

COMP424/524-06A Topics in Software Engineering

Part I – CTL Model Checking

9. Computation Tree Logics

Robi Malik

THE UNIVERSITY OF
WAIKATO DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Examples

	CTL*	CTL	PLTL
AG (warm \Rightarrow AF \neg warm)			
AG (warm \Rightarrow F \neg warm)			
G (warm \Rightarrow X \neg warm)			
A (F warm \Rightarrow F ok)			
A (ok U error)			
G (warm \Rightarrow EF \neg warm)			

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 4

Formal Syntax of CTL*

State formulas

- Every atomic proposition is a state formula.
- If ϕ and ψ are state formulas then so are $\neg\phi$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \Rightarrow \psi$, $\phi \Leftrightarrow \psi$.
- If ϕ is a path formula, then **A** ϕ and **E** ϕ are state formulas.

Path formulas

- Every state formula is a path formula.
- If ϕ and ψ are path formulas, then so are **X** ϕ , **F** ϕ , **G** ϕ , ϕ **U** ψ .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 2

PLTL and CTL in NuSMV

-- CTL

SPEC

AG (request \rightarrow AF grant)

-- PLTL

LTLSPEC

G (request \rightarrow F grant)

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 5

Three Temporal Logics

CTL*

Every state formula is a CTL*-formula.

CTL

Every state formula in which temporal combinators are applied to state formulas only is a CTL-formula.

PLTL

Every path formula without any path quantifier is a PLTL-formula.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 3

Semantics of CTL*

Given

- Kripke structure $K = (Q, Prop, T, q_0, I)$,
- CTL*-formula ϕ ,

we want to define

under which conditions the formula ϕ is true in a state $q \in Q$.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 6

Defining the Semantics

- The truth of a **state formula** depends on the state
 - $\neg \text{train1onA} \vee \neg \text{train2onA}$
 - $\mathbf{AG} \neg \text{collision}$
- The truth of a **path formula** depends on the execution path
 - $\mathbf{GF} \text{req}$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 7

Path Formulas

Given:

- Path formula φ

$$\mathbf{G} R_A \quad \mathbf{F} P_A \quad \mathbf{G} \neg(P_A \wedge P_B)$$

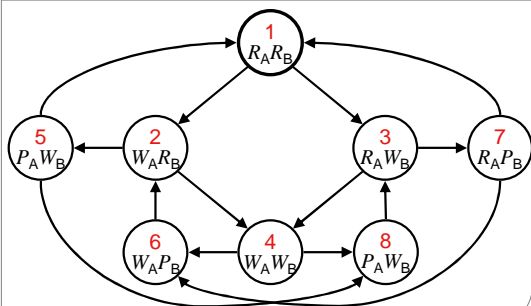
- Execution path $\sigma = \langle \sigma_0, \sigma_1, \dots \rangle$

To determine whether φ is true in σ :

- Determine truth of subformulas.
- Evaluate the temporal combinator for φ ...

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 10

Example Kripke Structure



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 8

Evaluating Temporal Combinators

- $\mathbf{X} \varphi$ is true on a path σ , if σ has more than one state, and φ is true in the second state of σ .
- $\mathbf{G} \varphi$ is true on a path σ , if φ is true in every state of σ .
- $\mathbf{F} \varphi$ is true on a path σ , if σ contains a state where φ is true.
- $\varphi \mathbf{U} \psi$ is true on a path σ , if σ contains a state q where ψ is true, and φ is true on every state in σ up to but not necessarily including q .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 11

Propositional Formulas

Given:

- Formula φ without temporal combinators

$$R_A \quad P_A \wedge P_B \quad W_A \Rightarrow P_A$$

- State $q \in Q$

To determine whether φ is true in q :

- Inspect the labels of state q .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 9

Path Quantifiers

Given:

- State formula φ with a path quantifier

$$\mathbf{EG} R_A \quad \mathbf{EF} P_A \quad \mathbf{AG} \neg(P_A \wedge P_B)$$

- State $q \in Q$

To determine whether φ is true in q :

- Determine truth of subformulas.
- Evaluate the path quantifier ...

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 12

Evaluating Path Quantifiers

- $A\phi$ is true in state q , if ϕ is true on every maximal path starting from q .
- $E\phi$ is true in state q , if ϕ is true on some maximal path starting from q .

Note:

- Execution paths must be **maximal**.
- A finite execution path can only be considered if it ends in a state without outgoing transitions.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 13

More Rules

$$A \phi \equiv \neg E \neg \phi$$

$$AG \phi \equiv \neg EF \neg \phi$$

$$AF \phi \equiv \neg EG \neg \phi$$

$$EG \phi \equiv \neg AF \neg \phi$$

$$EF \phi \equiv \neg AG \neg \phi$$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 16

At Last ...

Given:

- Path formula ϕ
- Kripke-structure K

We say:

- ϕ is **satisfied in K** , if ϕ is true for every maximal execution of K .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 14

Reading

Bérard et. al.:
Chapter 2 – Temporal Logic
Chapter 12 – NuSMV

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 17

Some Rules

$$G \phi \equiv \neg F \neg \phi$$

$$F \phi \equiv \text{true } U \phi$$

$$\phi W \psi \equiv (\phi U \psi) \vee G \phi$$

All path formulas can be written using the combinators **U** and **X** only.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-9 Slide 15