;
DEFINE w4 := 0;
DEFINE w5 := i0;
ASSIGN init(w3) := w4;
ASSIGN next(w3) := w5;
DEFINE w7 := !(w3);
DEFINE w9 := 1;
DEFINE w10 := w5 & w6;
ASSIGN init(w8) := w9;
ASSIGN next(w8) := w10;
DEFINE w6 := w7 & w8;
DEFINE w2 := w3 | w6;
```

MC builds internal representation of transition system

Transition system M

S set of states (finite)

R binary relation on states
assumed total, each state has at least one arrow out

A set of atomic formulas

L function S -> set of atomic formulas that hold in that state

Lars backwards ☺ finite Kripke structure

Path in M

Infinite sequence of states

$\pi = s0\ s1\ s2 \ldots \qquad st$

Path in M

$s0 \rightarrow s1 \rightarrow s2 \rightarrow \ldots$

$\xrightarrow{}$
R

$(s0,s1) \in R$

$(s1,s2) \in R$

etc

Properties

Express desired behaviour over time using special logic

LTL (linear temporal logic)

CTL (computation tree logic)

CTL* (more expressive logic with both
. LTL and CTL as subsets)

CTL*

path quantifers
A “for all computation paths”
E “for some computation path”
can prefix assertions made from
Linear operators
G “globally=always”
F “sometimes”
X “nexttime”
U “until”

about a path

CTL* formulas (syntax)

path formulas

$f ::= s \mid \neg f \mid f1 \vee f2 \mid X\, f \mid f1\, U\, f2$

state formulas (about an individual state)

$s ::= a \mid \neg s \mid s1 \vee s2 \mid E\, f$

atomic formulas

Build up from core

$$A\,f \quad = \quad \neg\, E \neg\, f$$

$$F\,f \quad = \quad \text{true}\ U\ f$$

$$G\,f \quad = \quad \neg\, F \neg\, f$$

Example

G (req -> F ack)

Example

G (req -> F ack)

A request will eventually lead to an acknowledgement

liveness

linear

Example (Gordon)

It is possible to get to a state where Started holds but Ready does not

Example (Gordon)

It is possible to get to a state where Started holds but Ready does not

$\mathbf{E}\ (F\ (\text{Started} \mathbin{\&} \neg\text{Ready}))$

Semantics

$M = (L, A, R, S)$

$M, s \models f$ f holds at state s in M
(and omit M if it is clear which M
we are talking about)

$M, \pi \models g$ g holds for path π in M

Semantics

Back to syntax and write down each case

$S \models a$ a in L(s)   (atomic)

$s \models \neg f$ not $(s \models f)$

$s \models f1 \vee f2$ $s \models f1$ or $s \models f2$

$s \models E\,(g)$ Exists π. head(π) = s and $\pi \models g$

Semantics

$\pi \models f \qquad s \models f$ and $head(\pi) = s$

$\pi \models \neg g \qquad$ not $(\pi \models g)$

$\pi \models g1 \vee g2 \qquad \pi \models g1$ or $\pi \models g2$

Semantics

$\pi \models X\, g$ $\qquad\qquad$ $tail(\pi) \models g$

$\pi \models g1\ U\ g2$

Exists $k \geq 0$. $\quad$ $drop\ k\ \pi \models g2$ $\qquad$ and

$\quad$ Forall $0 \leq j < k$. $\quad$ $drop\ j\ \pi \models g1$

(note: I mean tail in the Haskell sense)

CTL

Branching time (remember upside-down tree)

Restrict path formulas (compare with CTL*)

$f ::= \neg f \mid s1 \vee s2 \mid X\, s \mid s1\ U\ s2$ $\leftarrow$

state formulas

Linear time ops (X,U,F,G) must be wrapped up in a path quantifier (A,E).

Back to CTL* formulas (syntax)

path formulas

$f ::= s \mid \neg f \mid f1 \vee f2 \mid X\, f \mid f1\, U\, f2$

state formulas (about an individual state)

$s ::= a \mid \neg s \mid s1 \vee s2 \mid E\, f$

atomic formulas

CTL

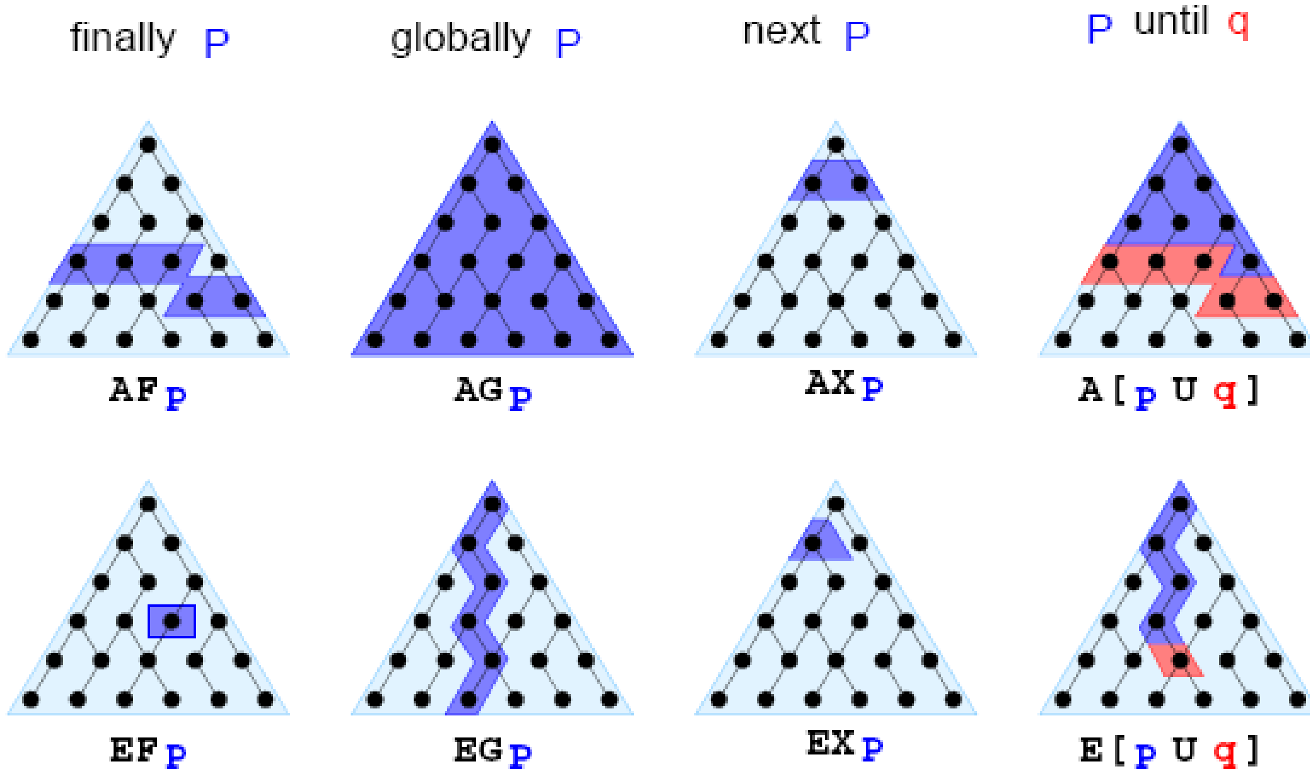
Another view is that we just have the combined operators AU, AX, AF, AG and EU, EX, EF, EG and only need to think about state formulas

A operators for necessity

E operators for possibility

f	::=	atomic
		| ¬f
All immediate successors		| AX f
Some immediate succesor		| EX f
All paths always		| AG f
Some path always		| EG f
All paths eventually		| AF f
Some path eventually		| EF f
		| f1 & f2
		| A (f1 U f2)
		| E (f1 U f2)

CTL


finally p
globally p
next p
p until q
AF p
AG p
AX p
A [p U q]
EF p
EG p
EX p
E [p U q]

Examples (Gordon)

It is possible to get to a state where Started holds but Ready does not

Examples (Gordon)

It is possible to get to a state where Started holds but Ready does not

$EF\ (Started\ \&\ \neg Ready)$

Examples (Gordon)

If a request Req occurs, then it will eventually be acknowledged by Ack

Examples (Gordon)

If a request Req occurs, then it will eventually be acknowledged by Ack

AG (Req -> AF Ack)

Examples (Gordon)

If a request Req occurs, then it continues to hold, until it is eventually acknowledged

Examples (Gordon)

If a request Req occurs, then it continues to hold, until it is eventually acknowledged

AG (Req -> A [Req U Ack])

LTL

LTL formula is of form A f where f is a path formula with subformulas that are atomic

(The f is what we write down. The A is implicit.)

Restrict path formulas (compare with CTL*)

$f ::= a \mid \neg f \mid f1 \vee f2 \mid X\, f \mid f1\, U\, f2$

Back to CTL* formulas (syntax)

path formulas

$f ::= s \mid \neg f \mid f1 \vee f2 \mid X\, f \mid f1\, U\, f2$

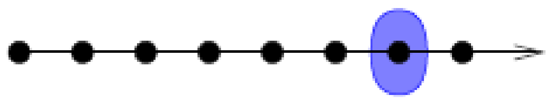
state formulas (about an individual state)

$s ::= a \mid \neg s \mid s1 \vee s2 \mid E\, f$

atomic formulas

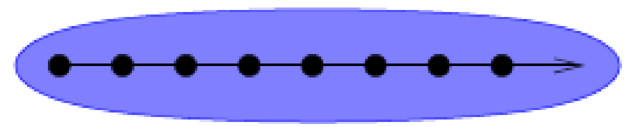
LTL

finally p



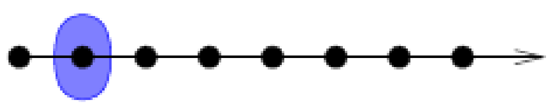
F p

globally p



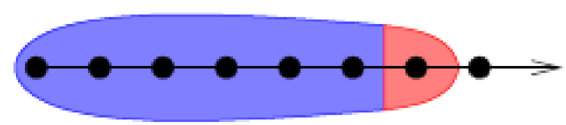
G p

next p



X p

p until q



p **U** q

LTL

It is the restricted path formulas that we think of as LTL specifications (See P&R again)

$G \neg (critical1 \ \& \ critical2)$ mutex

FG initialised eventually stays initialised

GF myMove myMove will always eventually hold

G (req -> F ack) request acknowledge pattern

In CTL but not LTL

AG EF start

Regardless of what state the program enters, there exists a computation leading back to the start state

AF AG p

In both

$AG\ (p \rightarrow AF\ q)$ in CTL

$G(p \rightarrow F\ q)$ in LTL

In LTL but not CTL

[G F p $\rightarrow$ F q]

if there are infinitely many p along the path, then there is an occurrence of q

F G p

In CTL* but not in LTL or CTL

E [G F p]

there is a path with infinitely many p

Further reading

Ed Clarke's course on **Bug Catching: Automated Progra Verification and Testing**

complete with moving bug on the home page!

Covers model checking relevant to hardware too.

http://www.cs.cmu.edu/afs/cs.cmu.edu/academic/class/15414-f06/www/index.html

For some history (by the inventors themselves) see this workshop celebrating 25 years of MC
http://www.easychair.org/FLoC-06/25MC-day227.html

Example revisited

A sequence beginning with the assertion of signal strt, and containing two not necessarily consecutive assertions of signal get, during which signal kill is not asserted, must be followed by a sequence containing two assertions of signal put before signal end can be asserted

AG~(strt & EX E[~get & ~kill U get & ~kill & EX E[~get & ~kill U get & ~kill & E[~put U end] or E[~put & ~end U (put & ~end & EX E[~put U end])]]])

Next lecture

How to model check CTL formulas