CS181u Applied Logic & Automated Reasoning

Lecture 7

Transition Systems

Linear Temporal Logic

Next Few Weeks:

Linear Temporal Logic (LTL)

We will assign symbols for expressing temporal system requirements like *always* (G), *eventually* (F), *next* (X), *until* (U), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems

We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts

Safety, liveness, mutual exclusion, ...

Temporal Logic Software

Symbolic Model Verifier (NuSMV)

Next Few Weeks:

Linear Temporal Logic (LTL)

We will assign symbols for expressing temporal system requirements like *always* (G), *eventually* (F), *next* (X), *until* (U), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems

We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

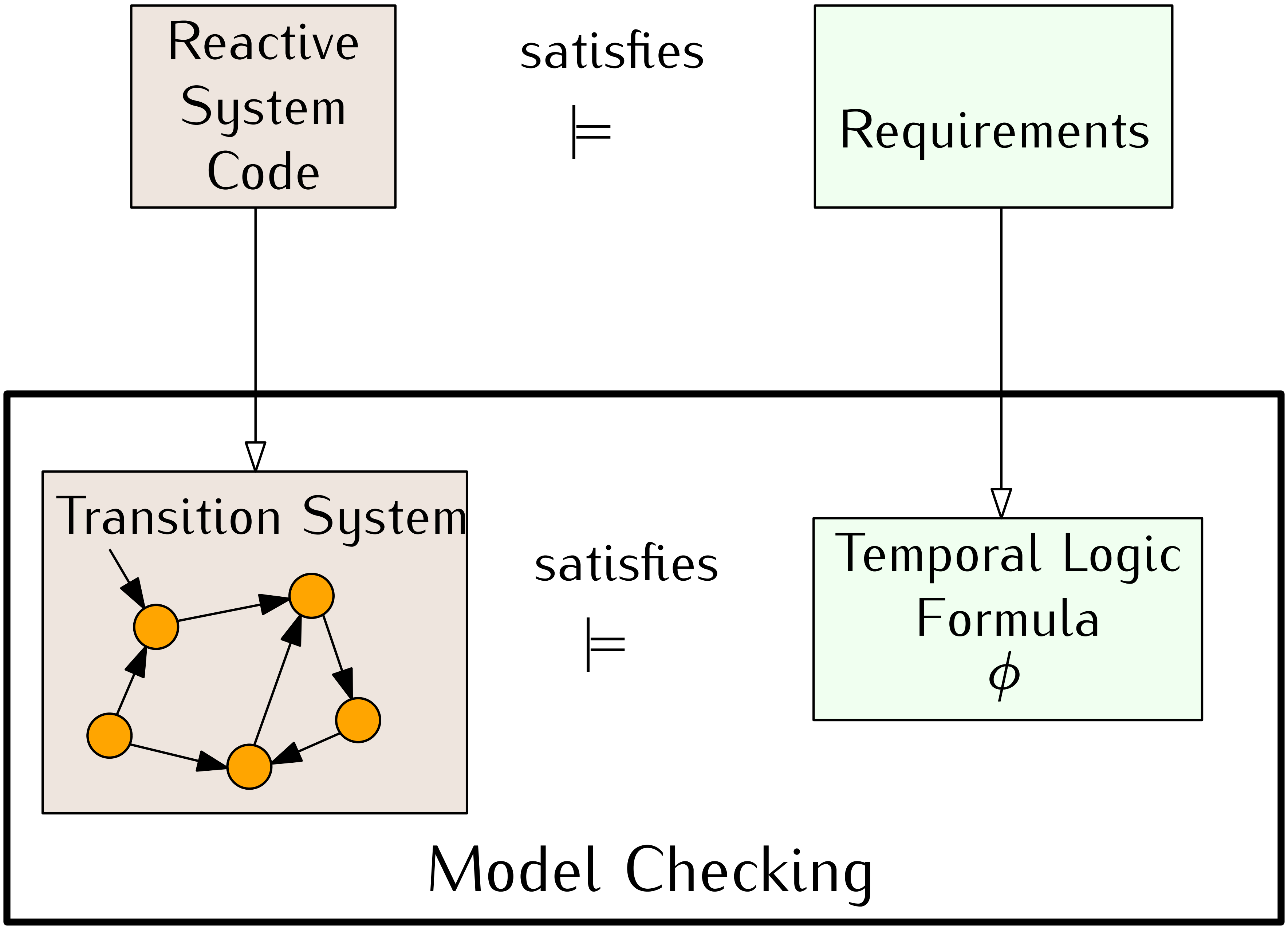
Concurrency Concepts

Safety, liveness, mutual exclusion, ... Today

Temporal Logic Software

Symbolic Model Verifier (NuSMV)

Remember the big picture



COMPUTER SECURITY

Hacker-Proof Code Confirmed

Actual specifications are subtler than a trip to the grocery store. Programmers may want to write a program that notarizes and time-stamps documents in the order in which they're received (a useful tool in, say, a patent office). In this case the specification would need to explain that the counter always increases (so that a document received later always has a higher number than a document received earlier) and that the program will never leak the key it uses to sign the documents.

Many important properties have a temporal component.

The light eventually turns green.

The door eventually opens.

Two processes are never in the critical section at the same time.

Sometime

Always

After

Never

Next

Forever

Finitely often

Eventually

Impossible

Until

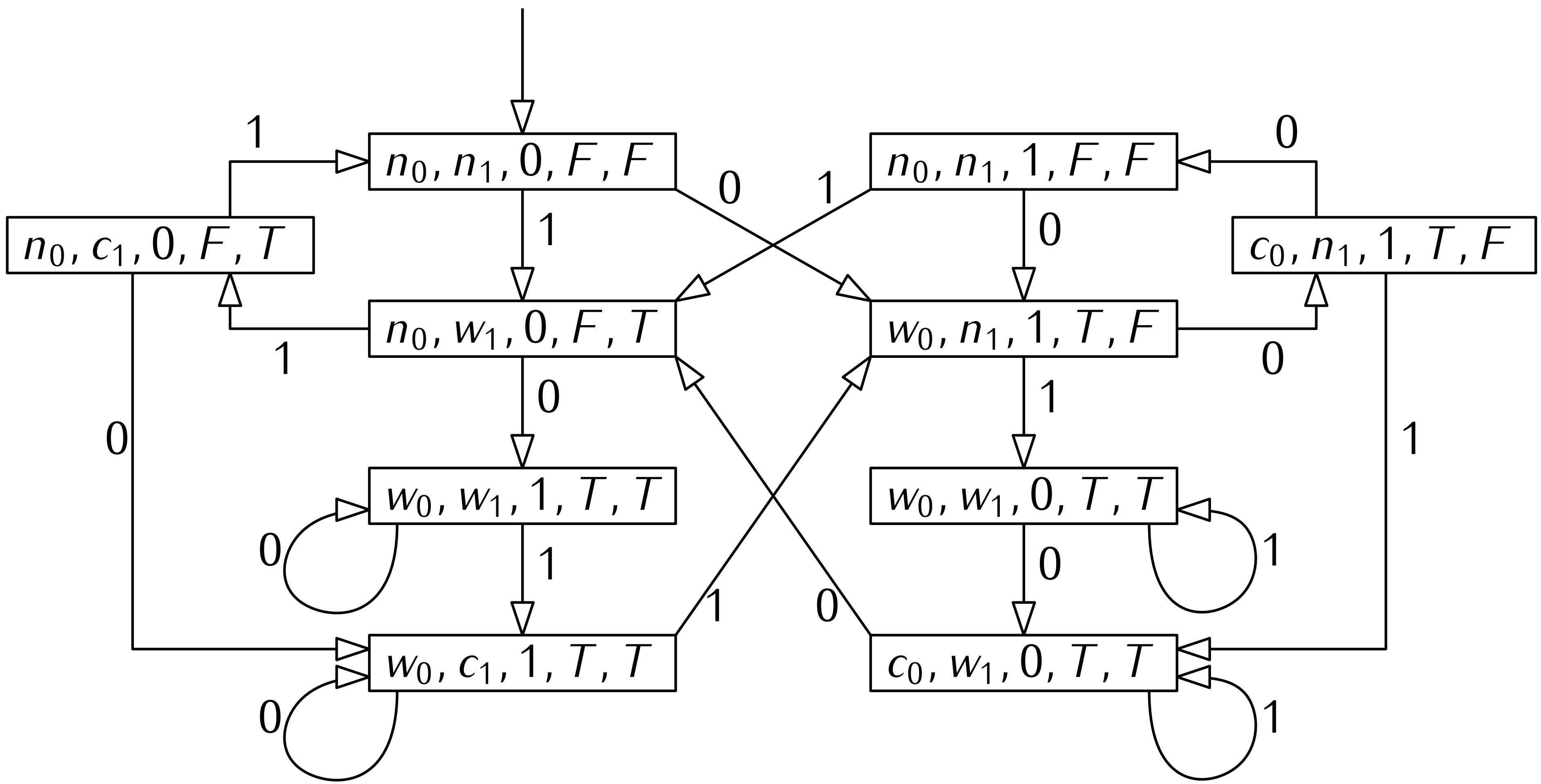
Infinitely often

Before

Temporal Logic and Transition Systems

We will give meaning to temporal logic formulas with respect to transitions systems. So, let's talk about transition systems first.

Transition system for $P_0||P_1$ from in-class activity.



Transition Systems

A transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is a set of states S and a set of initial states I, along with a transition relation $\rightarrow$ and labelling function L.

The transition relation $\rightarrow$ is equivalent to a set of directed graph edges, with the states as nodes.

For example, $((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T)) \in \rightarrow$

Alternatively, we can write
$(n_0, n_1, 0, F, F) \rightarrow (n_0, w_1, 0, F, T)$.

Important assumption: no dead states. Every state has an outgoing transition, even if only to itself.

Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$

Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$

For example, one path from our two-process mutual exclusion transition diagram:

$((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T), (n_0, c_1, 0, F, T))^\omega$

Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$

For example, one path from our two-process mutual exclusion transition diagram:

$((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T), (n_0, c_1, 0, F, T))^\omega$

We will use the symbol π for paths.
We write $\pi = s_1, s_2, s_3 \ldots$
We write π^i to indicate the ith suffix of π.
e.g. $\pi^3 = s_3, s_4, s_5 \ldots$

Transition System Example

$$S = \{0, 1, 2\} \qquad I = \{0\} \qquad AP = \{p, q, r\}$$

$$\rightarrow = \{(0, 1), (1, 0), (0, 2), (1, 2)\}$$

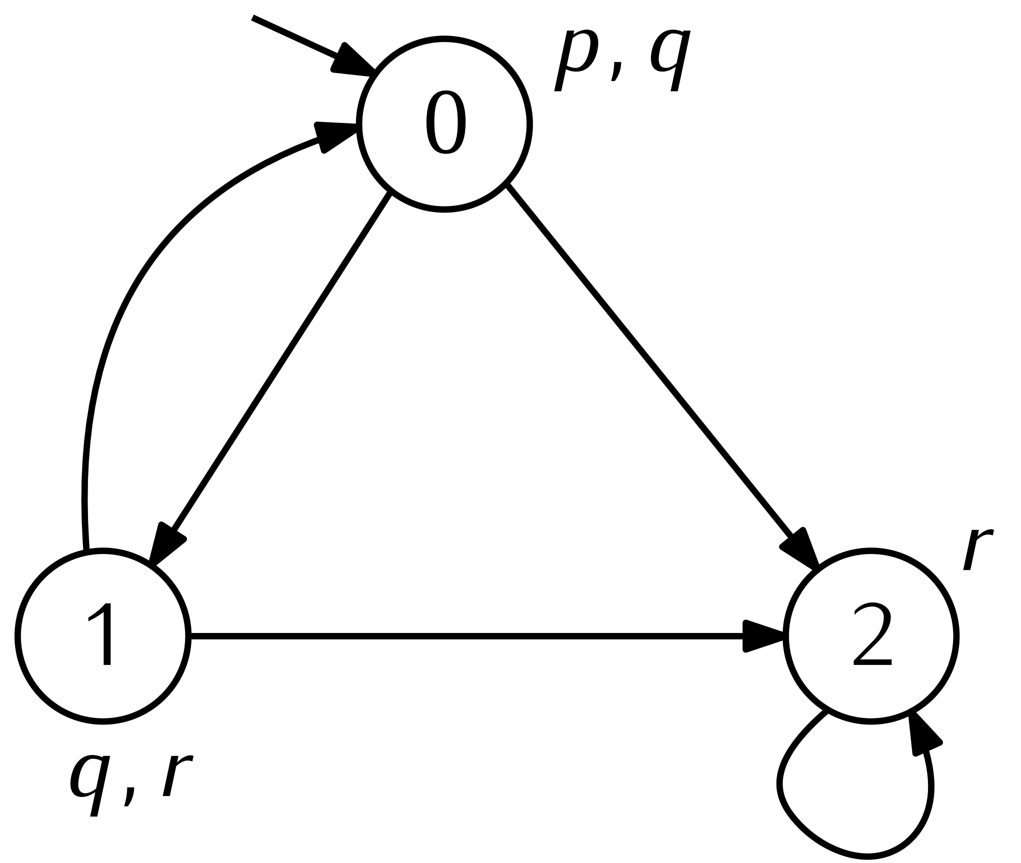
$$L(0) = \{p, q\} \qquad L(1) = \{q, r\} \qquad L(2) = \{r\}$$

Transition System Example

$$S = \{0, 1, 2\} \qquad I = \{0\} \qquad AP = \{p, q, r\}$$

$$\rightarrow = \{(0, 1), (1, 0), (0, 2), (1, 2)\}$$

$$L(0) = \{p, q\} \qquad L(1) = \{q, r\} \qquad L(2) = \{r\}$$



Syntax of Linear Temporal Logic Formulas

Suppose α and β are LTL formulas.
Suppose p_i is a propositional atom.
Then the following are all LTL formulas.

$$\top$$

$$\bot$$

Syntax of Linear Temporal Logic Formulas

Suppose α and β are LTL formulas.
Suppose p_i is a propositional atom.
Then the following are all LTL formulas.

$$\top$$

$$\bot$$

$$p_i$$

Syntax of Linear Temporal Logic Formulas

Suppose α and β are LTL formulas.
Suppose p_i is a propositional atom.
Then the following are all LTL formulas.

$$\top$$

$$\bot$$

$$p_i$$

$$\neg\alpha \quad \alpha \vee \beta \qquad \alpha \wedge \beta \quad \alpha \rightarrow \beta$$

Syntax of Linear Temporal Logic Formulas

Suppose α and β are LTL formulas.
Suppose p_i is a propositional atom.
Then the following are all LTL formulas.

$$\top$$

$$\bot$$

$$p_i$$

$$\neg\alpha \quad \alpha \vee \beta \qquad \alpha \wedge \beta \quad \alpha \rightarrow \beta$$

$$G\alpha \quad F\alpha \quad X\alpha \quad \alpha U\beta \quad \alpha R\beta \quad \alpha W\beta$$

Syntax of Linear Temporal Logic Formulas

Suppose α and β are LTL formulas.
Suppose p_i is a propositional atom.
Then the following are all LTL formulas.

$$\top$$

$$\bot$$

$$p_i$$

$$\neg\alpha \quad \alpha \vee \beta \quad \alpha \wedge \beta \quad \alpha \rightarrow \beta$$

$$\underbrace{G\alpha \quad F\alpha \quad X\alpha \quad \alpha U\beta}_{\text{Today's focus}} \quad \alpha R\beta \quad \alpha W\beta$$

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**
$\pi \models p \wedge q$	iff	$\pi \models p \wedge \pi \models q$	p and q hold **now**
$\pi \models p \vee q$	iff	$\pi \models p \vee \pi \models q$	p or q hold **now**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**
$\pi \models p \wedge q$	iff	$\pi \models p \wedge \pi \models q$	p and q hold **now**
$\pi \models p \vee q$	iff	$\pi \models p \vee \pi \models q$	p or q hold **now**
$\pi \models Xp$	iff	$\pi^2 \models p$	p holds **next**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**
$\pi \models p \wedge q$	iff	$\pi \models p \wedge \pi \models q$	p and q hold **now**
$\pi \models p \vee q$	iff	$\pi \models p \vee \pi \models q$	p or q hold **now**
$\pi \models Xp$	iff	$\pi^2 \models p$	p holds **next**
$\pi \models Gp$	iff	$\forall i \geq 1 \quad \pi^i \models p$	p holds **always**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**
$\pi \models p \wedge q$	iff	$\pi \models p \wedge \pi \models q$	p and q hold **now**
$\pi \models p \vee q$	iff	$\pi \models p \vee \pi \models q$	p or q hold **now**
$\pi \models Xp$	iff	$\pi^2 \models p$	p holds **next**
$\pi \models Gp$	iff	$\forall i \geq 1 \quad \pi^i \models p$	p holds **always**
$\pi \models Fp$	iff	$\exists i \geq 1 \quad \pi^i \models p$	p holds **eventually**

Semantics of Linear Temporal Logic Formulas

Suppose π is a path and p and q are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula ϕ

$\pi \models p$	iff	$p \in L(s_1) \wedge p \in AP$	p holds **now**
$\pi \models \neg p$	iff	$\pi \not\models p$	$\neg p$ holds **now**
$\pi \models p \wedge q$	iff	$\pi \models p \wedge \pi \models q$	p and q hold **now**
$\pi \models p \vee q$	iff	$\pi \models p \vee \pi \models q$	p or q hold **now**
$\pi \models Xp$	iff	$\pi^2 \models p$	p holds **next**
$\pi \models Gp$	iff	$\forall i \geq 1 \quad \pi^i \models p$	p holds **always**
$\pi \models Fp$	iff	$\exists i \geq 1 \quad \pi^i \models p$	p holds **eventually**
$\pi \models pUq$	iff	$\exists i \geq 1 \;\; \pi^i \models q \;\; \wedge$ $\forall \;\; 1 \leq j < i \quad \pi^j \models p$	p holds **until** q holds

Semantics of Linear Temporal Logic Formulas

We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Semantics of Linear Temporal Logic Formulas

We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let's define what it means for a transition system to satisfy a property, $\mathcal{M} \models \phi$.

Semantics of Linear Temporal Logic Formulas

We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let's define what it means for a transition system to satisfy a property, $\mathcal{M} \models \phi$.

We say that transition system $\mathcal{M}$ satisfies property ϕ if for every path π of $\mathcal{M}$, $\pi \models \phi$.

Semantics of Linear Temporal Logic Formulas

We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let's define what it means for a transition system to satisfy a property, $\mathcal{M} \models \phi$.

We say that transition system $\mathcal{M}$ satisfies property ϕ if for every path π of $\mathcal{M}$, $\pi \models \phi$.

$$\mathcal{M} \models \phi \Leftrightarrow \forall \pi \; [\pi \models \phi]$$

LTL Model Checking

LTL Model Checking

$$\mathcal{M} \models \phi \Leftrightarrow \forall \pi \ [\pi \models \phi]$$

LTL Model Checking

$$\mathcal{M} \models \phi \Leftrightarrow \forall \pi \; [\pi \models \phi]$$

$$\mathcal{M} \not\models \phi \Leftrightarrow \exists \pi \; [\pi \models \neg \phi]$$

Counterexample path!

Some exercises

Does G distribute over $\vee$?

$$G(p \vee q) \equiv Gp \vee Gq \ ?$$

Some exercises

Does G distribute over $\vee$?

$$G(p \vee q) \equiv Gp \vee Gq \ ?$$

Does G distribute over $\wedge$?

$$G(p \wedge q) \equiv Gp \wedge Gq \ ?$$

Some exercises

Does G distribute over $\vee$?

$$G(p \vee q) \equiv Gp \vee Gq \ ?$$

Does G distribute over $\wedge$?

$$G(p \wedge q) \equiv Gp \wedge Gq \ ?$$

Does F distribute over $\vee$?

$$F(p \vee q) \equiv Fp \vee Fq \ ?$$

Does F distribute over $\wedge$?

$$F(p \wedge q) \equiv Fp \wedge Fq \ ?$$

Some exercises

Does G distribute over $\vee$?

$$G(p \vee q) \equiv Gp \vee Gq \ ?$$

Does G distribute over $\wedge$?

$$G(p \wedge q) \equiv Gp \wedge Gq \ ?$$

Does F distribute over $\vee$?

$$F(p \vee q) \equiv Fp \vee Fq \ ?$$

Does F distribute over $\wedge$?

$$F(p \wedge q) \equiv Fp \wedge Fq \ ?$$

Do U and X have any distributive properties?

$$X(p \vee q) \equiv \dots \qquad (p \wedge q)U(r \wedge t) \equiv \dots$$

Some exercises

Do G and F commute?

$$FGp \equiv GFp \quad ?$$

Some exercises

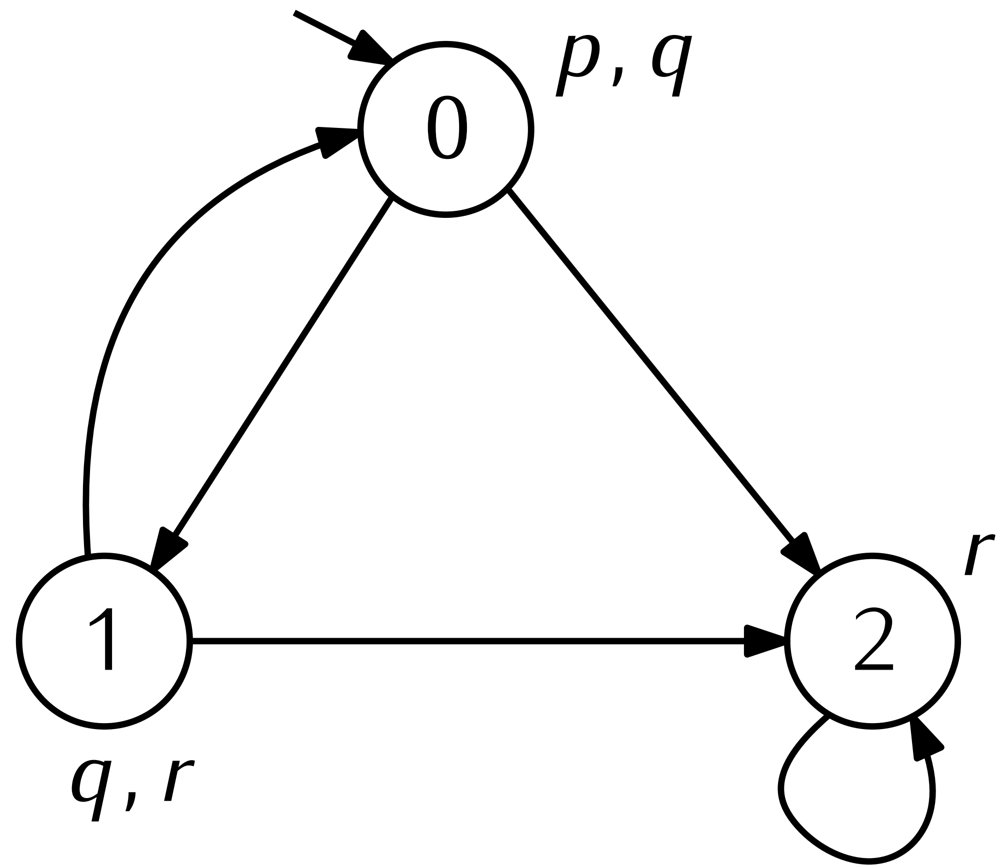
Do G and F commute?

$$FGp \equiv GFp \quad ?$$

FGp	$\mathcal{M}$ **converges** to p
GFp	**infinitely often** p

Transition System Example

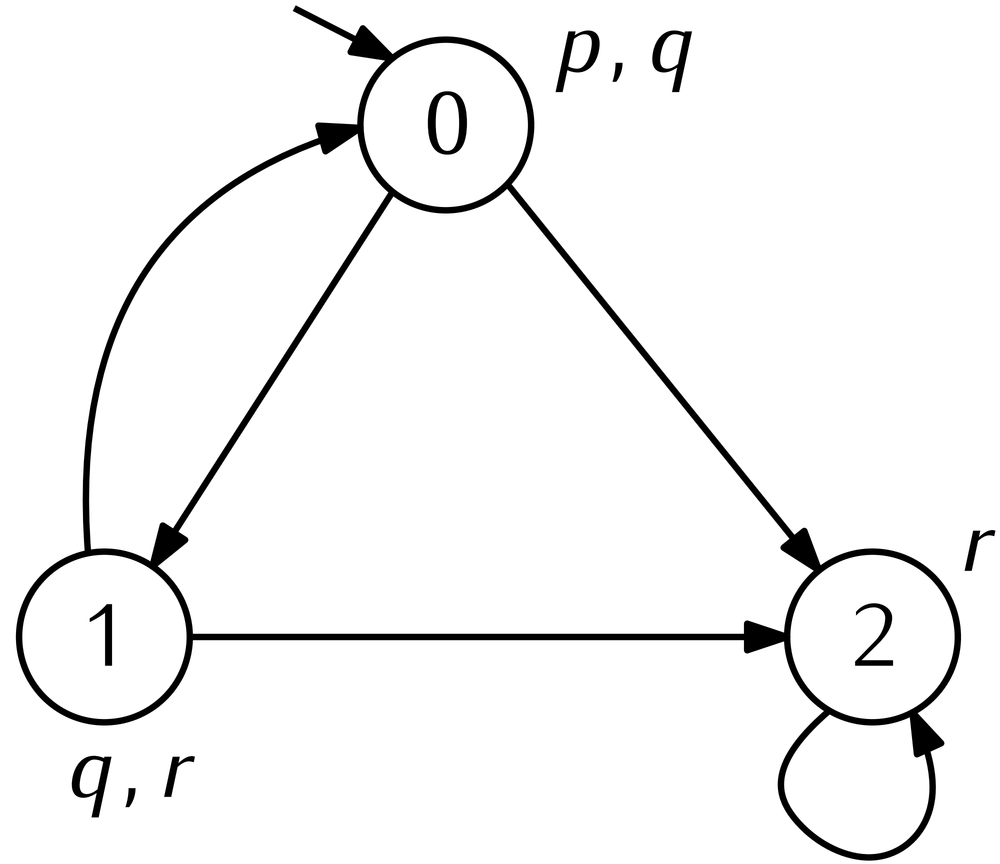
Do these properties hold?



Transition System Example

Do these properties hold?

$\mathcal{M} \models p \wedge q$

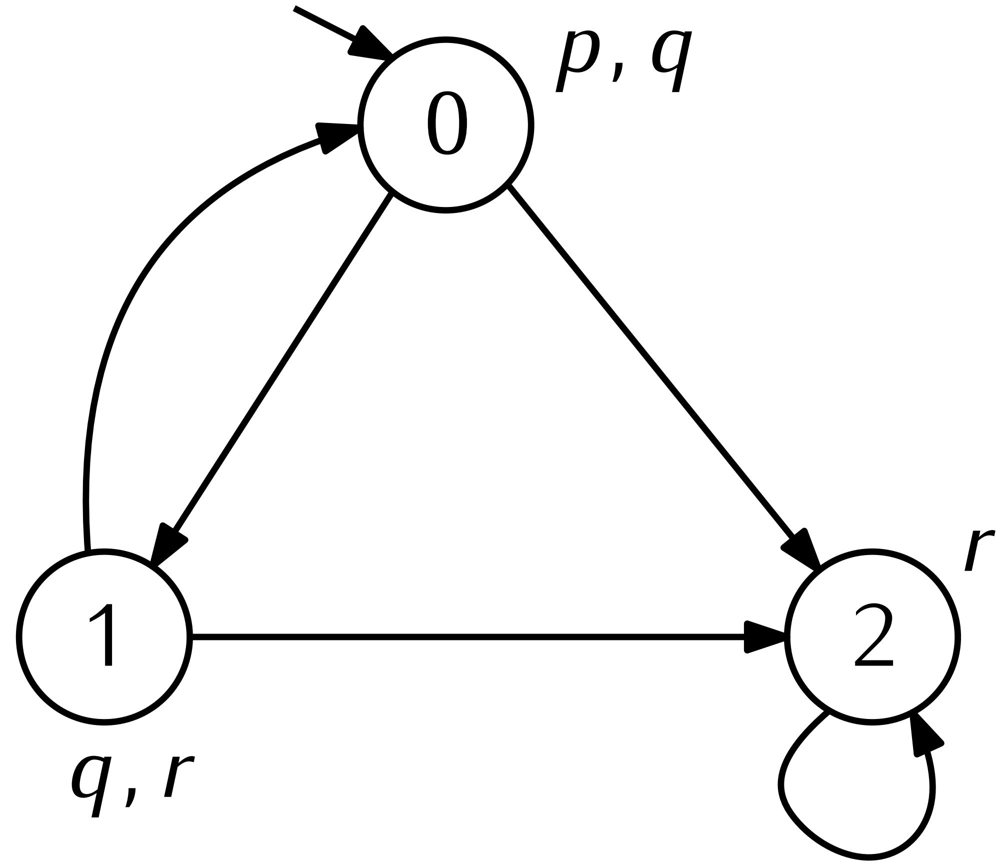


Transition System Example

Do these properties hold?

$\mathcal{M} \models p \land q$

$\mathcal{M} \models \neg r$



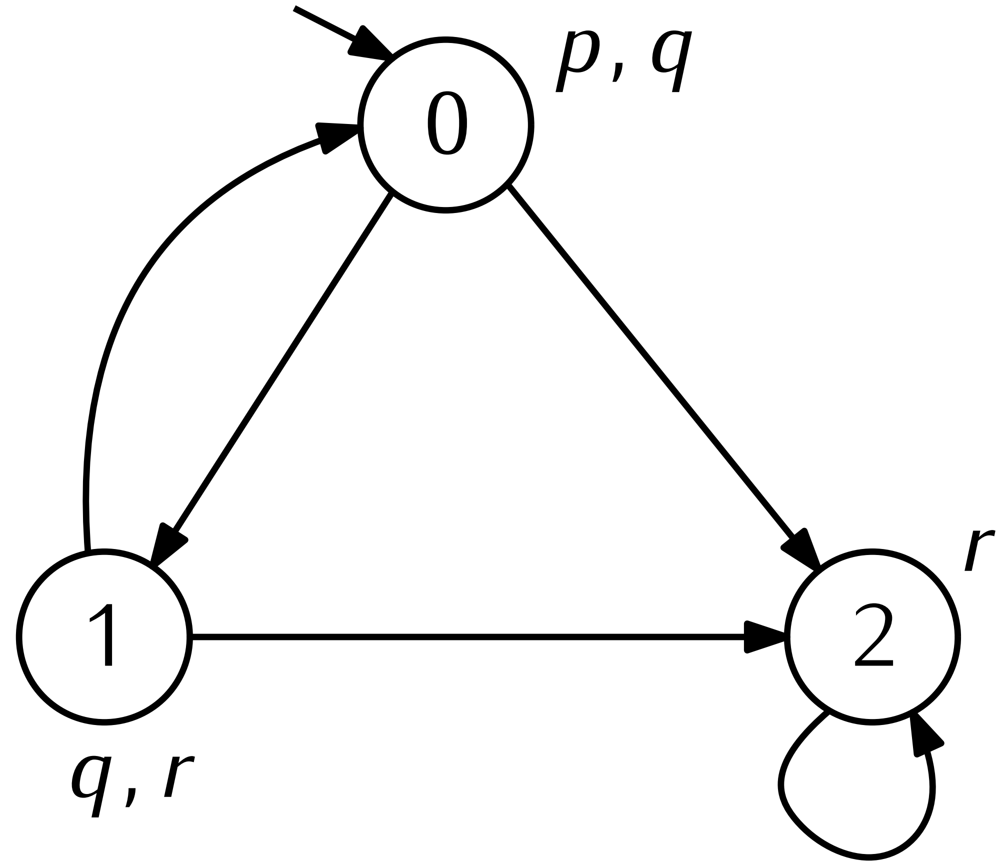
Transition System Example

Do these properties hold?

$\mathcal{M} \models p \land q$

$\mathcal{M} \models \neg r$

$\mathcal{M} \models X r$



Transition System Example

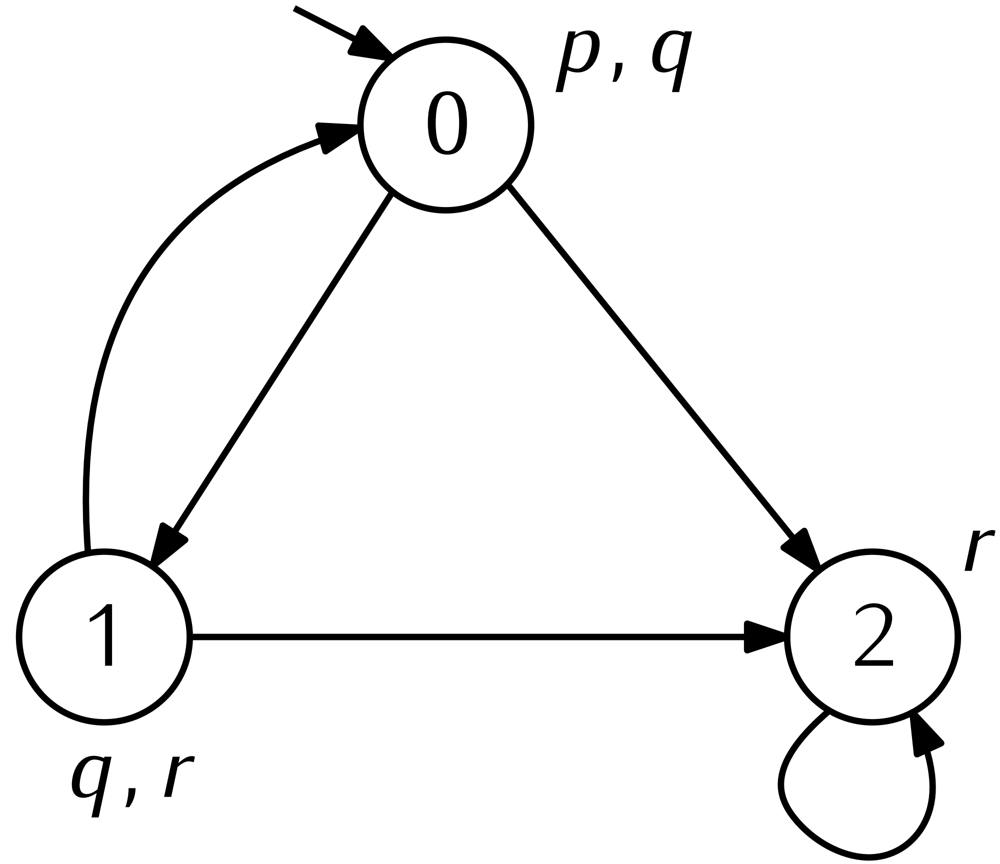
Do these properties hold?

$\mathcal{M} \models p \wedge q$

$\mathcal{M} \models \neg r$

$\mathcal{M} \models X r$

$\mathcal{M} \models X(q \wedge r)$



Transition System Example

Do these properties hold?

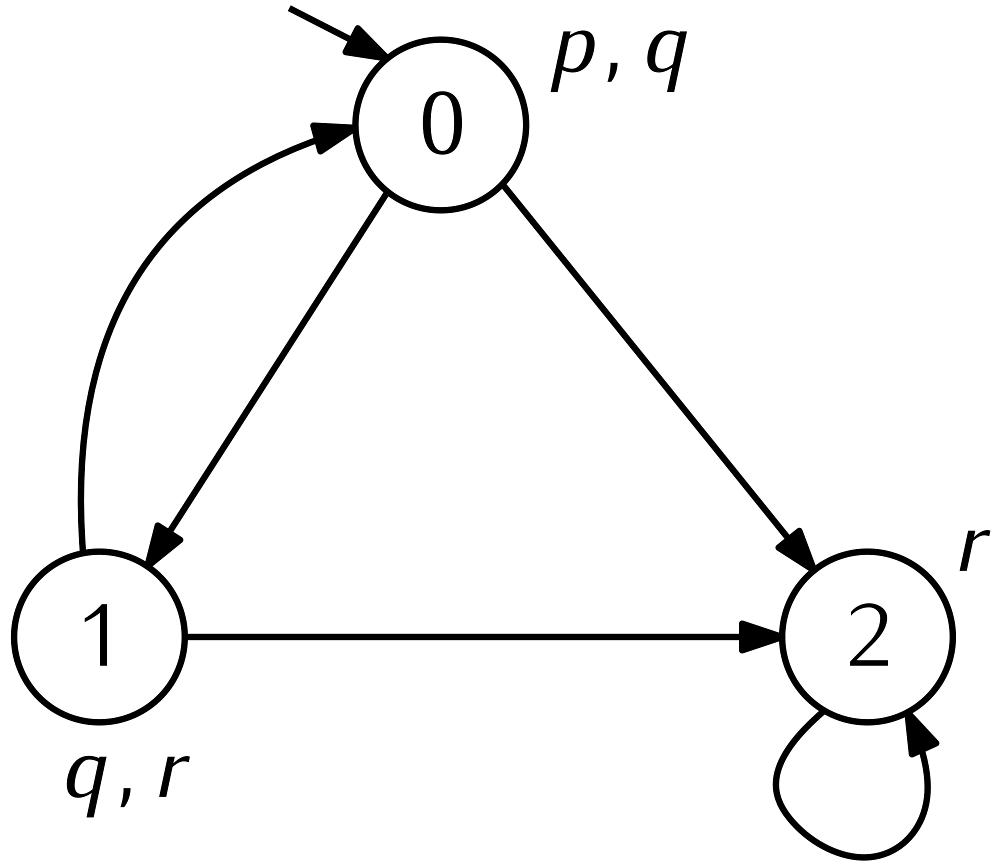
$\mathcal{M} \models p \wedge q$

$\mathcal{M} \models \neg r$

$\mathcal{M} \models X r$

$\mathcal{M} \models X(q \wedge r)$

$\mathcal{M} \models G\neg(p \wedge r)$



Transition System Example

Do these properties hold?

$\mathcal{M} \models p \wedge q$

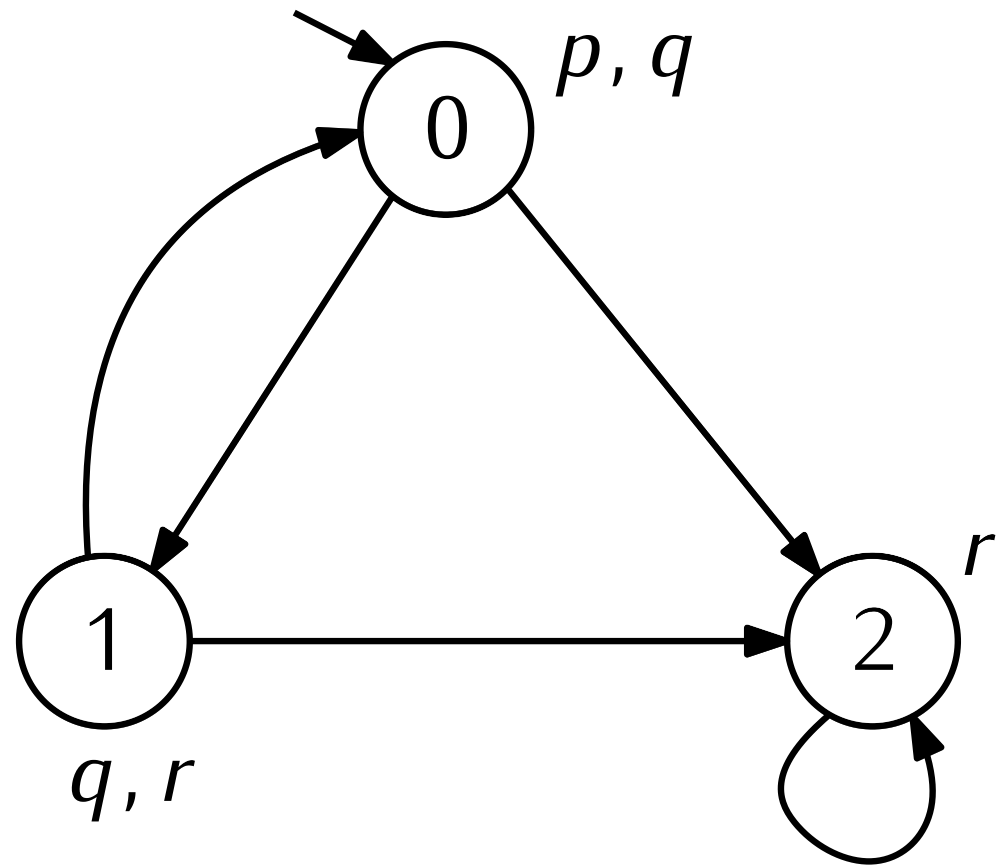
$\mathcal{M} \models \neg r$

$\mathcal{M} \models Xr$

$\mathcal{M} \models X(q \wedge r)$

$\mathcal{M} \models G\neg(p \wedge r)$

$\mathcal{M} \models GFp$



Transition System Example

Do these properties hold?

$\mathcal{M} \models p \wedge q$

$\mathcal{M} \models \neg r$

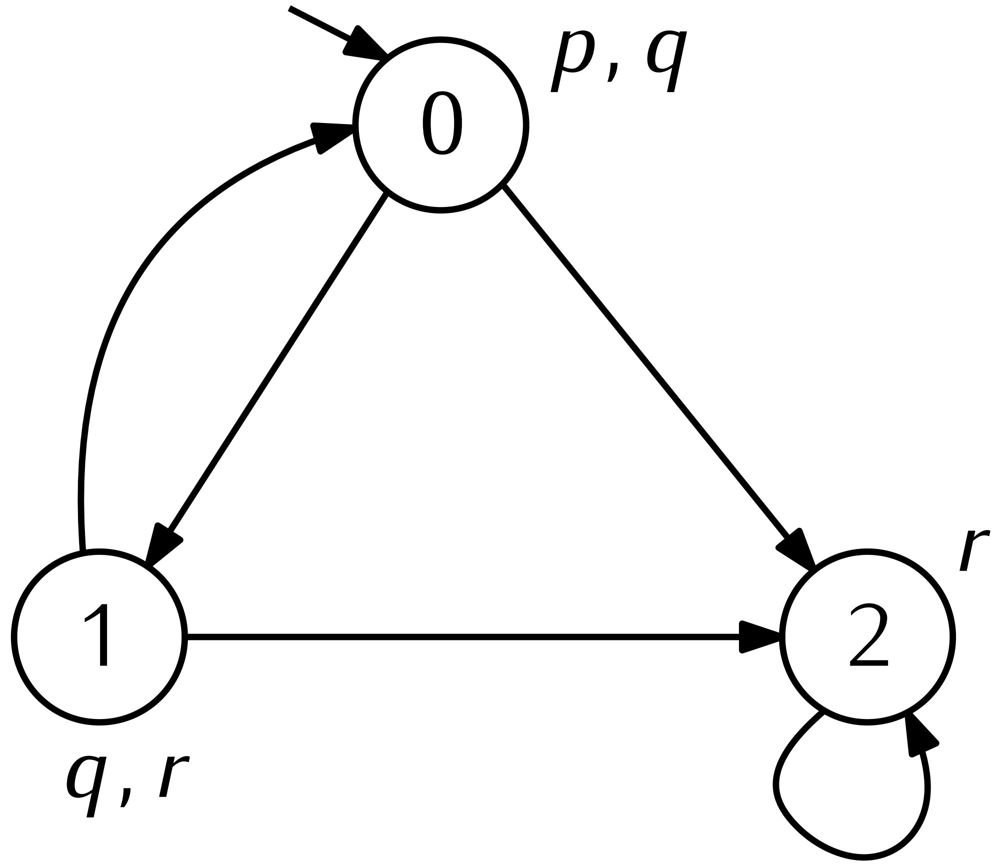
$\mathcal{M} \models Xr$

$\mathcal{M} \models X(q \wedge r)$

$\mathcal{M} \models G\neg(p \wedge r)$

$\mathcal{M} \models GFp$

$\mathcal{M} \models F(\neg q \wedge r) \Rightarrow FGr$



Transition System Example

Do these properties hold?

$$\mathcal{M} \models p \wedge q$$

$$\mathcal{M} \models \neg r$$

$$\mathcal{M} \models Xr$$

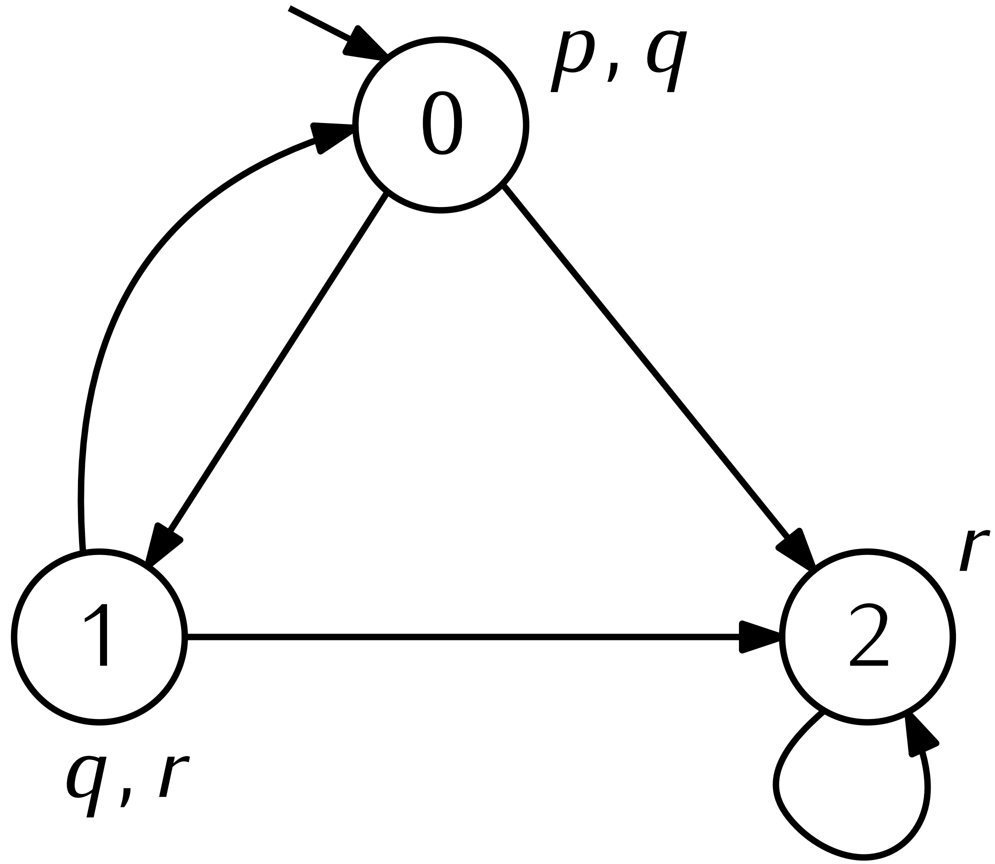
$$\mathcal{M} \models X(q \wedge r)$$

$$\mathcal{M} \models G\neg(p \wedge r)$$

$$\mathcal{M} \models GFp$$

$$\mathcal{M} \models F(\neg q \wedge r) \Rightarrow FGr$$

$$\mathcal{M} \models GFp \Rightarrow GFr$$



Transition System Example

Do these properties hold?

$\mathcal{M} \models p \wedge q$

$\mathcal{M} \models \neg r$

$\mathcal{M} \models Xr$

$\mathcal{M} \models X(q \wedge r)$

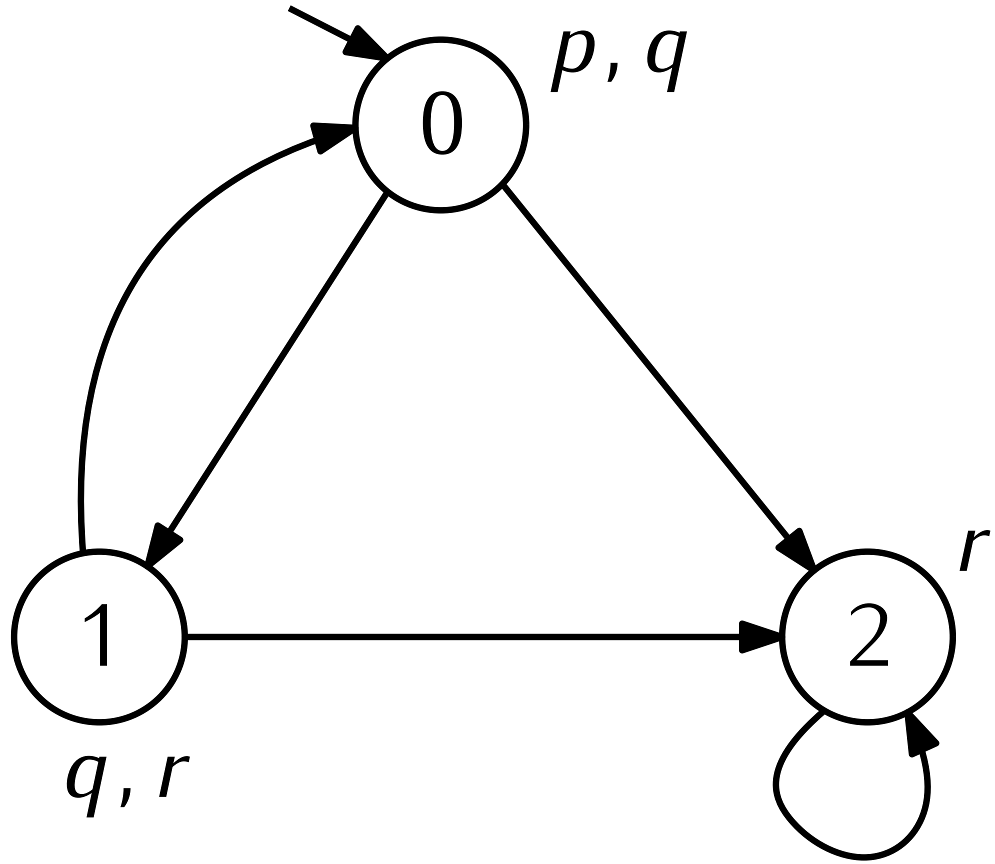
$\mathcal{M} \models G\neg(p \wedge r)$

$\mathcal{M} \models GFp$

$\mathcal{M} \models F(\neg q \wedge r) \Rightarrow FGr$

$\mathcal{M} \models GFp \Rightarrow GFr$

$\mathcal{M} \models GFr \Rightarrow GFp$



Linear Temporal Logic (LTL)

We will assign symbols for expressing temporal system requirements like *always* (G), *eventually* (F), *next* (X), *until* (U), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems

We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts

Safety, liveness, mutual exclusion, ...

Verification Software

Symbolic Model Verifier (NuSMV)

Linear Temporal Logic (LTL)

We will assign symbols for expressing temporal system requirements like *always* (G), *eventually* (F), *next* (X), *until* (U), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems

We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts

Safety, liveness, mutual exclusion, ...

Verification Software

Symbolic Model Verifier (NuSMV)

Next time