

# CS256/Winter 2009 Lecture #3

Zohar Manna

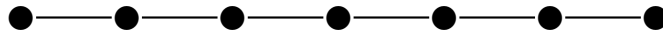
## TEMPORAL LOGIC(S)

Languages that can specify the behavior of a reactive program.

Two views:

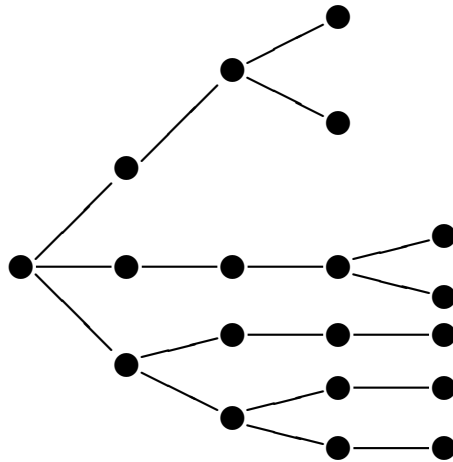
(1) the program generates a set of sequences of states

- the models of temporal logic are infinite sequences of states
- LTL (linear time temporal logic)  
[Manna, Pnueli] approach



(2) the program generates a tree, where the branching points represent nondeterminism in the program

- the models of temporal logic are infinite trees
- CTL (computation tree logic)  
[Clarke, Emerson] at CMU  
Also CTL\*.



## Temporal logic: underlying assertion language

Assertion language  $\mathcal{L}$ :

first-order language over

interpreted typed symbols

(functions and relations over

concrete domains)

$$\text{Example: } x > 0 \rightarrow x + 1 > y \\ x, y \in \mathbf{Z}^+$$

formulas in  $\mathcal{L}$  called:

state formulas or assertions

## Temporal logic: underlying assertion language (Con't)

A state formula is evaluated over a single state to yield a truth value.

For state  $s$  and state formula  $p$

$$s \models p \quad \text{if} \quad s[p] = \text{T}$$

We say:

$p$  holds at  $s$   
 $s$  satisfies  $p$   
 $s$  is a  $p$ -state

**Example:**

For state  $s : \{x : 4, y : 1\}$

$$s \models x = 0 \vee y = 1$$

$$s \not\models x = 0 \wedge y = 1$$

$$s \models \exists z. x = z^2$$

## Temporal logic: underlying assertion language (Con't)

$p$  is state-satisfiable if

$$s \models p \quad \text{for some state } s$$

$p$  is state-valid if

$$s \models p \quad \text{for all states } s$$

$p$  and  $q$  are state-equivalent if

$$s \models p \quad \text{iff} \quad s \models q \quad \text{for all states } s$$

**Example:**  $(x, y : \text{integer})$

state-valid:  $x \geq y \leftrightarrow x+1 > y$

state-equivalent:  $x = 0 \rightarrow y = 1$

and

$$x \neq 0 \vee y = 1$$

## TEMPORAL LOGIC (TL)

A formalism for specifying sequences of states

TL = assertions + temporal operators

- assertions (state formulas):

First-order formulas

describing the properties of a single state

- temporal operators

Fig 0.15

## Future Temporal Operators

- $\square p$  – Henceforth  $p$
- $\diamond p$  – Eventually  $p$
- $p\mathcal{U}q$  –  $p$  Until  $q$
- $p\mathcal{W}q$  –  $p$  Waiting-for (Unless)  $q$
- $\bigcirc p$  – Next  $p$

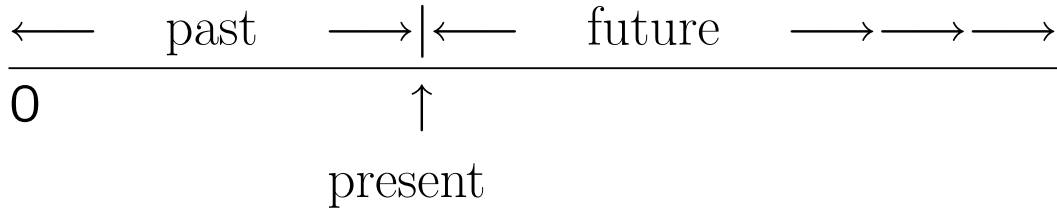
## Past Temporal Operators

- $\Box p$  – So-far  $p$
- $\Diamond p$  – Once  $p$
- $p\mathcal{S}q$  –  $p$  Since  $q$
- $p\mathcal{B}q$  –  $p$  Back-to  $q$
- $\ominus p$  – Previously  $p$
- $\oslash p$  – Before  $p$

Fig. 0.15. The temporal operators



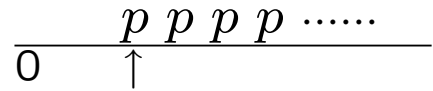
future temporal operators



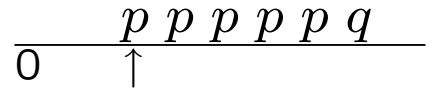
$\diamond q$  — Eventually  $q$



$\square p$  — Henceforth  $p$

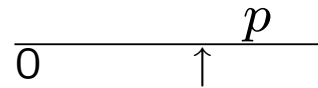


$p\mathcal{U}q$  —  $p$  Until  $q$



$p\mathcal{W}q$  —  $p$  Wait-for (Unless)  $q$       $\square p \vee p\mathcal{U}q$

$\bigcirc p$  — Next  $p$



past temporal operators

$\diamondleftarrow q$	— Once $q$	$\frac{q}{0 \quad \uparrow}$
$\squareleftarrow p$	— So-far $p$	$\frac{p \ p \ p \ p \ p \ p}{0 \quad \uparrow}$
$p \mathcal{S} q$	— $p$ Since $q$	$\frac{q \ p \ p \ p \ p \ p}{0 \quad \uparrow}$
$p \mathcal{B} q$	— $p$ Back-to $q$	$\squareleftarrow p \vee p \mathcal{S} q$
$\ominus p$	— Previously $p$ (false at position 0)	$\frac{p}{0 \quad \uparrow}$
$\odot p$	— Before $p$ (true at position 0)	

## Temporal Logic: Syntax

- Every assertion is a temporal formula
- If  $p$  and  $q$  are temporal formulas (and  $u$  is a variable), so are:

$$\neg p \quad p \vee q \quad p \wedge q \quad p \rightarrow q \quad p \leftrightarrow q$$

$$\exists u.p \quad \forall u.p$$

$$\Box p \quad \Diamond p \quad p\mathcal{U}q \quad p\mathcal{W}q \quad \bigcirc p$$

$$\Boxminus p \quad \Diamondminus p \quad p\mathcal{S}q \quad p\mathcal{B}q \quad \ominus p \quad \odot p$$

Example:

$$\Box(x > 0 \rightarrow \Diamondminus y = x)$$

$$p\mathcal{U}q \rightarrow \Diamond q$$

## Temporal Logic: Semantics

Temporal formulas are evaluated over a model  
(an infinite sequence of states)

$$\sigma : s_0, s_1, s_2, \dots$$

- The semantics of temporal logic formula  $p$  at a position  $j \geq 0$  in a model  $\sigma$ ,

$$(\sigma, j) \models p$$

“formula  $p$  holds at position  $j$  of model  $\sigma$ ”,  
is defined by induction on  $p$ :

$$\sigma : s_0, s_1, \dots, s_j, \dots$$

$\uparrow$   
 $(\sigma, j)$

## Temporal Logic: Semantics (Con't)

For state formula (assertion)  $p$   
(i.e., no temporal operators)

- $(\sigma, j) \models p \iff s_j \models p$

---

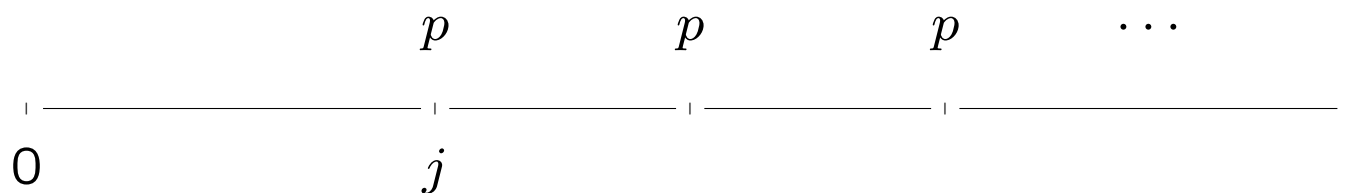
For a temporal formula  $p$ :

- $(\sigma, j) \models \neg p \iff (\sigma, j) \not\models p$

- $(\sigma, j) \models p \vee q \iff (\sigma, j) \models p \text{ or } (\sigma, j) \models q$

## Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models \Box p \iff$   
for all  $k \geq j$ ,  $(\sigma, k) \models p$

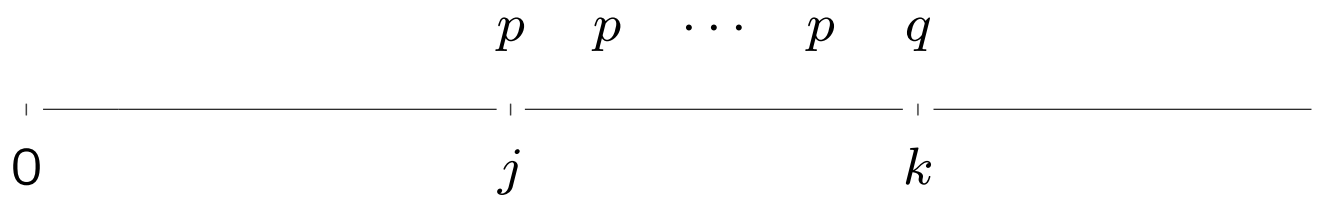


- $(\sigma, j) \models \Diamond p \iff$   
for some  $k \geq j$ ,  $(\sigma, k) \models p$



## Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models p\mathcal{U}q \iff$   
 for some  $k \geq j$ ,  $(\sigma, k) \models q$ ,  
 and for all  $i$ ,  $j \leq i < k$ ,  $(\sigma, i) \models p$



- $(\sigma, j) \models p\mathcal{W}q \iff$   
 $(\sigma, j) \models p\mathcal{U}q$  or  $(\sigma, j) \models \Box p$

- $(\sigma, j) \models \bigcirc p \iff$   
 $(\sigma, j+1) \models p$







## Temporal Logic: Semantics (Con't)

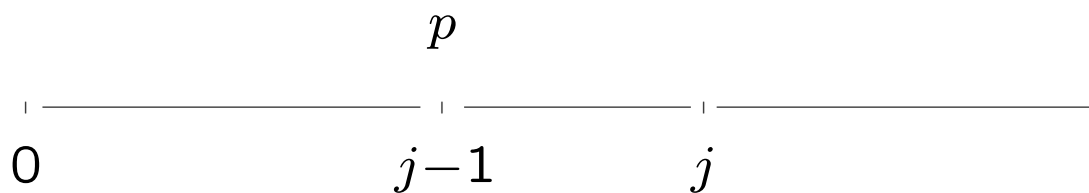
- $(\sigma, j) \models p \mathcal{S} q \iff$   
for some  $k, 0 \leq k \leq j$ ,  $(\sigma, k) \models q$   
and for all  $i, k < i \leq j$ ,  $(\sigma, i) \models p$



- $(\sigma, j) \models p \mathcal{B} q \iff$   
 $(\sigma, j) \models p \mathcal{S} q$  or  $(\sigma, j) \models \Box p$

## Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models \ominus p \iff$   
 $j \geq 1$  and  $(\sigma, j-1) \models p$



- $(\sigma, j) \models \odot p \iff$   
either  $j = 0$  or else  $(\sigma, j-1) \models p$

## Simple Examples

Given temporal formula  $\varphi$ , describe model  $\sigma$ ,  
such that

$$(\sigma, 0) \models \varphi$$

$$p \rightarrow \diamond q$$

if initially  $p$  then eventually  $q$

$$\frac{p \quad q}{0}$$

$$\square(p \rightarrow \diamond q)$$

every  $p$  is eventually followed by a  $q$

$$\frac{p \quad q \quad p \quad q}{0}$$

$$\square \diamond q$$

every position is eventually followed by a  $q$ ,

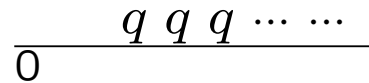
i.e.,

infinitely many  $q$ 's

$$\frac{q \quad q}{0}$$

## Simple Examples (Con't)

$\diamond \square q$

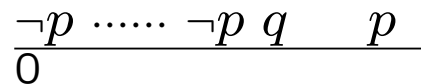


eventually permanently  $q$ ,  
i.e.,  
finitely many  $\neg q$ 's

$\square \diamond p \rightarrow \square \diamond q$

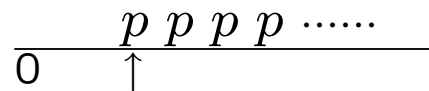
if there are infinitely many  $p$ 's  
then there are infinitely many  $q$ 's

$(\neg p) \mathcal{W} q$



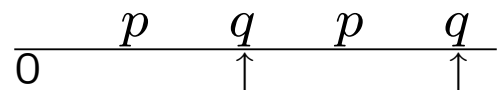
$q$  precedes  $p$  (if  $p$  occurs)

$\square(p \rightarrow \bigcirc p)$



once  $p$ , always  $p$

$\square(q \rightarrow \diamond p)$



every  $q$  is preceded by a  $p$

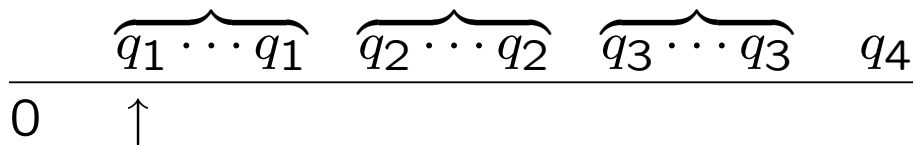
## Nested Waiting-for Formulas

$$\boxed{q_1 \mathcal{W} q_2 \mathcal{W} q_3 \mathcal{W} q_4}$$

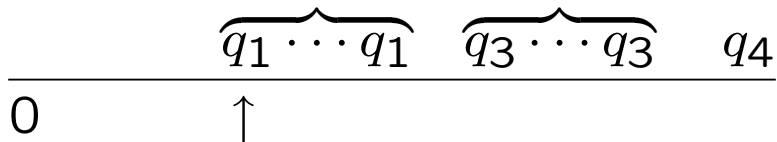
stands for

$$q_1 \mathcal{W} (q_2 \mathcal{W} (q_3 \mathcal{W} q_4))$$

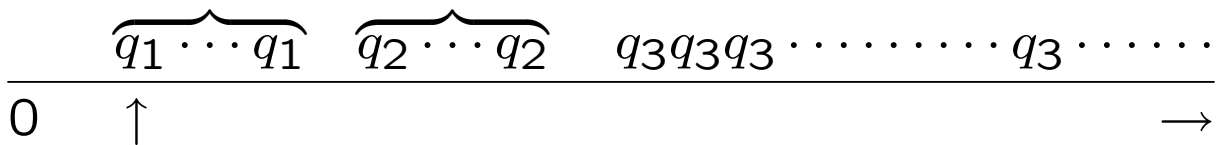
intervals of continuous  $q_i$



- possibly empty interval



- possibly infinite interval



Abbreviation:

$p \Rightarrow q$  for  $\Box(p \rightarrow q)$  “ $p$  entails  $q$ ”

**Example:**

$p \Rightarrow \Diamond q$

stands for

$\Box(p \rightarrow \Diamond q)$

## Past/Future Formulas

Past Formula –

formula with no future operators

Future Formula –

formula with no past operators

A state formula is both a past and a future formula.

## Definitions

- For temporal formula  $p$ , sequence  $\sigma$  and position  $j \geq 0$ :

$(\sigma, j) \models p$ :  $p$  holds at position  $j$  of  $\sigma$   
 $\sigma$  satisfies  $p$  at  $j$   
 $j$  is a  $p$ -position in  $\sigma$ .

- For temporal formula  $p$  and sequence  $\sigma$ ,

$$\sigma \models p \quad \text{iff} \quad (\sigma, 0) \models p$$

$\sigma \models p$ :  $p$  holds on  $\sigma$   
 $\sigma$  satisfies  $p$

## Satisfiable/Valid

For temporal formula  $p$ ,

- $p$  is satisfiable if  $\sigma \models p$  for some sequence (model)  $\sigma$
- $p$  is valid if  $\sigma \models p$  for all sequences (models)  $\sigma$

$p$  is valid iff  $\neg p$  is unsatisfiable

**Example:**  $(x : \text{integer})$

$\diamond(x = 0)$  is satisfiable

$\diamond(x = 0) \vee \square(x \neq 0)$  is valid

$\diamond(x = 0) \wedge \square(x \neq 0)$  is unsatisfiable

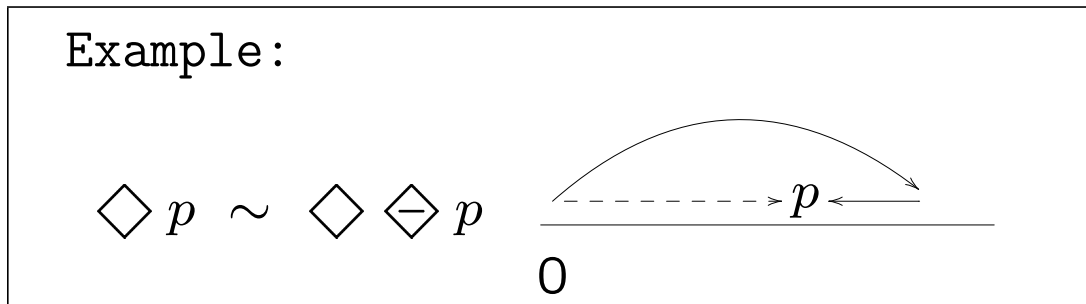


## Equivalence

For temporal formulas  $p$  and  $q$ :

$p$  is equivalent to  $q$ , written  $p \sim q$   
 if  $p \leftrightarrow q$  is valid

(i.e.,  $p$  and  $q$  have the same truth-value at the first  
 position of every model)



$\varphi \sim \psi$ : for any  $\sigma$ ,  
 $(\sigma, 0) \models \varphi$  iff  $(\sigma, 0) \models \psi$ .

$\varphi$  valid: for any  $\sigma$ ,  $(\sigma, 0) \models \varphi$ .

Therefore,

$$\varphi, \psi \text{ valid} \Rightarrow \varphi \sim \psi.$$

$\varphi$  unsatisfiable: for any  $\sigma$ ,  $(\sigma, 0) \not\models \varphi$ .

For the same reason,

$$\varphi, \psi \text{ unsatisfiable} \Rightarrow \varphi \sim \psi.$$

## *first*

Characterizes the first position.

*first*:  $\neg \ominus T$

$(\sigma, j) \models \textit{first}$ : true for  $j = 0$   
false for  $j > 0$

Then

- $T \sim \Box T \sim \textit{first}$
- $T, \Box T, \textit{first}$  are valid

Assume  $V = \{\text{integer } x\}$

*first* :  $\neg \ominus (x = 0 \vee x \neq 0)$

$T$  :  $(x = 0 \vee x \neq 0)$

$\Box T$  :  $\Box (x = 0 \vee x \neq 0)$

For arbitrary  $\sigma$ :

$(\sigma, 0) \models \textit{first}$      $(\sigma, 0) \models T$      $(\sigma, 0) \models \Box T$   
 $(\sigma, j) \not\models \textit{first}$      $(\sigma, j) \models T$      $(\sigma, j) \models \Box T$     for  $j > 0$

## Congruence

For temporal formulas  $p$  and  $q$ :

$p$  is congruent to  $q$ , written  $p \approx q$

if  $\Box(p \leftrightarrow q)$  is valid

$\varphi \approx \psi$ : for any  $\sigma, j$ ,  $(\sigma, j) \models \varphi$  iff  $(\sigma, j) \models \psi$

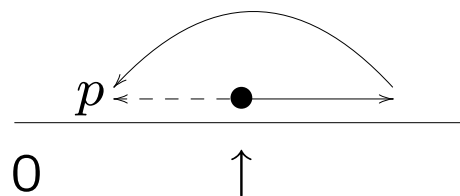
**Example:**

$$\top \approx \Box \top$$

$$\top \not\approx \textit{first}$$

$\top$  may be true in the second state, but *first* is not

$$\Diamond p \not\approx \Diamond \Box p \quad \text{because } \Rightarrow, \text{ but } \not\Leftarrow$$



$$\Box p \approx \neg \Diamond \neg p$$

$$\neg \bigcirc p \approx \bigcirc \neg p$$

### Note

$A \approx B$  iff  $A \Rightarrow B$  and  $B \Rightarrow A$  are valid

$A \sim B$  iff  $A \rightarrow B$  and  $B \rightarrow A$  are valid

## Congruences

“conjunction character” — match well with  $\wedge$

“disjunction character” — match well with  $\vee$

$\square$  and  $\boxminus$  have conjunction character

$\diamond$  and  $\diamondleftarrow$  have disjunction character

$\mathcal{U}$ ,  $\mathcal{W}$ ,  $\mathcal{S}$ ,  $\mathcal{B}$  first argument has  
conjunction character  
second argument has  
disjunction character

$$\square(p \wedge q) \approx \square p \wedge \square q$$

$$\diamond(p \vee q) \approx \diamond p \vee \diamond q$$

$$p\mathcal{U}(q \vee r) \approx (p\mathcal{U}q) \vee (p\mathcal{U}r)$$

$$(p \wedge q)\mathcal{U}r \approx (p\mathcal{U}r) \wedge (q\mathcal{U}r)$$

$$p\mathcal{W}(q \vee r) \approx (p\mathcal{W}q) \vee (p\mathcal{W}r)$$

$$(p \wedge q)\mathcal{W}r \approx (p\mathcal{W}r) \wedge (q\mathcal{W}r)$$

## Expansions

$$\Box p \approx (p \wedge \bigcirc \Box p)$$

$$\Diamond p \approx (p \vee \bigcirc \Diamond p)$$

$$p \mathcal{U} q \approx [q \vee (p \wedge \bigcirc (p \mathcal{U} q))]$$

$$\Box p \approx (p \wedge \sim \Box p)$$

$$\Diamond p \approx (p \vee \ominus \Diamond p)$$

$$p \mathcal{S} q \approx [q \vee (p \wedge \ominus (p \mathcal{S} q))]$$

## Strict Operators

(present not included)

$$\begin{array}{ccc}
 [ \longleftarrow \longrightarrow ] & \bullet & [ \longrightarrow ] \\
 s_0 & \uparrow & s_{j+1} \\
 & s_j &
 \end{array}$$

$$\widehat{\square} p \approx \circ \square p \qquad \widehat{\boxminus} p \approx \odot \boxminus p$$

$$\widehat{\diamond} p \approx \circ \diamond p \qquad \widehat{\boxplus} p \approx \ominus \boxplus p$$

$$p \widehat{\mathcal{U}} q \approx \circ (p \mathcal{U} q) \qquad p \widehat{\mathcal{S}} q \approx \ominus (p \mathcal{S} q)$$

$$p \widehat{\mathcal{W}} q \approx \circ (p \mathcal{W} q) \qquad p \widehat{\mathcal{B}} q \approx \odot (p \mathcal{B} q)$$

## Next and Previous Values of Exps

When evaluating  $x$  at position  $j \geq 0$

$x$  refers to  $s_j[x]$

$x^+$  refers to  $s_{j+1}[x]$

$x^-$  refers to  $\begin{cases} s_{j-1}[x] & \text{if } j > 0 \\ s_0[x] & \text{if } j = 0 \end{cases}$

Example:

$\sigma: \langle x: 0 \rangle, \langle x: 1 \rangle, \langle x: 2 \rangle, \dots$

satisfies

$$x = 0 \wedge \square(x^+ = x + 1) \wedge \bigcirc \square(x = x^- + 1)$$

## Temporal Logic: Substitutivity

The ability to substitute equals for equals in a formula and obtain a formula with identical meaning.

- For state formula  $\phi(u)$

$$\text{if } p \sim q \text{ then } \phi(p) \sim \phi(q)$$

**Example:**

Consider state formula  $\phi(u): r \wedge u$

$$\begin{array}{l} \text{Since} \\ \text{then} \end{array} \quad \begin{array}{l} \diamond p \sim \diamond \neg p \\ r \wedge \diamond p \sim r \wedge \diamond \neg p. \end{array}$$



## Temporal Logic: Substitutivity (Con't)

This does not hold if  $\phi(u)$  is a temporal formula.

**Example:**

Consider temporal formula  $\phi(u): \Box u$

$$\begin{array}{l} \Diamond p \sim \Diamond \neg p \\ \text{but } \Box \Diamond p \not\sim \Box \Diamond \neg p \end{array} \quad \begin{array}{c} \text{---} \curvearrowright \text{---} \\ \text{---} \dashrightarrow p \longleftarrow \text{---} \\ \text{0} \end{array}$$

- For temporal formula  $\phi(u)$   
if  $p \approx q$  then  $\phi(p) \approx \phi(q)$

**Example:**

Consider the temporal formula  $\phi(u): q\mathcal{U}u$

$$\begin{array}{l} \text{Since} \quad \Box p \approx \neg \Diamond \neg p \\ \text{therefore} \quad q\mathcal{U}(\Box p) \approx q\mathcal{U}(\neg \Diamond \neg p) \end{array}$$