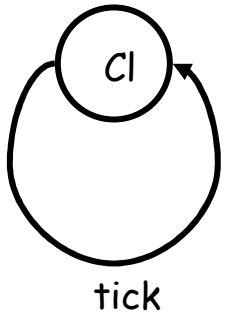
Modal and Temporal Logic

Transition systems

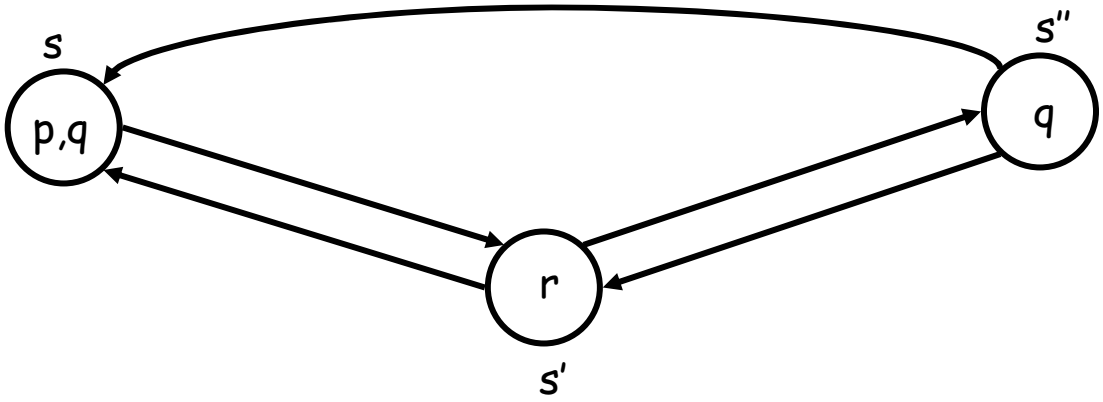
a set of states S
a set of labels A
a set of transitions: $s \xrightarrow{a} s_0$ where $s, s_0 \in S, a \in A$



Here: $S = \{Cl\}$, $A = \{tick\}$, and $Cl \xrightarrow{tick} Cl$

Kripke structures

Labels appear at states ("colours") often instead of on transitions



Modal Logic: Syntax

$\Phi ::= tt \mid ff \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\,\Phi \mid \langle K \rangle\,\Phi$

A formula can be

- the constant true (formula tt), the constant false (formula ff),
- a conjunction of formulas $\Phi_1 \wedge \Phi_2$, a disjunction of formulas $\Phi_1 \vee \Phi_2$,
- a formula $[K]\,\Phi$, where K is any set of actions, read as "box K Φ", or "for all K-derivatives .,"
- a formula $\langle K \rangle\,\Phi$, where K is any set of actions, read as "diamond K Φ", or "for some K-derivative .."

Modal Logic: Semantics

We define when a state E of a transition system satisfies a formula Φ.

Either E satisfies Φ, $E \models \Phi$, or it doesn't, $E \not\models \Phi$

$E \models tt$

$E \not\models ff$

$E \models \Phi_1 \wedge \Phi_2$ iff $E \models \Phi_1$ and $E \models \Phi_2$

$E \models \Phi_1 \vee \Phi_2$ iff $E \models \Phi_1$ or $E \models \Phi_2$

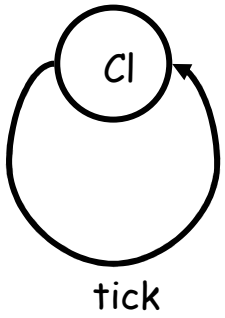
$E \models [K]\Phi$ iff $\forall F \in \{E' : E \xrightarrow{a} E' \text{ and } a \in K\}: F \models \Phi$

$E \models [K]\Phi$ iff $\exists F \in \{E' : E \xrightarrow{a} E' \text{ and } a \in K\}: F \models \Phi$

Examples

1. E ⊨ <tick>tt from E there is a tick transition.
2. E ⊨<tick><tock>tt from E there is a tick and then a tock transition.
3. E ⊨<{tick,tock}>tt from E there is a tick or a tock transition.
4. E ⊨ [tick]ff there is not a tick transition from E.
5. E ⊨<tick>ff this is "equivalent" to ff
6. E ⊨ [tick]tt this is "equivalent" to true

Checking satisfaction



Does Cl have the property [tick](<tick>tt ∧ [tock]ff) ?

Checking satisfaction

$Cl \models [tick](\langle tick\rangle tt \wedge [tock]ff)$

iff $\forall F \in \{E : Cl \xrightarrow{tick} E\}: F \models \langle tick\rangle tt \wedge [tock]ff$

iff $Cl \models \langle tick\rangle tt \wedge [tock]ff$

iff $Cl \models \langle tick\rangle tt$ and $Cl \models [tock]ff$

iff $\exists F \in \{E : Cl \xrightarrow{tick} E\}$ and $Cl \models [tock]ff$

iff $\exists F \in \{Cl\}$ and $Cl \models [tock]ff$

iff $Cl \models [tock]ff$

iff $\{E : Cl \xrightarrow{tock} E\} = \emptyset$

iff $\emptyset = \emptyset$

Syntactic sugar

Let A be a set of all actions.

We write

- $a_1, \ldots a_n$ for $\{a_1, \ldots a_n\}$
- $-$ for the set A
- $-K$ for the set $A - K$
- $- a_1, \ldots a_n$ for $A - \{a_1, \ldots a_n\}$

More examples

$E \models [-]ff$: E is deadlocked

$E \models \langle - \rangle tt$: some action can be executed from E

$E \models \langle - \rangle tt \wedge [-a]ff$: a must happen next from E

(Something can happen, and nothing but a can happen.)

$E \models \langle - \rangle tt \wedge [-]\Phi$: Φ holds after one step

$E \models \langle - \rangle tt \wedge [-](\langle - \rangle tt \wedge [-](\langle - \rangle tt \wedge [-a]ff))$: ?

Negation

Modal logic can be extended with a negation operator : $E \models \neg\Phi$ iff $E \not\models \Phi$

Negation is redundant: For every Φ there is Φ^c such that for any E

$E \models \Phi^c$ iff $E \not\models \Phi$

Φ^c is inductively defined as follows:

$$tt^c = ff \qquad ff^c = tt$$

$$(\Phi_1 \wedge \Phi_2)^c = \Phi_1{}^c \vee \Phi_2{}^c \qquad (\Phi_1 \vee \Phi_2)^c = \Phi_1{}^c \wedge \Phi_2{}^c$$

$$([K]\,\Phi)^c = \langle K\rangle\Phi^c \qquad (\langle K\rangle\Phi)^c = [K]\,\Phi^c$$

Negation

Proposition: For every state F and formula Φ: $F \models \Phi^c$ iff $F \not\models \Phi$

Proof: By induction on the structure of Φ.

Basis: Φ = tt and Φ = ff. Trivial.

Induction step:

Case $\Phi = \Phi_1 \wedge \Phi_2$

$F \models (\Phi_1 \wedge \Phi_2)^c$

iff $F \models \Phi_1^c \vee \Phi_2^c$

iff $F \models \Phi_1^c$ or $F \models \Phi_2^c$ (by clause for $\vee$)

iff $F \not\models \Phi_1$ or $F \not\models \Phi_2$ (by i.h.)

iff $F \not\models \Phi_1 \wedge \Phi_2$ (by clause for $\wedge$)

Satisfiability, validity, equivalence

A formula is satisfiable if some state of a transition system satisfies it.

A formula is unsatisfiable if no state of any transition system satisfies it.

A formula is valid if all states of all transition systems satisfy it.

Two formulas are equivalent if they are satisfied by exactly the same states of any transition system.

Exercise

Are the following statements true?

If Φ valid then Φ satisfiable

If Φ satisfiable then Φ^c unsatisfiable

If Φ valid then Φ^c unsatisfiable

If Φ unsatisfiable then Φ^c valid

Exercise

Are the following statements true?

If $(\Phi \Rightarrow \Psi)$ valid and Φ valid then Ψ valid

If $(\Phi \Rightarrow \Psi)$ satisfiable and Φ satisfiable then Ψ satisfiable

If $(\Phi \Rightarrow \Psi)$ valid and Φ satisfiable then Ψ satisfiable

Exercise

Are the following formulas valid, unsatisfiable or satisfiable (Φ and Ψ are arbitrary modal formulas)?

$\langle a \rangle tt \wedge [a] ff$

$\langle a \rangle [b] (\langle a \rangle tt \wedge [a] ff)$

$\langle a \rangle [b] (\langle a \rangle tt \wedge [a] ff) \wedge [-] \langle b \rangle tt$

$\langle a \rangle [b] (\langle a \rangle tt \wedge [a] ff) \wedge [-] \langle - \rangle tt$

$\langle a \rangle (\Phi \vee \Psi) \Rightarrow (\langle a \rangle \Phi \vee \langle a \rangle \Psi)$

Bisimulation invariance

A binary relation B between states of a transition system is a bisimulation provided that, whenever $(E, F) \in B$ and $a \in A$,

- if $E \xrightarrow{a} E'$ then $F \xrightarrow{a} F'$ for some F' such that $(E', F') \in B$, and

- if $F \xrightarrow{a} F'$ then $E \xrightarrow{a} E'$ for some E' such that $(E', F') \in B$

Two states E and F are bisimulation equivalent, $E \sim F$, if there is a bisimulation relation B such that $(E, F) \in B$.

Bisimulation invariance

$E \equiv F$ if for all modal Φ, $E \models \Phi$ iff $F \models \Phi$ (E and F have the same modal properties.)

A transition system is finitely branching if for each $a \in A$ and state E, the set $\{F : E \xrightarrow{a} F\}$ is finite.

Bisimulation invariance

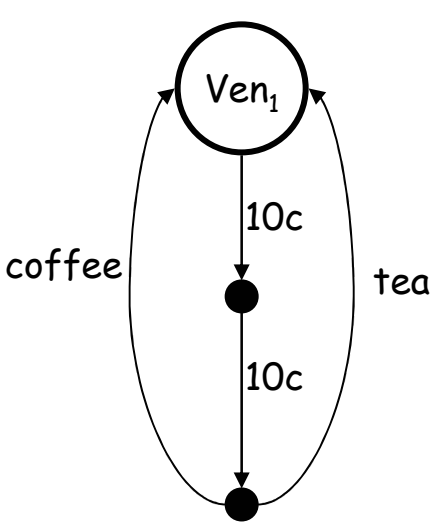
Two bisimulation equivalent states have the same modal properties.

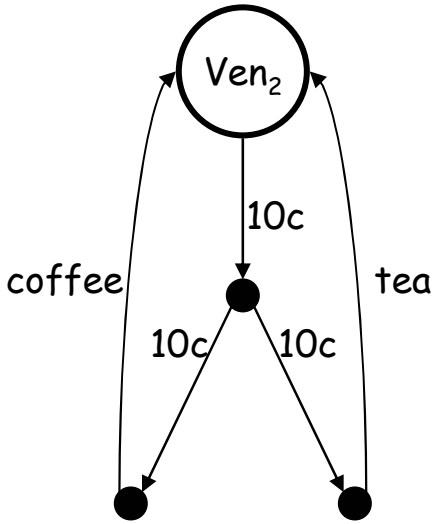
Proposition If $E \sim F$ then $E \equiv F$.

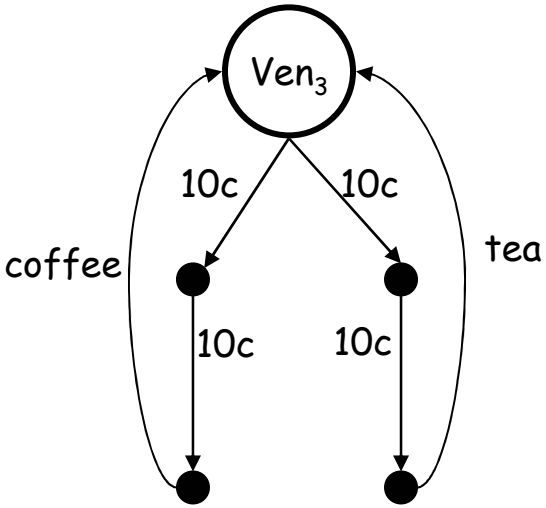
Proposition If E and F belong to a finitely branching transition system and $E \equiv F$ then $E \sim F$.

Exercises

Consider the following three vending machines, Ven_i, $1 \leq i \leq 3$.







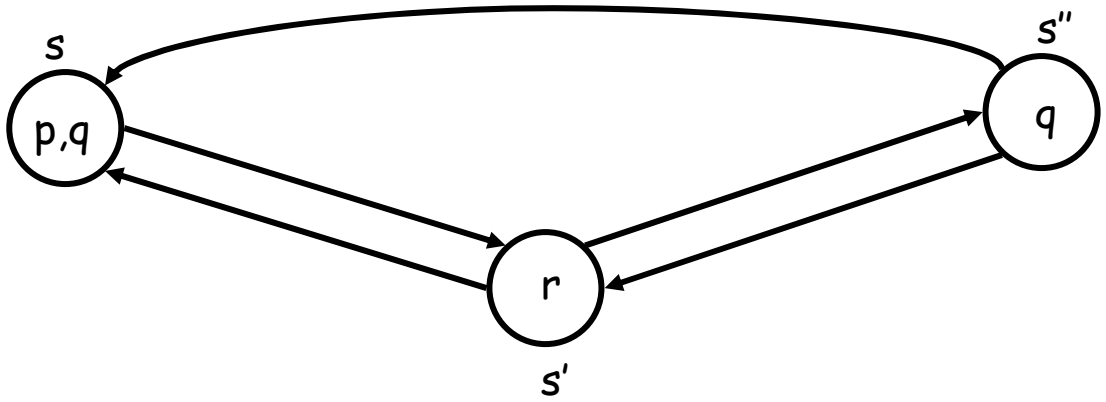
Provide 3 modal formulas Φ_i, such that $Ven_i \models \Phi_i$ and $Ven \not\models \Phi_j$ when $i \neq j$.

Variants

Take Kripke structures where labels appear at states ("colours") instead of on transitions.

Kripke model is a Kripke structure + a labelling function

$$L : S \to \text{Colours} \qquad (S \text{ are states}).$$



Variants

Assume p ranges over colours

Modal Logic:

Syntax

$\Phi ::= p \mid \neg p \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [-]\Phi \mid \langle - \rangle \Phi$

Semantics

$E \models p$	iff	$E \in L(p)$
$E \not\models \neg p$	iff	$E \notin L(p)$
$E \models \Phi_1 \wedge \Phi_2$	iff	$E \models \Phi_1$ and $E \models \Phi_2$
$E \models \Phi_1 \vee \Phi_2$	iff	$E \models \Phi_1$ or $E \models \Phi_2$
$E \models [-]\Phi$	iff	$\forall F \in \{E' : E \rightarrow E'\}: F \models \Phi$
$E \models \langle - \rangle \Phi$	iff	$\exists F \in \{E' : E \rightarrow E'\}: F \models \Phi$

Properties

- Mutual exclusion
- Absence of deadlocks
- Absence of starvation

PROBLEM: None of these properties is expressible in modal logic!

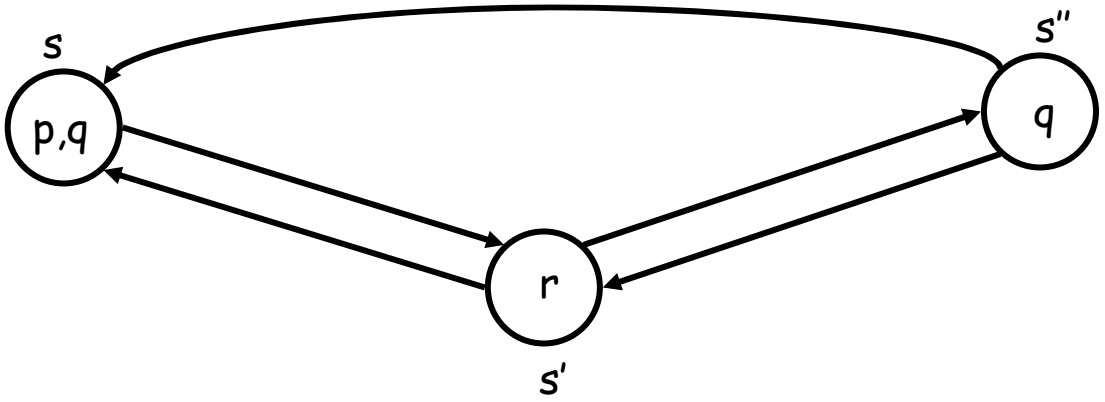
Modal logic cannot express "longterm properties" such as absence of deadlock

Runs in a transition system

A run from state E_0 is a finite or infinite length sequence of transitions

$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots \xrightarrow{a_n} E_n \xrightarrow{a_{n+1}} \ldots$ with "maximal" length.

Similarly, for a Kripke model.



Then an example run is $s \to s' \to s'' \to s \to \ldots$

Runs in a transition system

Runs provide a means for expressing long term features.

Mutual exclusion: no run has the property that two components are in their critical section at the same time.

Absence of deadlock: every run has infinite length

Absence of starvation: in every run if a component requests entry into critical section then eventually that component will be in its critical section

Temporal operators on runs

Next: (K) Φ

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots \rightarrow E_i \xrightarrow{a_{i+1}}$$

$a_1 \in K \qquad \models \Phi \qquad \ldots$

Until: Φ U Ψ

Note: the index i can be 0

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots \rightarrow E_i \xrightarrow{a_{i+1}}$$

$\models \Phi \qquad \models \Phi \qquad \models \Psi$

Temporal operators on runs

Eventually: $F\,\Psi = tt\ U\ \Psi$ Note: the index i can be 0

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots \rightarrow E_i \xrightarrow{a_{i+1}}$$
$$\ldots \qquad \models \Psi \qquad \ldots$$

Always: $G\,\Psi = \neg F \neg\, \Psi$

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots \rightarrow E_i \xrightarrow{a_{i+1}}$$
$$\models \Psi \qquad \models \Psi \qquad \models \Psi \quad \ldots$$

Linear time temporal logic (LTL)

Syntax

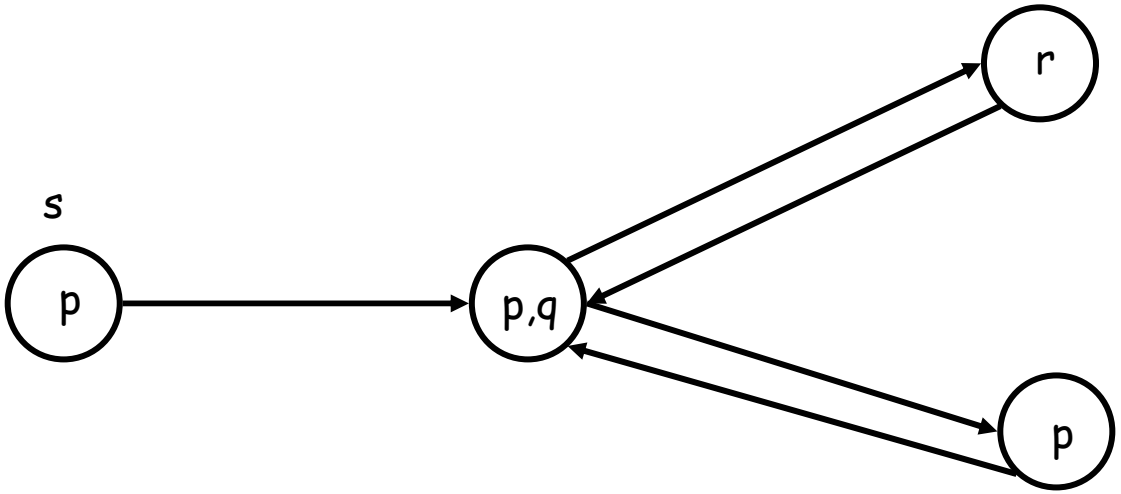
$\Phi ::= p \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid (\text{-})\,\Phi \mid \Phi\ U\ \Psi$

Semantics

A state E of a Kripke model satisfies an LTL formula Φ,

written $E \models \Phi$, if for any run π from E, the run $\pi \models \Phi$.

Exercise



Which of the following are true?

$s \models p \, U \, q$

$s \models F \, p$

$s \models F(G \, r \vee G \, p)$

$s \models F \, r$

$s \models G \, (p \vee r)$

Branching time logic

For each temporal operator such as F (eventually), create two variants

1. AF "for all runs eventually" (strong)
2. E F "for some run eventually" (weak)

Modal operators are also branching time temporal operators

[K] = A¬(K) ¬

<K> = E (K)

Therefore, we can extend modal logic with branching time temporal operators.

Computational tree logic (CTL)

Syntax $\Phi ::= tt \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \langle K \rangle \Phi \mid A\,(\Phi\ U\ \Psi) \mid E\,(\Phi\ U\ \Psi)$

Semantics

$E \models \neg\Phi$ iff $E \not\models \Phi$

$E_0 \models A\,(\Phi\ U\ \Psi)$ iff for all runs $E_0 \xrightarrow{a_1} E1 \xrightarrow{a_2} \ldots$ there is $i \geq 0$ with $E_i \models \Psi$ and for all j: $0 \leq j < i$, $E_j \models \Phi$.

$E_0 \models E\,(\Phi\ U\ \Psi)$ iff for some run $E_0 \xrightarrow{a_1} E1 \xrightarrow{a_2} \ldots$ there is $i \geq 0$ with $E_i \models \Psi$ and for all j: $0 \leq j < i$, $E_j \models \Phi$.

Derived operators

$A\ F\ \Phi = A\ (tt\ U\ \Phi)$

$E\ F\ \Phi = E\ (tt\ U\ \Phi)$

$A\ G\ \Phi = \neg\ E\ F\ \neg\Phi$

$E\ G\ \Phi = \neg\ A\ F\ \neg\Phi$

Safety "nothing bad ever happens": in every run bad is never true.

A G good

Liveness "something good eventually happens": in every run good is eventually true. A F good

Weak Safety in some run bad is never true. E G good

Weak Liveness in some run good is eventually true. E F good

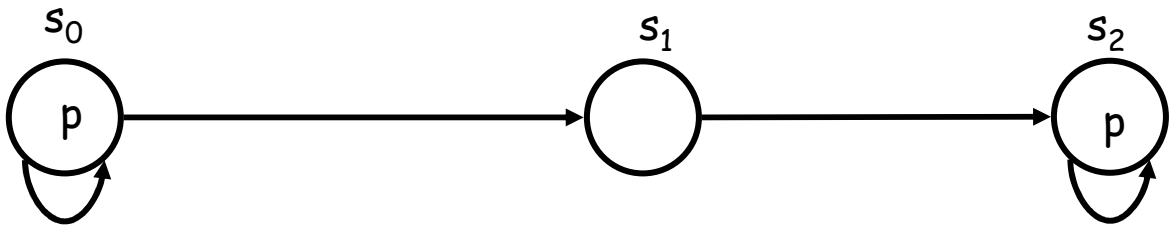
Examples

Absence of deadlock: A G <-> tt

Absence of starvation (for one component): A G ([req1] A F <exit1> tt)

Expressivity of CTL and LTL

Consider the property: on every path there is a point after which p is always true



Cannot express this in CTL

- would need something like AF P
- where P is something like: property p true from now on
- but P must start with a path quantifier A or E
- so cannot talk about current path, only about all or some paths

Note: property true, but AF AG p false (consider path $s_0 s_0 s_0 \ldots$)

Expressivity of CTL and LTL

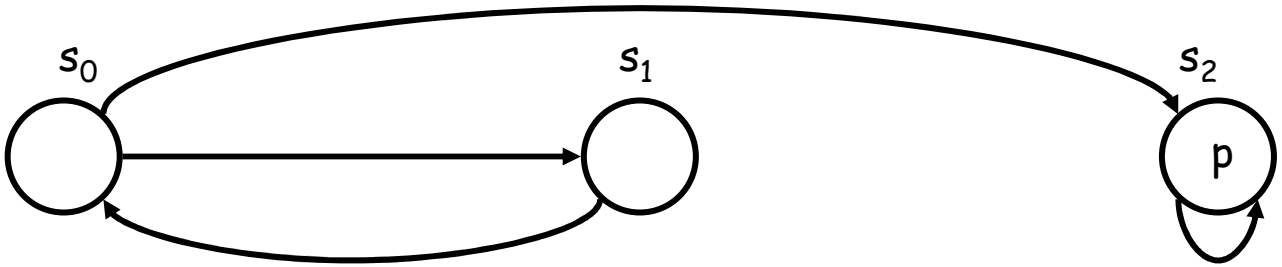
The property can be expressed in LTL: F G p

On the other hand the property

A G (E F p)

from every state it is possible to get to a state for which p holds

cannot be expressed in LTL



CTL* is the logic obtained by the union of LTL and CTL

Model Checking CTL formulas

$||\Phi|| = \{E \mid E \models \Phi\}$

Model checking is "bottom up" by computing $||\Psi||$ for any subformula of Φ and then computing $||\Phi||$

- $\neg ||\Phi|| = - ||\Phi||$,
- $||\Phi_1 \wedge \Phi_2|| = ||\Phi_1|| \cap ||\Phi_2||$
- $||\langle K \rangle \Phi_1|| = \{F \mid \exists F' \in ||\Phi||, a \in K . F \xrightarrow{a} F'\}$

Model Checking CTL formulas

$||E(\Phi\ U\ \Psi)|| = \bigcup_{S_i} S_i$

where $S_1 = ||\Psi||$ and $S_{i+1} = S_i \cup \{F \in ||\Phi||: \exists\ a, F' \in S_i.\ F \xrightarrow{a} F'$

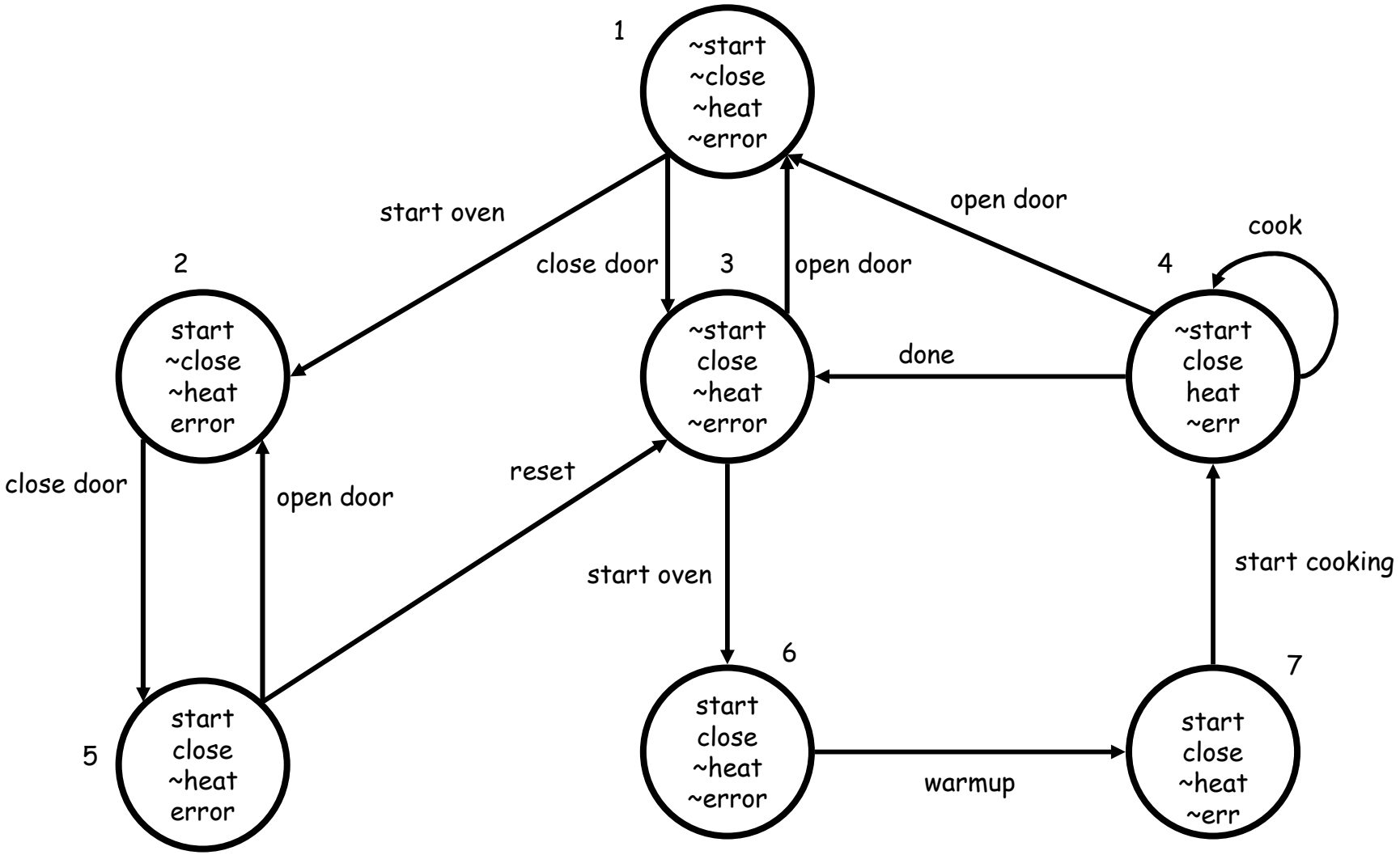
$||A(\Phi\ U\ \Psi)|| = \bigcup_{S_i} S_i$

where $S_1 = ||\Psi||$

and $S_{i+1} = S_i \cup \{F \in ||\Phi||:$ $\exists\ a, F'.\ F \xrightarrow{a} F'$ and

$\forall\ a, F'.$ if $F \xrightarrow{a} F'$ then $F' \in S_i\}$

Example: a microwave oven



Example: a microwave oven

We check the CTL formula $A\ G\ (start \Rightarrow A\ F\ heat)$
which is equivalent to $\neg\ E\ F\ (start \wedge E\ G \neg\ heat)$

$||\ start\ || = \{2,5,6,7\}$
$||\ \neg\ heat\ || = \{1,2,3,5,6\}$

$||\ E\ G \neg\ heat\ || = \{1,2,3,5\}$

$||\ E\ F\ (start \wedge E\ G \neg\ heat)\ || = \{1,2,3,4,5,6,7\}$

$||\ \neg\ E\ F\ (start \wedge E\ G \neg\ heat)\ || = \varnothing$

The initial state 1 does not satisfy the property.