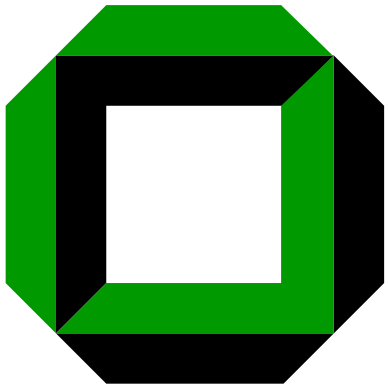
Formale Systeme

Prof. P.H. Schmitt

Fakultät für Informatik
Universität Karlsruhe (TH)

Winter 2007/2008



Vorlesungstermine

Do.24.01.
letztes Übungsblatt
Praxisaufgabe zu SPIN
Fr.25.01. keine Vorlesung
Do.31.01.
Fr.01.02.
Do.07.02. keine Vorlesung
Fr.08.02 keine Vorlesung
Do.14.02 (Wiederholung)
Fr.15.02. keine Vorlesung
1.Klausur 18.02. 14:00

Änderung des Verfahrens zu

Anmeldung für die Klausur

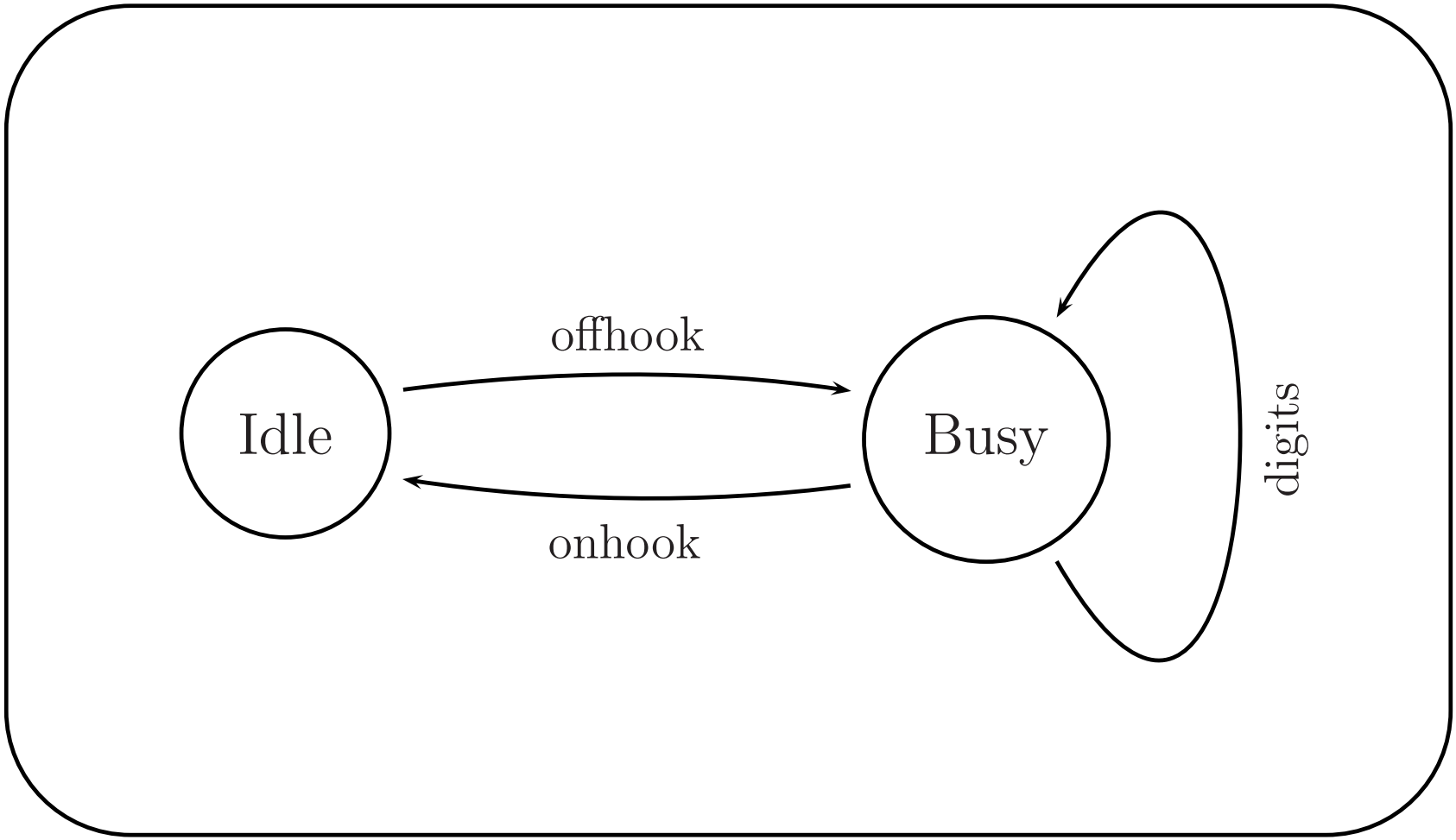
Anmeldung nur noch elektronisch!

bis Mi.13.Februar

Lineare Temporale Logik

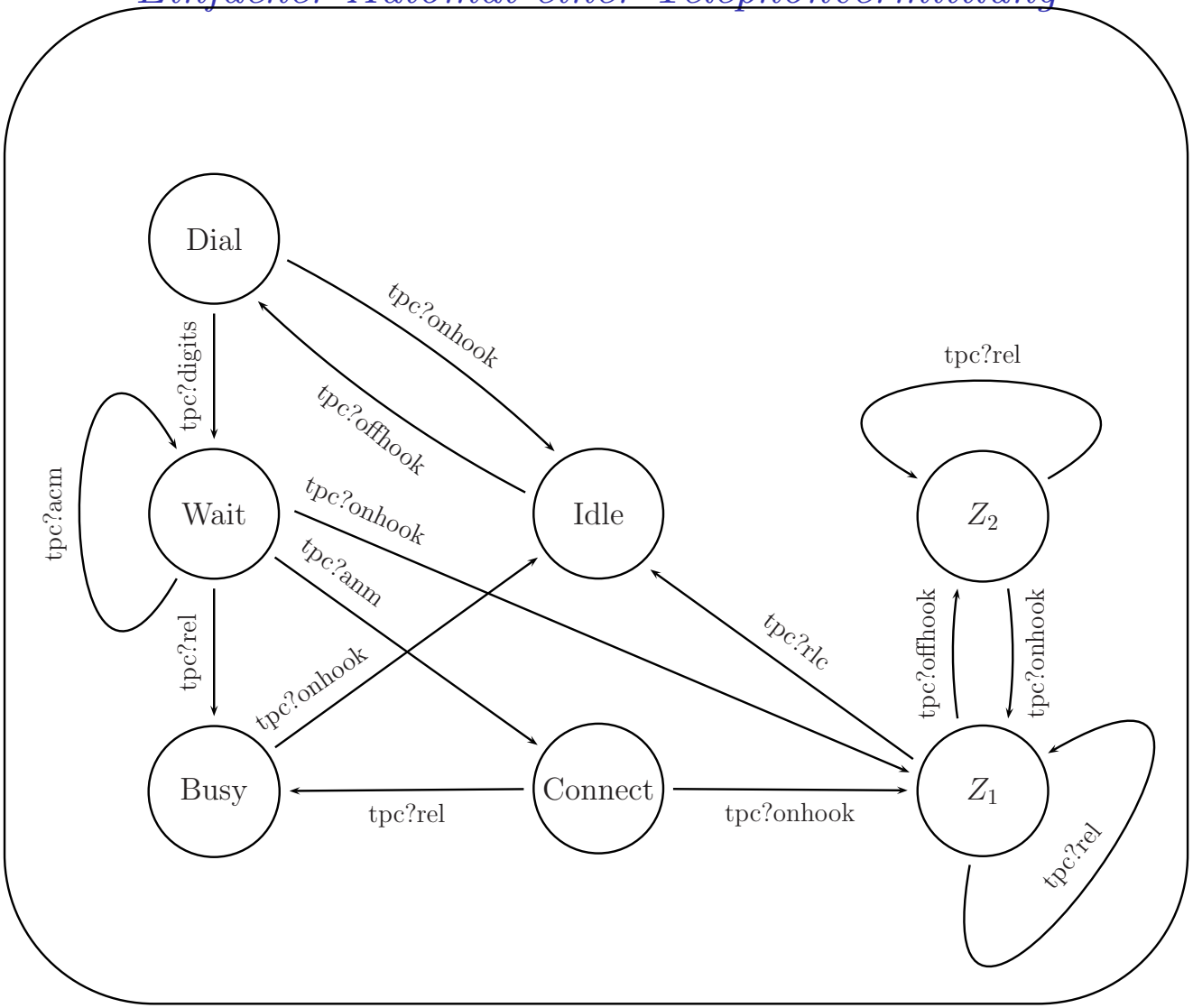
Einführendes Beispiel

Einfaches Modell eines Telefonteilnehmers



Einführendes Beispiel

Einfacher Automat einer Telephonvermittlung



Einführendes Beispiel

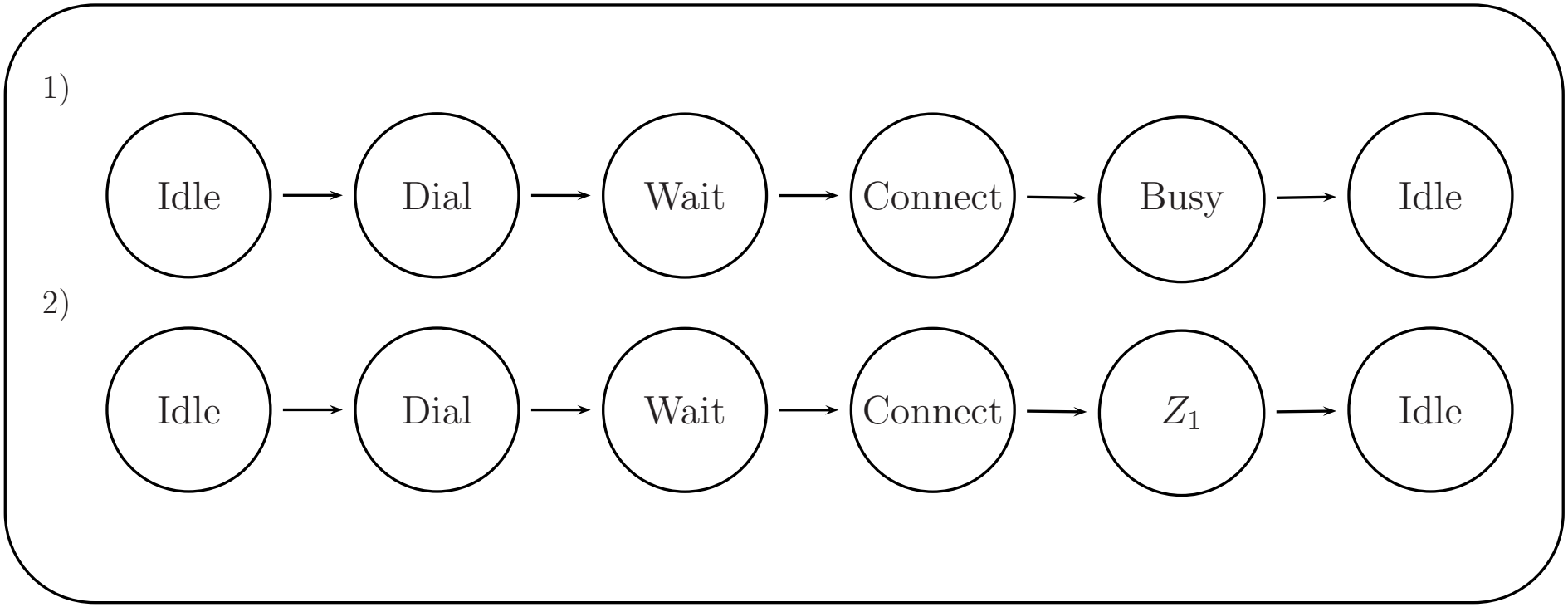
Nachrichtenvokabular

tpc?*xxx* bedeutet Nachricht *xxx* wird von Kanal *tpc* empfangen
tpc!*xxx* bedeutet Nachricht *xxx* wird über Kanal *tpc* geschickt

Nachricht	Bedeutung
offhook	Hörer wurde abgehoben
onhook	Hörer wurde aufgelegt
digits	Nummer wurde gewählt
iam	initial address message
acm	address complete message
rel	Einleitung des Verbindungsabbaus (release)
anm	End-zu-Endverbindung hergestellt
rlc	Quittierung des Verbindungsabbaus

Einführendes Beispiel

Beispielabläufe



LTL

Lineare Temporale Logik

Omega-Strukturen

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

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

mit der Intention

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

ξ_n steht für das bei n beginnende Endstück von ξ:

$$\xi_n(m) = \xi(n + m)$$

Inbesondere gilt $\xi_0 = \xi$.

LTL Formeln: LTLFor

Σ 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.

LTL Semantik

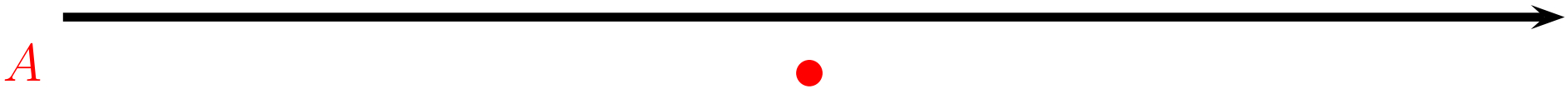
Sei $\mathcal{R} = (\mathbb{N}, <, \xi)$ eine omega-Struktur und A eine *TLT* Formel.

$\xi \models p$	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	$\xi_1 \models A$

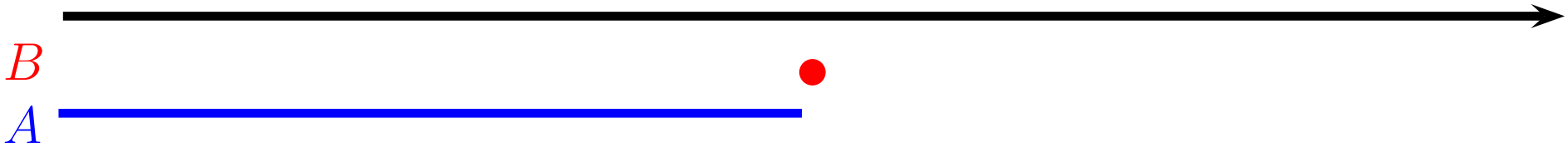
Visualisierung der LTL-Semantik

Szenarium für $\Box A$

Szenarium für $\Diamond A$



Szenarium für $A \mathbf{U} B$



Reduktion auf **U** *und* **1**

$$\Diamond A \leftrightarrow \quad \mathbf{1}\ \mathbf{U}\ A$$
$$\Box A \leftrightarrow \neg(\mathbf{1}\ \mathbf{U}\ \neg A)$$

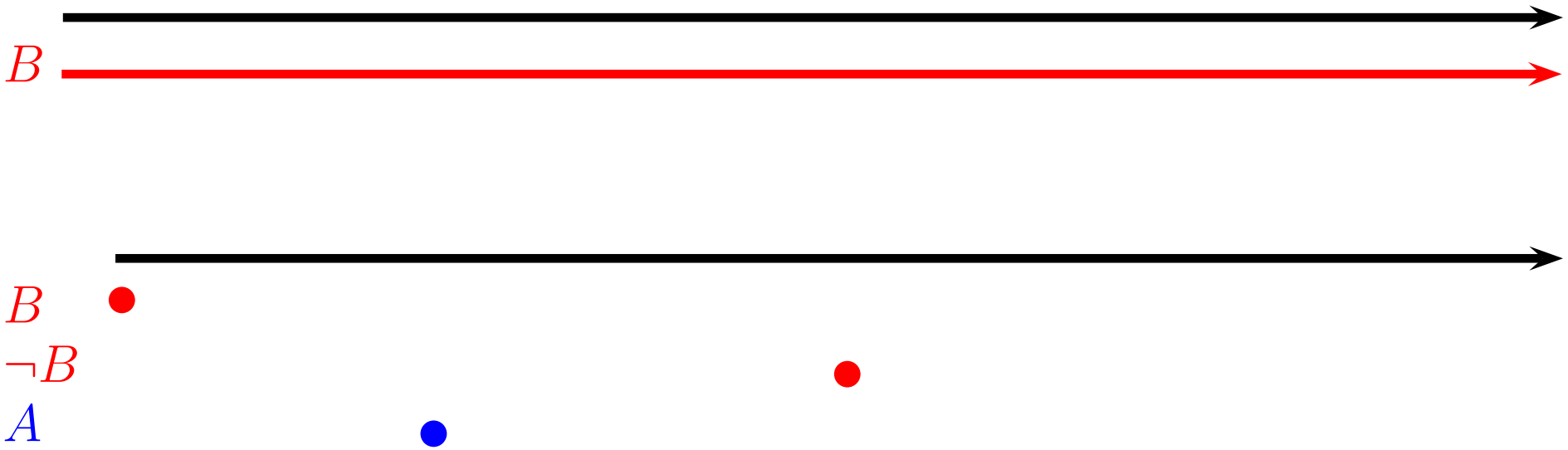
Zusätzliche Operatoren

$\xi \models A \; \mathbf{U}_w \; B$ 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 **V**

Szenarien für A **V** B



Lemma

1. $A \mathbf{U} B \leftrightarrow (A \mathbf{U}_w B) \wedge \Diamond B$
2. $A \mathbf{U}_w B \leftrightarrow A \mathbf{U} B \vee \Box(A \wedge \neg B)$
3. $A \mathbf{V} B \leftrightarrow \neg(\neg A \mathbf{U} \neg B)$
4. $A \mathbf{U} B \leftrightarrow (B \vee (A \wedge X (A \mathbf{U} B)))$
5. $A \mathbf{V} B \leftrightarrow (B \wedge A) \vee (B \wedge X (A \mathbf{V} B))$

Beispiel

Sei p ein aussagenlogisches Atom.
Gesucht ist eine LTL-Formel A_{2p}, so daß für jedes ξ 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 TLT-Formel A mit

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

Beispiele aus Mustersammlungen

```
REQUIREMENT: When a connection is not made to the server,
    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:  [](OpenNetworkConnection ->
          [](NetworkError -> <>ErrorMessage))
SOURCE: Jeff Isom \cite{isom:98}
DOMAIN: GUI
```

Beispiele aus Mustersammlungen

```
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:  <>QueuedMailSent ->
           (!QueuedMailSent U SMTPServerConnected)
SOURCE: Jeff Isom \cite{isom:98}
DOMAIN: GUI
```