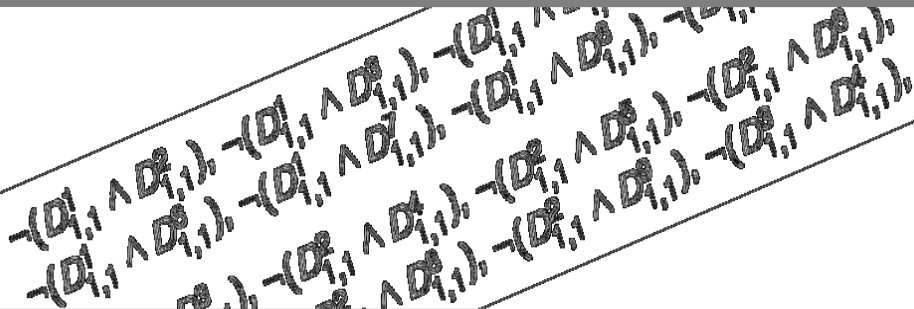


# Formale Systeme

## Lineare Temporale Logik

Prof. Dr. Bernhard Beckert | WS 2010/2011

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



## Definition

Eine **omega-Struktur**  $\mathcal{R} = (\mathbb{N}, <, \xi)$  für eine aussagenlogische Signatur  $P$  besteht aus der geordneten Menge der natürlichen Zahlen

$$(\mathbb{N}, <)$$

interpretiert als Menge abstrakter Zeitpunkte und einer Funktion

$$\xi : \mathbb{N} \rightarrow 2^P$$

mit der Intention

$$p \in \xi(n) \Leftrightarrow \text{in } \mathcal{R} \text{ ist } p \text{ zum Zeitpunkt } n \text{ wahr}$$

$\xi_n$  steht für das bei  $n$  beginnende Endstück von  $\xi$ :

$$\xi_n(m) = \xi(n + m) \quad \text{insbes. } \xi_0 = \xi$$

## Definition

$\Sigma$  eine Menge aller AL-Atome. *LTLFor* wird definiert durch

- 1  $\Sigma \subseteq LTLFor$
- 2  $\mathbf{1}, \mathbf{0} \in LTLFor$
- 3 Liegen  $A, B$  in *LTLFor*, dann auch alle aussagenlogischen Kombinationen von  $A$  und  $B$ .
- 4 für  $A, B \in LTLFor$  gilt auch
  - 1  $\Box A \in LTLFor$  und
  - 2  $\Diamond B \in LTLFor$  und
  - 3  $A \mathbf{U} B \in LTLFor$
  - 4  $X A$

Die Symbole  $\Box$ ,  $\Diamond$ ,  $X$  und  $\mathbf{U}$  heißen temporale Modaloperatoren.

## Definition

Sei  $\mathcal{R} = (\mathbb{N}, <, \xi)$  eine omega-Struktur und  $A$  eine LTL Formel.

$\xi \models p$             gdw     $p \in \xi(0)$     ( $p$  ein AL Atom)

$\xi \models op(A, B)$             für AL-Kombinationen  $op(A, B)$   
von  $A$  und  $B$  wie üblich

$\xi \models \Box A$             gdw    für alle  $n \in \mathbb{N}$  gilt  $\xi_n \models A$

$\xi \models \Diamond A$             gdw    es gibt ein  $n \in \mathbb{N}$  mit  $\xi_n \models A$

$\xi \models A \mathbf{U} B$             gdw    es gibt  $n \in \mathbb{N}$  mit  $\xi_n \models B$  und  
für alle  $m$  mit  $0 \leq m < n$  gilt  $\xi_m \models A$

$\xi \models X A$             gdw     $\xi_1 \models A$

# Visualisierung der LTL-Semantik

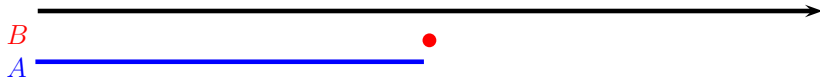
Szenarium für  $\Box A$



Szenarium für  $\Diamond A$



Szenarium für  $A \cup B$



# Reduktion auf U und 1

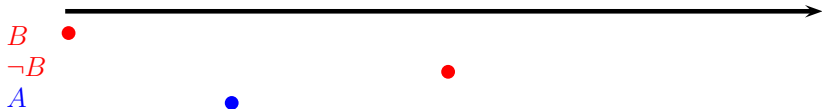
$$\begin{aligned}\diamond A &\leftrightarrow \mathbf{1 U A} \\ \square A &\leftrightarrow \neg(\mathbf{1 U \neg A})\end{aligned}$$

$\xi \models A \mathbf{U}_w B$     gdw    für alle  $n \in \mathbb{N}$  gilt  $\xi_n \models (A \wedge \neg B)$  oder  
es gibt  $n \in \mathbb{N}$  mit  $\xi_n \models B$  und  
für alle  $m$  mit  $0 \leq m < n$  gilt  $\xi_m \models A$

$\xi \models A \mathbf{V} B$     gdw     $\xi \models B$  und für alle  $n \in \mathbb{N}$  gilt  
falls  $\xi_n \models \neg B$  dann gibt es ein  $m$  mit  
 $0 \leq m < n$  und  $\xi_m \models A$

# Visualisierung von $\vee$

Szenarien für  $A \vee B$





$$① \quad A \mathbf{U} B \leftrightarrow (A \mathbf{U}_w B) \wedge \diamond B$$

$$② \quad A \mathbf{U}_w B \leftrightarrow A \mathbf{U} B \vee \square(A \wedge \neg B)$$

$$③ \quad A \mathbf{V} B \leftrightarrow \neg(\neg A \mathbf{U} \neg B)$$

$$④ \quad A \mathbf{U} B \leftrightarrow (B \vee (A \wedge X(A \mathbf{U} B)))$$

$$⑤ \quad A \mathbf{V} B \leftrightarrow (B \wedge A) \vee (B \wedge X(A \mathbf{V} B))$$

Sei  $p$  ein aussagenlogisches Atom.

Gesucht ist eine LTL-Formel  $A_{2p}$ , so daß für jedes  $\xi$  gilt

$$\xi \models A_{2p} \quad \text{gdw} \quad (n \text{ ist gerade} \Leftrightarrow p \in \xi(n))$$

$$A_{2p} = p \wedge X \neg p \wedge \Box(p \leftrightarrow XX p)$$

Erstaunlicherweise gibt es keine LTL-Formel  $A$  mit

$$\xi \models A \quad \text{gdw} \quad (n \text{ ist gerade} \Rightarrow p \in \xi(n))$$

REQUIREMENT: When a connection is not made to the server, the application should report an error and reset network component to initial state.

REFINEMENT: After `OpeningNetworkConnection`, an `ErrorMessage` will pop up in response to a `NetworkError`.

PATTERN: Response

SCOPE: After

PARAMETERS: Propositional

LTL:  $[\ ] (\text{OpenNetworkConnection} \rightarrow [\ ] (\text{NetworkError} \rightarrow \langle \rangle \text{ErrorMessage}))$

SOURCE: Jeff Isom \cite{isom:98}

DOMAIN: GUI

REQUIREMENT: When a connection is made to the SMTP server, all queued messages in the OutBox mail will be transferred to the server.

REFINEMENT: Before QueuedMailSent, SMTPServerConnected

PATTERN: Existence

SCOPE: Before

ALTERNATE: Global Precedence

PARAMETERS: Propositional

LTL:  $\langle \rangle$ QueuedMailSent  $\rightarrow$

$(\neg$ QueuedMailSent  $\cup$  SMTPServerConnected)

SOURCE: Jeff Isom \cite{isom:98}

DOMAIN: GUI