Communication and Concurrency
Lecture 6

Colin Stirling (cps)

School of Informatics

7th October 2013

Temporal logic CTL$^-$: syntax

$$\Phi \quad ::= \quad \texttt{tt} \mid \texttt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K\rangle\Phi$$
$$\texttt{AG}\ \Phi \mid \texttt{EF}\ \Phi \mid \texttt{AF}\ \Phi \mid \texttt{EG}\ \Phi$$

A formula can be

Temporal logic CTL$^-$: syntax

$$\Phi \quad ::= \quad \texttt{tt} \mid \texttt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K\rangle\Phi$$
$$\texttt{AG}\ \Phi \mid \texttt{EF}\ \Phi \mid \texttt{AF}\ \Phi \mid \texttt{EG}\ \Phi$$

A formula can be

- a formula of Hennessy-Milner logic,

Temporal logic CTL$^-$: syntax

$$\Phi \quad ::= \quad \texttt{tt} \mid \texttt{ff} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [K]\Phi \mid \langle K\rangle\Phi$$
$$\texttt{AG}\ \Phi \mid \texttt{EF}\ \Phi \mid \texttt{AF}\ \Phi \mid \texttt{EG}\ \Phi$$

A formula can be

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

Temporal logic CTL$^-$: syntax

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

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

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

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

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

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 "$\mathtt{EG}\ \Phi$."

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

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

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."

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

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

Examples

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

Examples

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

Exercise

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

Does $P \models \Phi$ hold when Φ is

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

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

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

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 $\texttt{AG}\ ([\texttt{exit1}]\texttt{ff} \lor [\texttt{exit2}]\texttt{ff})$
- Absence of deadlock
- Absence of starvation

Specification: temporal properties

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

Specification: temporal properties

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

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

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

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

Exercise

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

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

Exercise

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

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