Model Checking.

Used for formal verification, testing, ...

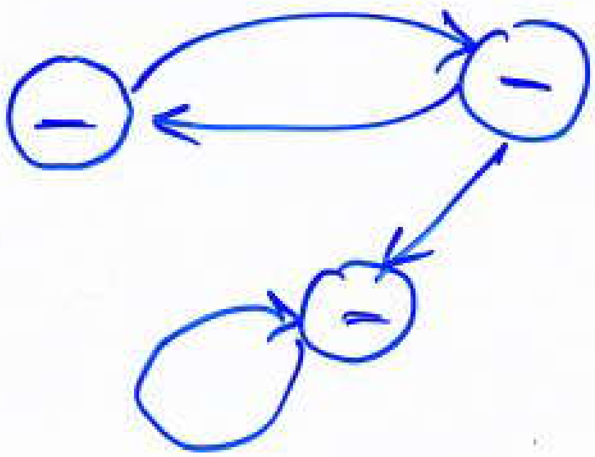
Idea: • describe system as a model M for an appropriate logic (e.g. LTL, CTL, ...)

• write down a specification of desired behavior as a formula φ of the logic

• check : $M \models \varphi$ (formula φ is true in model M)

In our case, M must "capture" change over time.

$\Rightarrow$ M is a labelled transition system (= Kripke structure)



Our logics will be interpreted over transition systems.

(modal temporal logics)

Goal: automated MC.

Linear-time temporal logic.

time $\approx$ a sequence of states, (LTL)
a path
(different from "branching time").

Syntax of LTL (in Backus Naur form)

$$\varphi ::= \top \mid \bot \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid$$
$$(X\varphi) \mid (F\varphi) \mid (G\varphi) \mid (\varphi\, U\, \varphi) \mid (\varphi\, W\, \varphi) \mid$$
$$(\varphi\, R\, \varphi)$$

e.g. $((G\,(p\,U\,(\neg r)) \to (F p))$

Convention:

- Unary connectives $\neg, X, G, F$ bind most tightly
- Then U, R, W
- Then $\wedge, \vee$
- Then $\to$.

e.g. $G(p\,U\,\neg r) \to Fp$

Conventions

- Unary connectives $\neg$, X, G, F bind most tightly
- Then U, R, W
- Then $\wedge$, $\vee$
- Then $\rightarrow$

e.g. $\big(G(p\,U(\neg r))\big) \rightarrow (F p)$

WFF ?

$F p \wedge G p \rightarrow W p$ ✗

$F(p \rightarrow G r) \vee \neg q\, U r$ ✓

$p\, U \underbrace{(q\, W r)\, p}_{\text{not wFF}}$ ✗

Semantics of LTL

Def A *model* $M = (S, \rightarrow, L)$

a set of states S together with a transition relation $\rightarrow$ (a binary relation on S), s.t. for every $s \in S$ there is $s' \in S$ with $s \rightarrow s'$

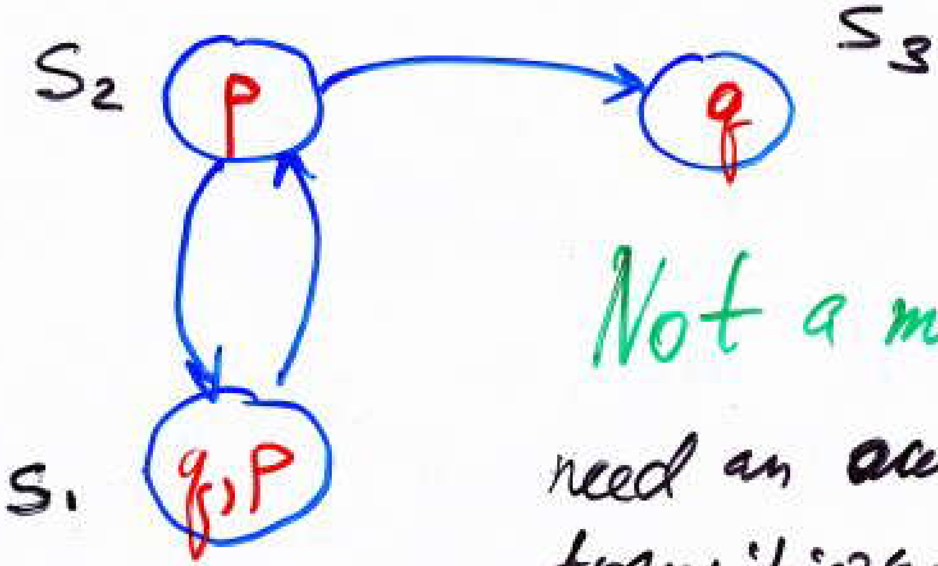
(i.e., no state can "deadlock")

and a labelling function

$$L : S \rightarrow \mathcal{P}ow(Atoms)$$

$Atoms$ = atomic propositions p, q, r etc.

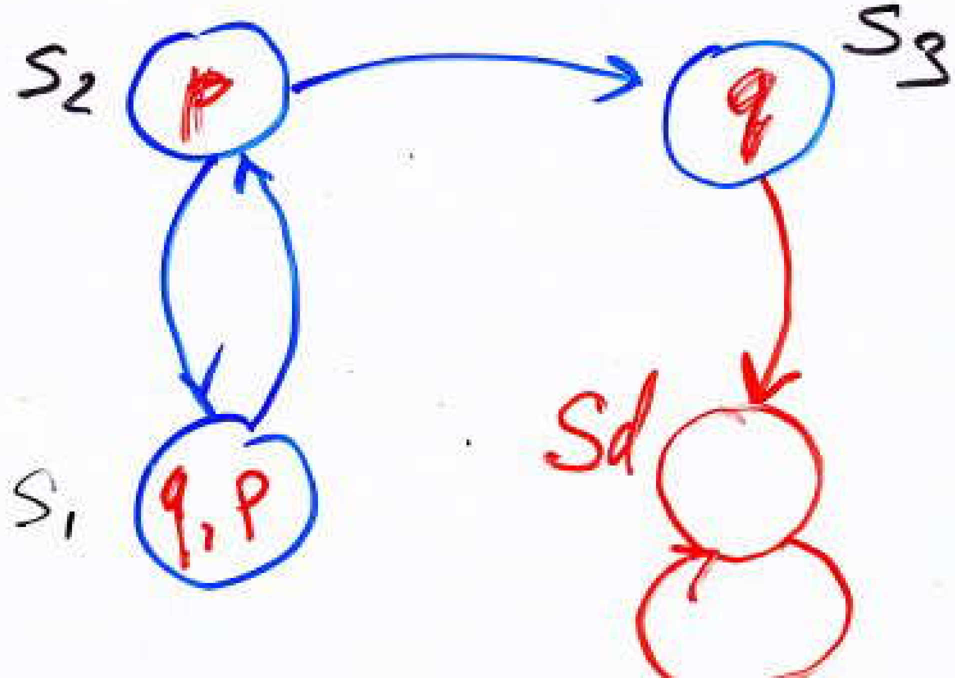
e.g. Atoms $= \{p, q\}$



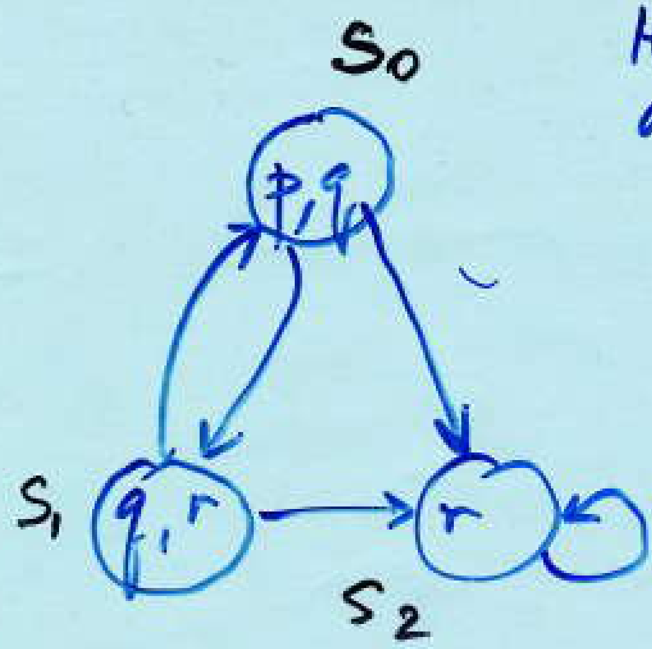
Not a model!

need an outgoing transition for each state

Modify:



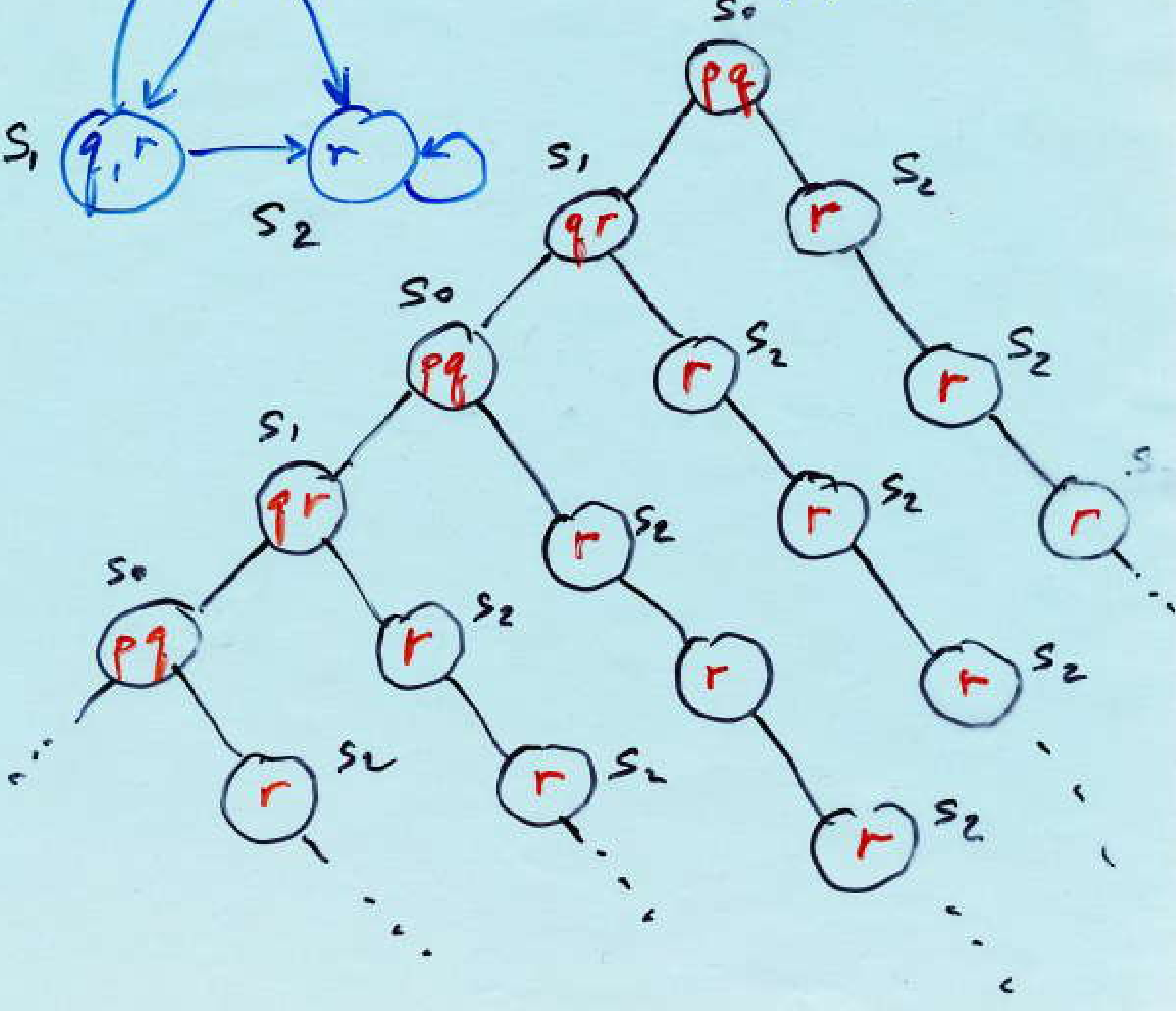
⇒ can think of models as infinite trees:



Here, truth assignments depend on states:

e.g. $\tau(p, s_0) = 1$

$\tau(p, s_1) = 0$



Examples:

<u>Def</u> A path π in a model $M=(S,\to,L)$ is an infinite sequence of states

$$s_1, s_2, s_3, \ldots$$

s.t. for all $i \geq 1$, $s_i \to s_{i+1}$.

We write $s_1 \to s_2 \to s_3 \to \ldots$

Notation:

π^i = suffix starting at s_i

e.g. $\pi^3 = s_3 \to s_4 \to \ldots$

Let $M=(S,\to,L)$ be a model,

let $\pi = s_1 \to s_2 \to \ldots$

be a path in M.

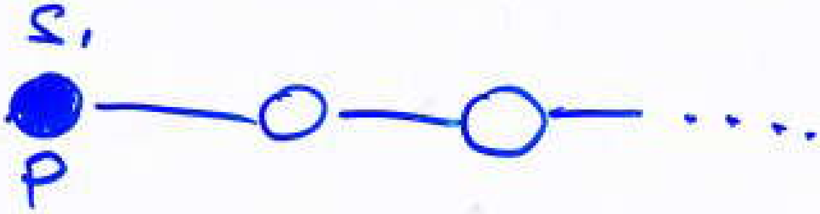
Def. φ is true in path π

$\parallel$

satisfied

($= \pi$ satisfies φ)

1. $\pi \models \top$
2. $\pi \not\models \bot$
3. $\pi \models p$ iff $p \in L(s_1)$



4. $\pi \models \neg\varphi$ iff $\pi \not\models \varphi$
5. $\pi \models \varphi_1 \wedge \varphi_2$ iff $\pi \models \varphi_1$ and $\pi \models \varphi_2$
6. $\pi \models \varphi_1 \vee \varphi_2$ iff $\pi \models \varphi_1$ or $\pi \models \varphi_2$
7. $\pi \models \varphi_1 \to \varphi_2$ iff $\pi \models \varphi_2$ whenever $\pi \models \varphi_1$

8. $\pi \models X\varphi$ iff $\pi^2 \models \varphi$

9. $\pi \models G\varphi$ iff for all i, $i \geq 1$ $\pi^i \models \varphi$

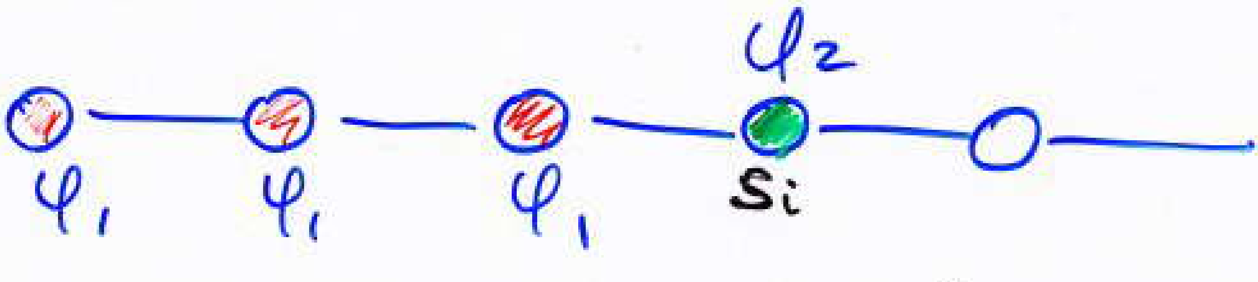
10. $\pi \models F\varphi$ iff exists i, $i \geq 1$ s.t. $\pi^i \models \varphi$

11. $\pi \models \varphi_1 U \varphi_2$ iff

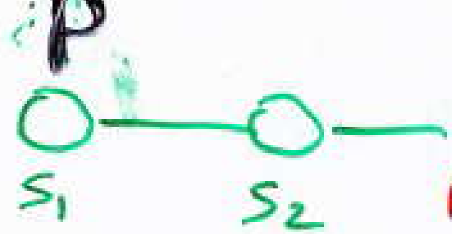
there is $i \geq 1$ s.t. $\pi^i \models \varphi_2$

and for all $j = 1, .., i-1$

we have $\pi^i \models \varphi_1$



$\pi \overset{?}{\models} q\, U\, p$ yes

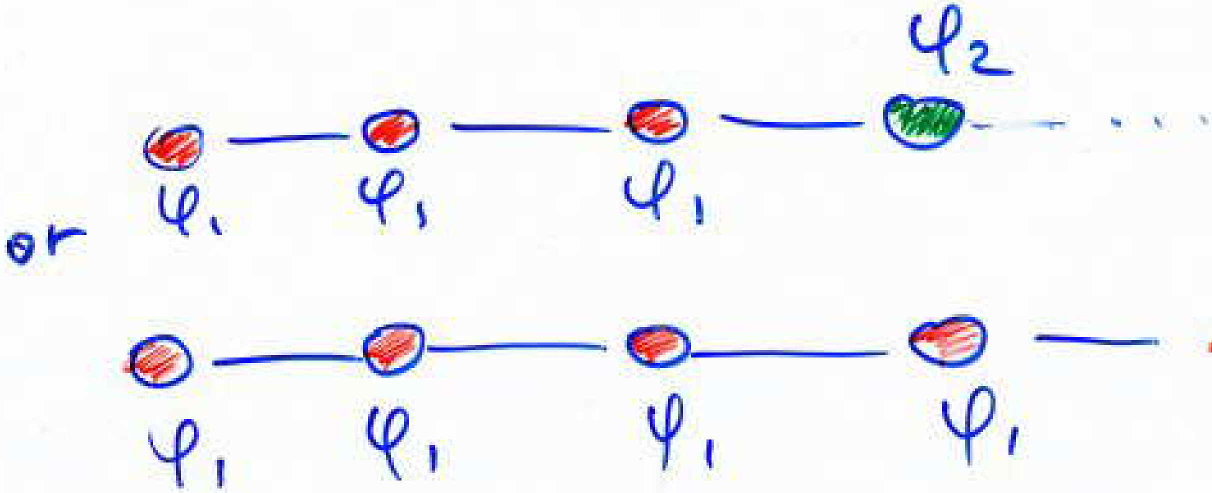


the set of states preceding s_1 is empty

12. $\pi \models \varphi_1 W \varphi_2$ iff either

there is $i \geq 1$ s.t. $\pi^i \models \varphi_2$
and for all $j = 1, \ldots, i-1$, $\pi^j \models \varphi_1$

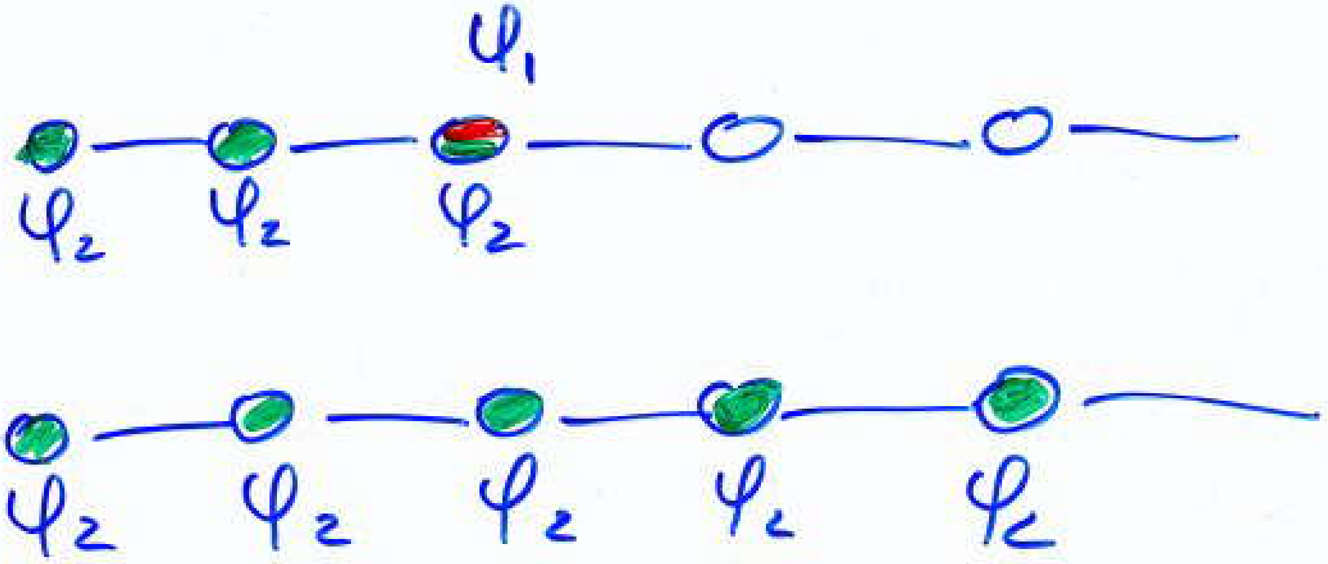
<u>**Or**</u> for all $k \geq 1$ $\pi^k \models \varphi_1$



13. $\pi \models \varphi_1 R \varphi_2$ iff either

there is some $i \geq 1$ s.t. $\pi^i \models \varphi_1$
and for all $j = 1, \ldots, i$, $\pi^j \models \varphi_2$

or $\pi^k \models \varphi_2$ for all $k \geq 1$.



Def Sup. $M = (S, \rightarrow, L)$ is a model, $s \in S$, and φ an LTL formula.

$M, s \vDash \varphi$ if for every path π of M starting at s, we have $\pi \vDash \varphi$.