CS256/Winter 2009 Lecture #3

Zohar Manna

TEMPORAL LOGIC(S)

Languages that can specify the behavior of a reactive program.

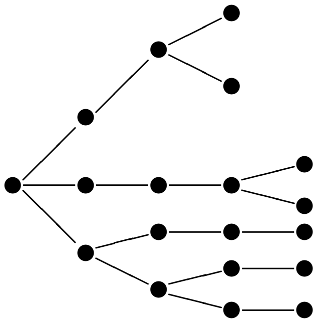
Two views:

(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)

```
Example: x > 0 → x + 1 > y
         x, y ∈ 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

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

We say:

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

`Example:`

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

$$s \Vdash x = 0 \lor y = 1$$
$$s \not\Vdash x = 0 \land y = 1$$
$$s \Vdash \exists z.\ x = z^2$$

Temporal logic: underlying assertion language (Con't)

p is state-satisfiable if

$s \Vdash p$ for some state s

p is state-valid if

$s \Vdash p$ for all states s

p and q are state-equivalent if

$s \Vdash p$ iff $s \Vdash q$ for all states s

`Example:` $(x, y$: integer$)$

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

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

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

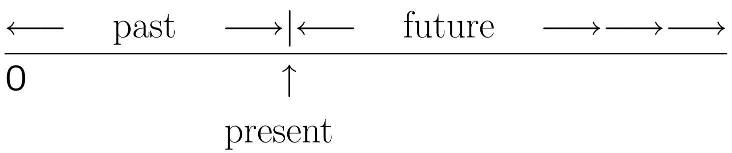
$\Box\, p$	–	Henceforth p
$\Diamond\, p$	–	Eventually p
$p\, \mathcal{U}\, q$	–	p Until q
$p\, \mathcal{W}\, q$	–	p Waiting-for (Unless) q
$\bigcirc\, p$	–	Next p

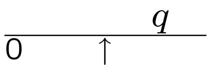
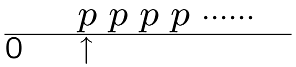
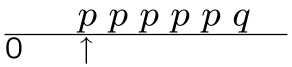
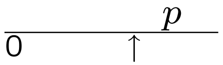
Past Temporal Operators

$\boxminus\, p$	–	So-far p
$\diamondminus\, p$	–	Once p
$p\, \mathcal{S}\, q$	–	p Since q
$p\, \mathcal{B}\, q$	–	p Back-to q
$\ominus\, p$	–	Previously p
$\widetilde{\ominus}\, p$	–	Before p

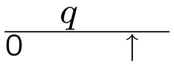
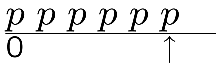
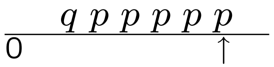
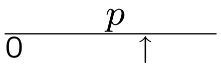
Fig. 0.15. The temporal operators

future temporal operators



$\Diamond q$	—	Eventually q	
$\Box p$	—	Henceforth p	
$p\,\mathcal{U} q$	—	p Until q	
$p\,\mathcal{W}\,q$	—	p Wait-for (Unless) q	$\Box p \ \lor\ p\,\mathcal{U}\,q$
$\bigcirc p$	—	Next p	

past temporal operators

$\diamondminus\, q$	—	Once q	
$\boxminus\, p$	—	So-far p	
$p\,\mathcal{S}\,q$	—	p Since q	
$p\,\mathcal{B}\,q$	—	p Back-to q	$\boxminus\, p \ \lor\ p\,\mathcal{S}\,q$
$\ominus\, p$	—	Previously p (false at position 0)	
$\circledtilde\, p$	—	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:

$$\neg\, p \qquad p \vee q \qquad p \wedge q \qquad p \rightarrow q \qquad p \leftrightarrow q$$

$$\exists u.p \qquad \forall u.p$$

$$\square\, p \qquad \Diamond\, p \qquad p\,\mathcal{U}\,q \qquad p\,\mathcal{W}\,q \qquad \bigcirc\, p$$

$$\boxminus\, p \qquad \diamondminus\, p \qquad p\,\mathcal{S}\,q \qquad p\,\mathcal{B}\,q \qquad \ominus\, p \qquad \circledtilde\, p$$

Example:

$$\square(x > 0 \rightarrow \diamondminus\, y = x)$$

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

Temporal Logic: Semantics

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

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

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

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

"formula p holds at position j of model σ", is defined by induction on p:

$$\begin{array}{cccccc} \sigma : & s_0, & s_1, & \ldots, & s_j, & \ldots \\ & & & & \uparrow & \\ & & & & (\sigma, j) & \end{array}$$

Temporal Logic: Semantics (Con't)

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

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

For a temporal formula p:

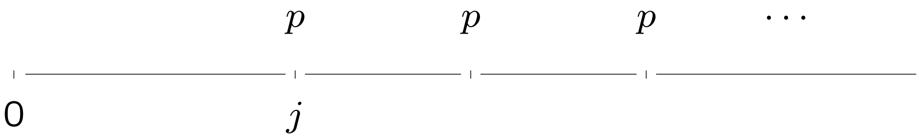
- $(\sigma, j) \models \neg p \iff (\sigma, j) \not\models p$

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

Temporal Logic: Semantics (Con't)

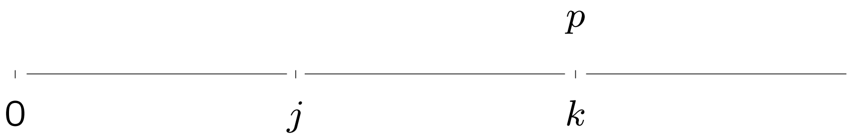
- $(\sigma, j) \models \Box\, p \iff$

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



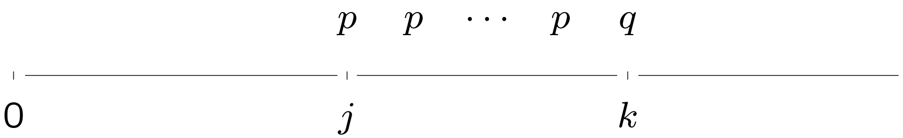
- $(\sigma, j) \models \Diamond\, p \iff$

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



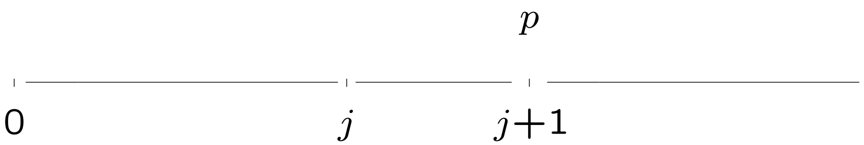
Temporal Logic: Semantics (Con't)

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



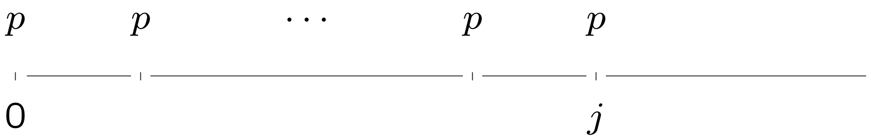
- $(\sigma, j) \models p\,\mathcal{W}\,q \quad \Longleftrightarrow$
  $(\sigma, j) \models p\,\mathcal{U}\,q$ or $(\sigma, j) \models \square\, p$

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

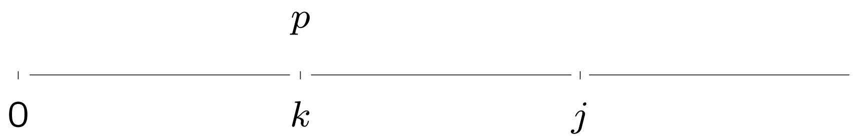


Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models \boxminus\, p \quad \Longleftrightarrow$
  for all k, $0 \leq k \leq j$, $(\sigma, k) \models p$



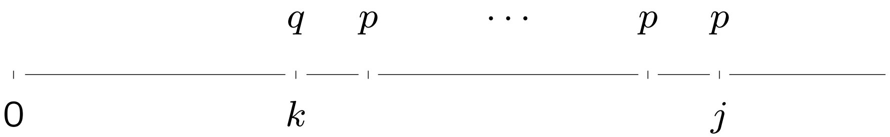
- $(\sigma, j) \models \lozengeminus\, p \quad \Longleftrightarrow$
  for some k, $0 \leq k \leq j$, $(\sigma, k) \models p$



Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models p \, \mathcal{S} \, q \quad \Longleftrightarrow$

  for some k, $0 \leq k \leq j$, $(\sigma, k) \models q$
  and for all i, $k < i \leq j$, $(\sigma, i) \models p$



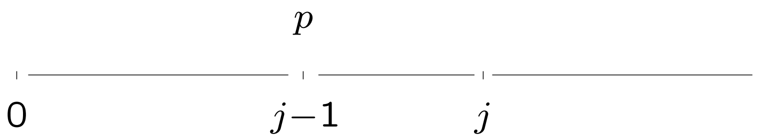
- $(\sigma, j) \models p \, \mathcal{B} \, q \quad \Longleftrightarrow$

  $(\sigma, j) \models p \, \mathcal{S} \, q$ or $(\sigma, j) \models \boxminus \, p$

Temporal Logic: Semantics (Con't)

- $(\sigma, j) \models \ominus \, p \quad \Longleftrightarrow$

  $j \geq 1$ and $(\sigma, j{-}1) \models p$



- $(\sigma, j) \models \bigcirc\!\!\!\!\!\sim \, p \quad \Longleftrightarrow$

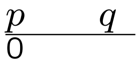
  either $j = 0$ or else $(\sigma, j{-}1) \models p$

Simple Examples

Given temporal formula φ, describe model σ, such that

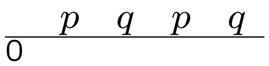
$$(\sigma, 0) \models \varphi$$

$p \to \Diamond q$



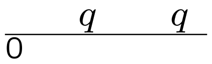
if initially p then eventually q

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



every p is eventually followed by a q

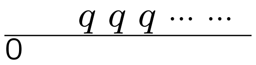
$\Box \Diamond q$



every position is eventually followed by a q,
i.e.,
infinitely many q's

Simple Examples (Con't)

$\Diamond \Box q$

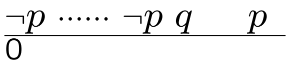


eventually permanently q,
i.e.,
finitely many $\neg q$'s

$\Box \Diamond p \to \Box \Diamond q$

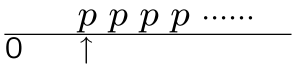
if there are infinitely many p's
then there are infinitely many q's

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



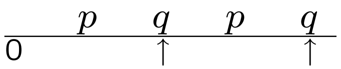
q precedes p (if p occurs)

$\Box(p \to \bigcirc p)$



once p, always p

$\Box(q \to \diamondminus p)$



every q is preceded by a p

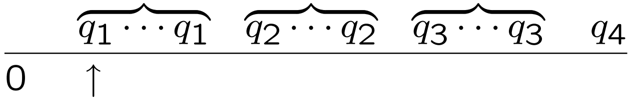
Nested Waiting-for Formulas

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

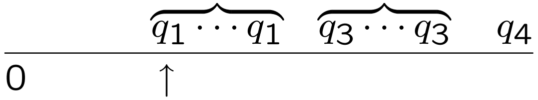
stands for

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

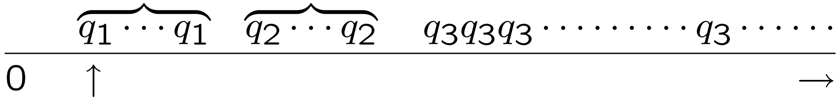
intervals of continuous q_i


$\overbrace{q_1\cdots q_1}$
$\overbrace{q_2\cdots q_2}$
$\overbrace{q_3\cdots q_3}$
q_4
0
↑

- possibly empty interval



- possibly infinite interval


$\overbrace{q_1\cdots q_1}$
$\overbrace{q_2\cdots q_2}$
$q_3q_3q_3\cdots\cdots\cdots q_3\cdots\cdots$
0
↑
→

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 σ and position $j \geq 0$:

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

- For temporal formula p and sequence σ,

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

  $\sigma \vDash p$: p holds on σ
  σ satisfies p

Satisfiable/Valid

For temporal formula p,

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

p is valid iff $\neg p$ is unsatisfiable

`Example:` (x : integer)
$\Diamond(x = 0)$ is satisfiable
$\Diamond(x = 0) \lor \Box(x \neq 0)$ is valid
$\Diamond(x = 0) \land \Box(x \neq 0)$ is unsatisfiable

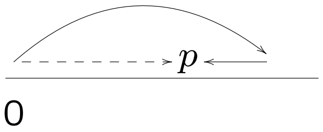
Equivalence

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)

Example:

$\Diamond p \sim \Diamond \Diamond\!\!\!\!\ominus p$



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

φ valid: for any σ, $(\sigma, 0) \vDash \varphi$.

Therefore,

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

φ unsatisfiable: for any σ, $(\sigma, 0) \nvDash \varphi$.

For the same reason,

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

first

Characterizes the first position.

first: $\neg \ominus \mathrm{T}$

$(\sigma, j) \vDash$ *first*: true for $j = 0$
false for $j > 0$

Then

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

Assume V={integer x}
$first : \neg \ominus (x = 0 \lor x \neq 0)$
$\mathrm{T} : (x = 0 \lor x \neq 0)$
$\Box\mathrm{T} : \Box(x = 0 \lor x \neq 0)$

For arbitrary σ:

$(\sigma, 0) \vDash first$	$(\sigma, 0) \vDash \mathrm{T}$	$(\sigma, 0) \vDash \Box\mathrm{T}$	
$(\sigma, j) \nvDash first$	$(\sigma, j) \vDash \mathrm{T}$	$(\sigma, j) \vDash \Box\mathrm{T}$	for $j > 0$

Congruence

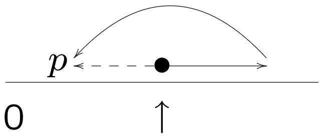
For temporal formulas p and q:
p is congruent to q, written $p \approx q$
if $\Box(p \leftrightarrow q)$ is valid
$\varphi \approx \psi$: for any σ, j, $(\sigma, j) \vDash \varphi$ iff $(\sigma, j) \vDash \psi$

`Example:`

$\mathrm{T} \approx \Box\,\mathrm{T}$

$\mathrm{T} \not\approx \mathit{first}$ T may be true in the second state, but first is not

$\Diamond p \not\approx \Diamond \diamondminus p$ because $\Rightarrow$, 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 $\vee$

$\Box$ and $\boxminus$ have conjunction character

$\Diamond$ and $\diamondminus$ have disjunction character

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

$$
\begin{aligned}
\Box(p \wedge q) &\approx \Box p \wedge \Box q \\
\Diamond(p \vee q) &\approx \Diamond p \vee \Diamond q \\
p\,\mathcal{U}\,(q \vee r) &\approx (p\,\mathcal{U}\,q) \vee (p\,\mathcal{U}\,r) \\
(p \wedge q)\,\mathcal{U}\,r &\approx (p\,\mathcal{U}\,r) \wedge (q\,\mathcal{U}\,r) \\
p\,\mathcal{W}\,(q \vee r) &\approx (p\,\mathcal{W}\,q) \vee (p\,\mathcal{W}\,r) \\
(p \wedge q)\,\mathcal{W}\,r &\approx (p\,\mathcal{W}\,r) \wedge (q\,\mathcal{W}\,r)
\end{aligned}
$$

Expansions

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

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

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

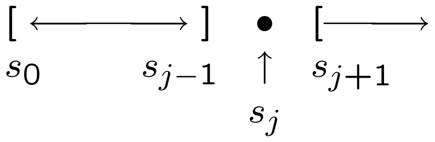
$$\boxminus\, p \;\approx\; (p \,\wedge\, \bigcirc\mkern-15mu\sim\; \boxminus\, p)$$

$$\Diamond\mkern-13mu-\; p \;\approx\; (p \,\vee\, \ominus\, \Diamond\mkern-13mu-\; p)$$

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

Strict Operators

(present not included)



$\widehat{\Box}p$	$\approx$	$\bigcirc \Box\, p$	$\widehat{\boxminus}p$	$\approx$	$\bigcirc\mkern-15mu\sim\; \boxminus\, p$
$\widehat{\Diamond}p$	$\approx$	$\bigcirc \Diamond\, p$	$\widehat{\Diamond\mkern-13mu-}\,p$	$\approx$	$\ominus \Diamond\mkern-13mu-\; p$
$p\,\widehat{\mathcal{U}}\,q$	$\approx$	$\bigcirc(p\,\mathcal{U}\,q)$	$p\,\widehat{\mathcal{S}}\,q$	$\approx$	$\ominus(p\,\mathcal{S}\,q)$
$p\,\widehat{\mathcal{W}}\,q$	$\approx$	$\bigcirc(p\,\mathcal{W}\,q)$	$p\,\widehat{\mathcal{B}}\,q$	$\approx$	$\bigcirc\mkern-15mu\sim\;(p\,\mathcal{B}\,q)$

Next and Previous Values of Exps

When evaluating x at position $j \geq 0$

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

`Example:`

σ: $\langle x{:}\,0\rangle,\ \langle x{:}\,1\rangle,\ \langle x{:}\,2\rangle,\ \ldots$

satisfies

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

Temporal Logic: Substitutivity

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

- For state formula $\phi(u)$

  if $p \sim q$ then $\phi(p) \sim \phi(q)$

`Example:`

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

Since $\Diamond p \ \sim\ \Diamond \diamondminus p$

then $r \wedge \Diamond p \ \sim\ r \wedge \Diamond \diamondminus p.$

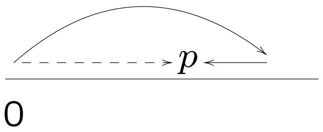
Temporal Logic: Substitutivity (Con't)

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

`Example:`

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

$$\begin{array}{ll} & \Diamond\, p \ \sim\ \Diamond \diamondminus\, p \\ \text{but} & \Box \Diamond\, p \not\sim\ \Box \Diamond \diamondminus\, p \end{array}$$



- For <u>temporal formula</u> $\phi(u)$

  if $p \approx q$ then $\phi(p) \approx \phi(q)$

`Example:`

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

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