Communication and Concurrency
Lecture 6

Colin Stirling (cps)

School of Informatics

7th October 2013

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

- a formula of Hennessy-Milner logic,

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $\mathtt{AG}\ \Phi$, read as "always Φ" or "globally Φ,"

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $\mathtt{AG}\ \Phi$, read as “always Φ” or “globally Φ,”
- a formula $\mathtt{EF}\ \Phi$, read as “possibly Φ,”

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $\mathtt{AG}\ \Phi$, read as "always Φ" or "globally Φ,"
- a formula $\mathtt{EF}\ \Phi$, read as "possibly Φ,"
- a formula $\mathtt{AF}\ \Phi$, read as "eventually Φ,"

Temporal logic CTL$^-$: syntax

$$\begin{array}{rcl} \Phi & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\ & & \mathtt{AG}\ \Phi \mid \mathtt{EF}\ \Phi \mid \mathtt{AF}\ \Phi \mid \mathtt{EG}\ \Phi \end{array}$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $\mathtt{AG}\ \Phi$, read as "always Φ" or "globally Φ,"
- a formula $\mathtt{EF}\ \Phi$, read as "possibly Φ,"
- a formula $\mathtt{AF}\ \Phi$, read as "eventually Φ,"
- a formula $\mathtt{EG}\ \Phi$, read as "EG Φ."

Temporal logic CTL$^-$: semantics

A run (of a process E_0) is a sequence of transitions of the form

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} E_2 \xrightarrow{a_3} \cdots$$

which is "maximal" in the sense that if it is finite then the final process is unable to do any action.

Temporal logic CTL$^-$: semantics

A run (of a process E_0) is a sequence of transitions of the form

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} E_2 \xrightarrow{a_3} \cdots$$

which is "maximal" in the sense that if it is finite then the final process is unable to do any action.

$$\begin{array}{lll}
E_0 \models \mathtt{AG}\,\Phi & \text{iff} & \text{for all runs } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & & \text{for all } i \geq 0,\ E_i \models \Phi \\
E_0 \models \mathtt{EF}\,\Phi & \text{iff} & \text{for some run } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & & \text{for some } i \geq 0,\ E_i \models \Phi \\
E_0 \models \mathtt{AF}\,\Phi & \text{iff} & \text{for all runs } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & & \text{for some } i \geq 0,\ E_i \models \Phi \\
E_0 \models \mathtt{EG}\,\Phi & \text{iff} & \text{for some run } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & & \text{for all } i \geq 0,\ E_i \models \Phi
\end{array}$$

Intuitive meaning

- $E_0 \models \mathtt{AG}\,\Phi$ means "all processes reachable from E_0 satisfy Φ."

Intuitive meaning

- $E_0 \models \texttt{AG}\,\Phi$ means "all processes reachable from E_0 satisfy Φ."
- $E_0 \models \texttt{EF}\,\Phi$ means "some process reachable from E_0 satisfies Φ."

Intuitive meaning

- $E_0 \models \texttt{AG}\ \Phi$ means "all processes reachable from E_0 satisfy Φ."
- $E_0 \models \texttt{EF}\ \Phi$ means "some process reachable from E_0 satisfies Φ."
- $E_0 \models \texttt{AF}\ \Phi$ means "eventually a process will be reached which satisfies Φ."

Intuitive meaning

- $E_0 \models \mathtt{AG}\ \Phi$ means "all processes reachable from E_0 satisfy Φ."
- $E_0 \models \mathtt{EF}\ \Phi$ means "some process reachable from E_0 satisfies Φ."
- $E_0 \models \mathtt{AF}\ \Phi$ means "eventually a process will be reached which satisfies Φ."
- $E_0 \models \mathtt{EG}\ \Phi$ means "some run always satisfies Φ."

Examples

- $E_0 \models \mathtt{AG}\ \langle - \rangle \mathtt{tt}$

Examples

- $E_0 \models \mathtt{AG}\ \langle - \rangle \mathtt{tt}$
- All processes reachable from E_0 can do some action.
  E_0 is *deadlock-free*.

Examples

- $E_0 \models \mathtt{AG}\,\langle - \rangle \mathtt{tt}$
- All processes reachable from E_0 can do some action.
  E_0 is *deadlock-free*.
- $E_0 \models \mathtt{AF}\,[-]\mathtt{ff}$

Examples

- $E_0 \models \mathtt{AG}\ \langle - \rangle \mathtt{tt}$
- All processes reachable from E_0 can do some action. E_0 is *deadlock-free*.
- $E_0 \models \mathtt{AF}\ [-]\mathtt{ff}$
- Eventually a process is reached which cannot execute any action. E is guaranteed to terminate.

Examples

- $E_0 \models \mathtt{AG}\ \langle - \rangle \mathtt{tt}$
- All processes reachable from E_0 can do some action. E_0 is *deadlock-free*.
- $E_0 \models \mathtt{AF}\ [-]\mathtt{ff}$
- Eventually a process is reached which cannot execute any action. E is guaranteed to terminate.
- $\mathtt{AG}\ [\mathtt{request}]\mathtt{AF}\ (\langle \mathtt{granted} \rangle \mathtt{tt} \wedge [-\mathtt{granted}]\mathtt{ff})$

Examples

- $E_0 \models \mathtt{AG}\ \langle - \rangle \mathtt{tt}$
- All processes reachable from E_0 can do some action. E_0 is *deadlock-free*.
- $E_0 \models \mathtt{AF}\ [-]\mathtt{ff}$
- Eventually a process is reached which cannot execute any action. E is guaranteed to terminate.
- $\mathtt{AG}\ [\mathtt{request}]\mathtt{AF}\ (\langle \mathtt{granted} \rangle \mathtt{tt} \wedge [-\mathtt{granted}]\mathtt{ff})$
- All requests will eventually be granted

Exercise

$$\mathtt{P} \stackrel{\text{def}}{=} \mathtt{a.P} + \mathtt{b.Q} \qquad \mathtt{Q} \stackrel{\text{def}}{=} \mathtt{c.Q}$$

Does $P \models \Phi$ hold when Φ is

	Y/N
$\mathrm{EF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{AG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{AF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{EG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{AG}\ \mathrm{EF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{AF}\ \mathrm{EG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{EF}\ \mathrm{AG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	
$\mathrm{EG}\ \mathrm{AF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	

Exercise

$$\mathtt{P} \stackrel{\text{def}}{=} \mathtt{a.P} + \mathtt{b.Q} \qquad \mathtt{Q} \stackrel{\text{def}}{=} \mathtt{c.Q}$$

Does $P \models \Phi$ hold when Φ is

	Y/N
$\mathtt{EF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	Y
$\mathtt{AG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	N
$\mathtt{AF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	N
$\mathtt{EG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	N
$\mathtt{AG}\ \mathtt{EF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	Y
$\mathtt{AF}\ \mathtt{EG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	N
$\mathtt{EF}\ \mathtt{AG}\ \langle \mathtt{c} \rangle \mathtt{tt}$	Y
$\mathtt{EG}\ \mathtt{AF}\ \langle \mathtt{c} \rangle \mathtt{tt}$	N

Example: Peterson's solution to mutual exclusion

$$
\begin{aligned}
\mathsf{B1f} &= \overline{\mathrm{b1rf}}.\mathsf{B1f} + \mathsf{b1wf.B1f} + \mathsf{b1wt.B1t} \\
\mathsf{B1t} &= \overline{\mathrm{b1rt}}.\mathsf{B1t} + \mathsf{b1wt.B1t} + \mathsf{b1wf.B1f} \\[1em]
\mathsf{B2f} &= \overline{\mathrm{b2rf}}.\mathsf{B2f} + \mathsf{b2wf.B2f} + \mathsf{b2wt.B2t} \\
\mathsf{B2t} &= \overline{\mathrm{b2rt}}.\mathsf{B2t} + \mathsf{b2wt.B2t} + \mathsf{b2wf.B2f} \\[1em]
\mathsf{K1} &= \overline{\mathrm{kr1}}.\mathsf{K1} + \mathsf{kw1.K1} + \mathsf{kw2.K2} \\
\mathsf{K2} &= \overline{\mathrm{kr2}}.\mathsf{K2} + \mathsf{kw2.K2} + \mathsf{kw1.K1} \\[1em]
\mathsf{P1} &= \overline{\mathrm{b1wt}}.\mathsf{req1}.\overline{\mathrm{kw2}}.\mathsf{P11} \\
\mathsf{P11} &= \mathsf{b2rt.P11} + \mathsf{b2rf.P12} + \mathsf{kr2.P11} + \\
&\quad\ \mathsf{kr1.P12} \\
\mathsf{P12} &= \mathsf{enter1.exit1}.\overline{\mathrm{b1wf}}.\mathsf{P1} \\[1em]
\mathsf{P2} &= \overline{\mathrm{b2wt}}.\mathsf{req2}.\overline{\mathrm{kw1}}.\mathsf{P21} \\
\mathsf{P21} &= \mathsf{b1rf.P22} + \mathsf{b1rt.P21} + \mathsf{kr1.P21} + \\
&\quad\ \mathsf{kr2.P22} \\
\mathsf{P22} &= \mathsf{enter2.exit2}.\overline{\mathrm{b2wf}}.\mathsf{P2} \\[1em]
\mathsf{Peterson} &= (\mathsf{P1} \mid \mathsf{P2} \mid \mathsf{K1} \mid \mathsf{B1f} \mid \mathsf{B2f}) \setminus L
\end{aligned}
$$

Specification: temporal properties

- Mutual exclusion

Specification: temporal properties

- Mutual exclusion
- Absence of deadlock

Specification: temporal properties

- Mutual exclusion
- Absence of deadlock
- Absence of starvation

Specification: temporal properties

- Mutual exclusion $\mathtt{AG}\ ([\mathtt{exit1}]\mathtt{ff} \vee [\mathtt{exit2}]\mathtt{ff})$
- Absence of deadlock
- Absence of starvation

Specification: temporal properties

- Mutual exclusion $\mathtt{AG}\,([\mathtt{exit1}]\mathtt{ff} \vee [\mathtt{exit2}]\mathtt{ff})$
- Absence of deadlock $\mathtt{AG}\,\langle - \rangle \mathtt{tt}$
- Absence of starvation

Specification: temporal properties

- Mutual exclusion $\mathtt{AG}\,([\mathtt{exit1}]\mathtt{ff} \vee [\mathtt{exit2}]\mathtt{ff})$
- Absence of deadlock $\mathtt{AG}\,\langle - \rangle \mathtt{tt}$
- Absence of starvation (for P1) $\mathtt{AG}\,([\mathtt{req1}]\mathtt{AF}\,\langle \mathtt{exit1} \rangle \mathtt{tt})$

Negation

Negation is also redundant in CTL$^-$: For every formula Φ of CTL$^-$ there is a formula Φ^c such that for every process E

$$E \models \Phi^c \quad \text{iff} \quad E \not\models \Phi$$

Negation

Negation is also redundant in CTL$^-$: For every formula Φ of CTL$^-$ there is a formula Φ^c such that for every process E

$$E \models \Phi^c \ \text{ iff } \ E \not\models \Phi$$

Φ^c is inductively defined as for HML, plus:

$$\begin{array}{rcl} (\mathtt{AG}\ \Phi)^c & = & \mathtt{EF}\ \Phi^c \\ (\mathtt{EF}\ \Phi)^c & = & \mathtt{AG}\ \Phi^c \\ (\mathtt{AF}\ \Phi)^c & = & \mathtt{EG}\ \Phi^c \\ (\mathtt{EG}\ \Phi)^c & = & \mathtt{AF}\ \Phi^c \end{array}$$

Proposition For every E_0 and for every Φ of CTL^-:

$$E_0 \models \Phi^c \text{ iff } E_0 \not\models \Phi \,.$$

Proposition For every E_0 and for every Φ of CTL^{-}:

$$E_0 \models \Phi^c \text{ iff } E_0 \not\models \Phi \, .$$

Proof: By induction on the structure of Φ.

Proposition For every E_0 and for every Φ of CTL$^-$:

$$E_0 \models \Phi^c \text{ iff } E_0 \not\models \Phi \,.$$

Proof: By induction on the structure of Φ.

Case $\Phi = \mathtt{AG}\ \Phi_1$.

$$\begin{array}{ll}
 & E_0 \models (\mathtt{AG}\ \Phi_1)^c \\
\text{iff} & E_0 \models \mathtt{EF}\ \Phi_1^c \\
\text{iff} & \text{for some run } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & \text{for some } i \geq 0 \text{ s.t. } E_i \models \Phi_1^c \\
\text{iff} & \text{for some run } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & \text{for some } i \geq 0 \text{ s.t. } E_i \not\models \Phi_1 \\
\text{iff} & \text{not for all run } E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots, \\
 & \text{for all } i \geq 0 \text{ s.t. } E_i \models \Phi_1 \\
\text{iff} & E_0 \not\models \mathtt{AG}\ \Phi_1
\end{array}$$

Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.

Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.

Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.
- A formula is valid all processes satisfy it.

Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.
- A formula is valid all processes satisfy it.
- Two formulas are equivalent if they are satisfied by exactly the same processes.

Which of the following are valid?

	Y/N
$\mathtt{AG}\ \Phi \longrightarrow \mathtt{AF}\ \Phi$	
$\mathtt{AF}\ \Phi \longrightarrow \mathtt{AG}\ \Phi$	
$\mathtt{AG}\ \Phi \longrightarrow \mathtt{EG}\ \Phi$	
$\mathtt{EG}\ \Phi \longrightarrow \mathtt{AG}\ \Phi$	
$\mathtt{AF}\ \Phi \longrightarrow \mathtt{EF}\ \Phi$	
$\mathtt{EF}\ \Phi \longrightarrow \mathtt{AF}\ \Phi$	
$\mathtt{EG}\ \Phi \longrightarrow \mathtt{EF}\ \Phi$	
$\mathtt{EF}\ \Phi \longrightarrow \mathtt{EG}\ \Phi$	
$\mathtt{AF}\ \Phi \longrightarrow \mathtt{EG}\ \Phi$	
$\mathtt{EG}\ \Phi \longrightarrow \mathtt{AF}\ \Phi$	

Which of the following are valid?

	Y/N
$\mathrm{AG}\ \Phi \longrightarrow \mathrm{AF}\ \Phi$	Y
$\mathrm{AF}\ \Phi \longrightarrow \mathrm{AG}\ \Phi$	N
$\mathrm{AG}\ \Phi \longrightarrow \mathrm{EG}\ \Phi$	Y
$\mathrm{EG}\ \Phi \longrightarrow \mathrm{AG}\ \Phi$	N
$\mathrm{AF}\ \Phi \longrightarrow \mathrm{EF}\ \Phi$	Y
$\mathrm{EF}\ \Phi \longrightarrow \mathrm{AF}\ \Phi$	N
$\mathrm{EG}\ \Phi \longrightarrow \mathrm{EF}\ \Phi$	Y
$\mathrm{EF}\ \Phi \longrightarrow \mathrm{EG}\ \Phi$	N
$\mathrm{AF}\ \Phi \longrightarrow \mathrm{EG}\ \Phi$	N
$\mathrm{EG}\ \Phi \longrightarrow \mathrm{AF}\ \Phi$	Y

Exercise

Which of the following are equivalent when Φ, Φ_1 and Φ_2 are arbitrary formulas of CTL$^-$?

		Y/N
$\mathrm{AG}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{AG}\ \Phi_1 \wedge \mathrm{AG}\ \Phi_2$	
$\mathrm{EF}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{EF}\ \Phi_1 \wedge \mathrm{EF}\ \Phi_2$	
$\mathrm{AF}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{AF}\ \Phi_1 \wedge \mathrm{AF}\ \Phi_2$	
$\mathrm{AG}\ \mathrm{AG}\ \Phi$	$\mathrm{AG}\ \Phi$	
$\mathrm{AF}\ \mathrm{AF}\ \Phi$	$\mathrm{AF}\ \Phi$	
$\mathrm{EF}\ \mathrm{EF}\ \Phi$	$\mathrm{EF}\ \Phi$	
$\mathrm{AG}\ \mathrm{EF}\ \mathrm{AG}\ \Phi$	$\mathrm{AG}\ \mathrm{EF}\ \Phi$	
$\mathrm{AG}\ \mathrm{EF}\ \mathrm{AG}\ \mathrm{EF}\ \Phi$	$\mathrm{AG}\ \mathrm{EF}\ \Phi$	

Exercise

Which of the following are equivalent when Φ, Φ_1 and Φ_2 are arbitrary formulas of CTL$^-$?

		Y/N
$\mathrm{AG}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{AG}\ \Phi_1 \wedge \mathrm{AG}\ \Phi_2$	Y
$\mathrm{EF}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{EF}\ \Phi_1 \wedge \mathrm{EF}\ \Phi_2$	N
$\mathrm{AF}\ (\Phi_1 \wedge \Phi_2)$	$\mathrm{AF}\ \Phi_1 \wedge \mathrm{AF}\ \Phi_2$	N
$\mathrm{AG}\ \mathrm{AG}\ \Phi$	$\mathrm{AG}\ \Phi$	Y
$\mathrm{AF}\ \mathrm{AF}\ \Phi$	$\mathrm{AF}\ \Phi$	Y
$\mathrm{EF}\ \mathrm{EF}\ \Phi$	$\mathrm{EF}\ \Phi$	Y
$\mathrm{AG}\ \mathrm{EF}\ \mathrm{AG}\ \Phi$	$\mathrm{AG}\ \mathrm{EF}\ \Phi$	N
$\mathrm{AG}\ \mathrm{EF}\ \mathrm{AG}\ \mathrm{EF}\ \Phi$	$\mathrm{AG}\ \mathrm{EF}\ \Phi$	Y