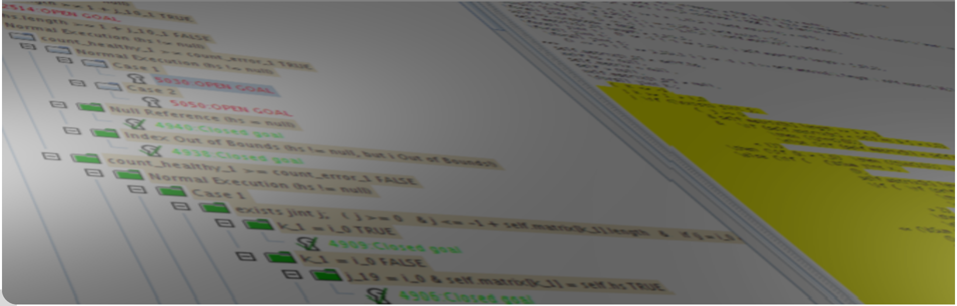
Formale Systeme

LTL und Büchi-Automaten

Prof. Dr. Peter H. Schmitt

KIT – Institut für Theoretische Informatik



Omega-Strukturen (Wiederholung)

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

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

mit der Intention

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

LTL und Büchi-Automaten

Für einen Automaten $\mathcal{B} = (S, V, s_0, \delta, F)$ mit

$$\begin{array}{rcl} V & = & 2^{\Sigma}, \quad \text{wobei} \\ \Sigma & = & \text{Menge aussagenlogischer Atome,} \end{array}$$

können wir

- Omega-Strukturen ξ über Σ und
- unendliche Wörter $w \in V^{\omega}$ über V

identifizieren.

Notation

Für die folgenden drei Beispiele vereinbaren wir die folgende Notation

- eine aussagenlogische Signatur Σ mit $p, q \in \Sigma$

Notation

Für die folgenden drei Beispiele vereinbaren wir die folgende Notation

- eine aussagenlogische Signatur Σ mit $p, q \in \Sigma$
- $V = 2^{\Sigma}$

Notation

Für die folgenden drei Beispiele vereinbaren wir die folgende Notation

- eine aussagenlogische Signatur Σ mit $p, q \in \Sigma$
- $V = 2^{\Sigma}$
- $P = \{b \in V \mid p \in b\}$

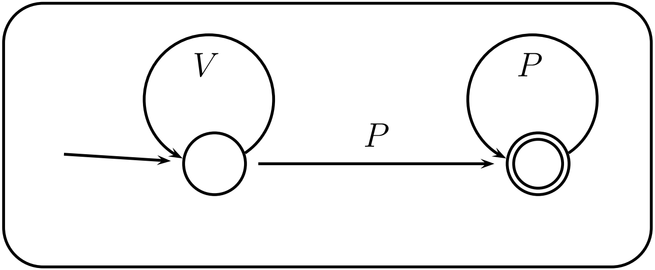
Notation

Für die folgenden drei Beispiele vereinbaren wir die folgende Notation

- eine aussagenlogische Signatur Σ mit $p, q \in \Sigma$
- $V = 2^{\Sigma}$
- $P = \{b \in V \mid p \in b\}$
- $Q = \{b \in V \mid q \in b\}$

Automat für $\Diamond\Box p$

Für den Automaten $\mathcal{A}_{dbp}$

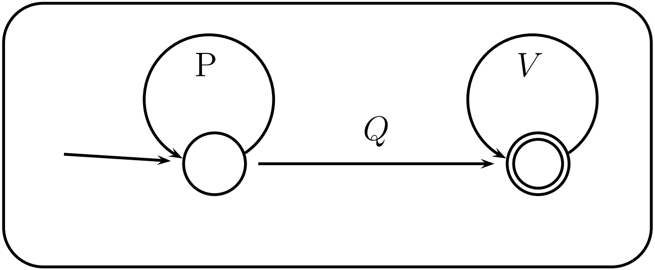


gilt

$$\xi \in L^{\omega}(\mathcal{A}_{dbp}) \quad \Leftrightarrow \quad \xi \models \Diamond\Box p$$

Automat für p **U** q

Für den Automaten $\mathcal{A}_{puntilq}$

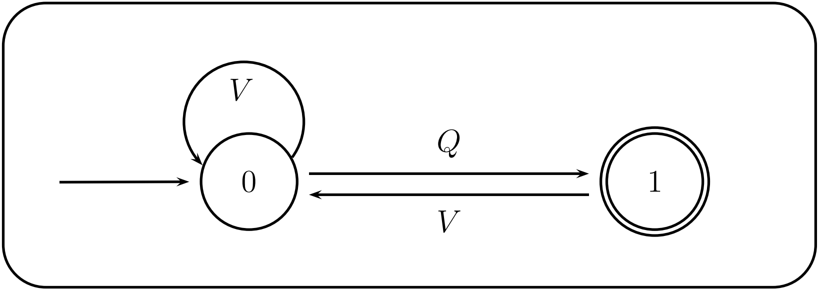


gilt

$$\xi \in L^\omega(\mathcal{A}_{puntilq}) \quad \Leftrightarrow \quad \xi \models p \, \mathbf{U} \, q$$

Automat für $\Box\Diamond q$

Für den Automaten $\mathcal{A}_{infq}$



gilt

$$\xi \in L^{\omega}(\mathcal{A}_{infq}) \quad \Leftrightarrow \quad \xi \models \Box\Diamond q$$

Lemma
Automat für Konjunktion

Seien

$$\mathcal{A}_1 = (S_1, V, s_1^0, \delta_1, F_1),$$
$$\mathcal{A}_2 = (S_2, V, s_2^0, \delta_2, F_2)$$

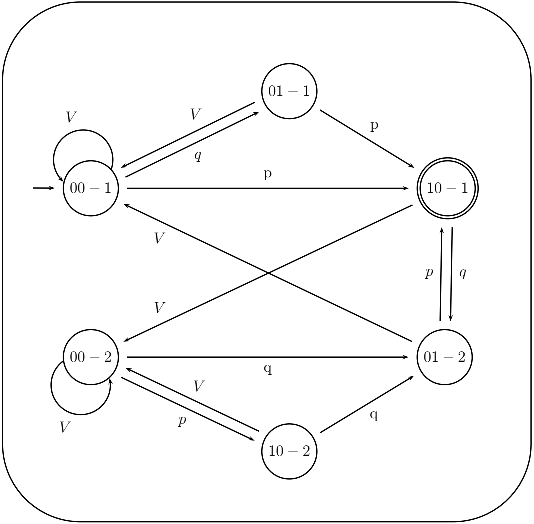
Büchi-Automaten,
C_1, C_2 LTL-Formeln mit

$$\mathcal{A}_1 \models C_1$$
$$\mathcal{A}_2 \models C_2$$

Dann gibt es einen Büchi-Automaten $\mathcal{C}$ mit

$$\mathcal{C} \models C_1 \wedge C_2$$

Automat für $\Box\Diamond p \wedge \Box\Diamond q$



Allgemeine Konstruktion für Konjunktionsautomaten

Gegeben $\mathcal{A}_i = (S_i, s_i^0, \delta_i, F_i)$
Gesucht $\mathcal{C} = (S, s^0, \delta, F)$ mit $L^\omega(\mathcal{C}) = L^\omega(\mathcal{A}_1) \cap L^\omega(\mathcal{A}_2)$.

$$
\begin{array}{lcl}
S & = & S_1 \times S_2 \times \{1, 2\} \\
s^0 & = & (s_1^0, s_2^0, 1) \\
F & = & F_1 \times S_2 \times \{1\} \\
\text{falls } s_1 \in F_1 \text{ und } i = 1 & & \\
(t_1, t_2, 2) \in \delta((s_1, s_2, i), a) & \Leftrightarrow & t_1 \in \delta_1(s_1, a) \text{ und } t_2 \in \delta_2(s_2, a) \\
\text{falls } s_2 \in F_2 \text{ und } i = 2 & & \\
(t_1, t_2, 1) \in \delta((s_1, s_2, i), a) & \Leftrightarrow & t_1 \in \delta_1(s_1, a) \text{ und } t_2 \in \delta_2(s_2, a) \\
\text{sonst} & & \\
(t_1, t_2, i) \in \delta((s_1, s_2, i), a) & \Leftrightarrow & i \in \{1, 2\}, \\
 & & t_1 \in \delta_1(s_1, a) \text{ und } t_2 \in \delta_2(s_2, a)
\end{array}
$$

Theorem

Zu jeder LTL-Formel

$$B$$

gibt es einen – effektiv konstruierbaren – Büchi-Automaten

$$\mathcal{A}_B$$

mit

$$L^\omega(\mathcal{A}_B) = \{\xi \in V^\omega \mid \xi \models B\}$$

Beweis: Konstruktion folgt
Weitere Details im Skriptum.

Beweis

Konstruktion

Gegeben: LTL-Formel B

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

nur: $\neg$, $\wedge$, $\vee$, $\mathbf{U}$, $\mathbf{V}$, X in B

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

nur: $\neg$, $\wedge$, $\vee$, $\mathbf{U}$, $\mathbf{V}$, X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

nur: $\neg$, $\wedge$, $\vee$, $\mathbf{U}$, $\mathbf{V}$, X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

$V = 2^P$

Beweis

Konstruktion

Gegeben: LTL-Formel B
P Menge der AL-Atome, B in Negationsnormalform
nur: $\neg, \wedge, \vee$, **U** , **V** , X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

$V = 2^P$
$subF(B)$ sei die Menge aller Teilformeln von B

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

nur: $\neg$, $\wedge$, $\vee$, **U** , **V** , X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

$V = 2^P$

$subF(B)$ sei die Menge aller Teilformeln von B

$$
\begin{array}{rcl}
S & = & \{s \subseteq subF(B) \mid \mathbf{0} \notin s, \mathbf{1} \in s \\
 & & \qquad \text{wenn } (C_1 \wedge C_2) \in s \text{ dann } C_1 \in s \text{ und } C_2 \in s \\
 & & \qquad \text{wenn } (C_1 \vee C_2) \in s \text{ dann } C_1 \in s \text{ oder } C_2 \in s \ \} \\
S_0 & = & \{s \in S \mid \ B \in s\}
\end{array}
$$

Beweis

Konstruktion

Gegeben: LTL-Formel B

P Menge der AL-Atome, B in Negationsnormalform

nur: $\neg, \wedge, \vee,$ $\mathbf{U}$, $\mathbf{V}$, X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

$V = 2^P$

$subF(B)$ sei die Menge aller Teilformeln von B

$$\begin{array}{lcl} S & = & \{s \subseteq subF(B) \mid \mathbf{0} \notin s, \mathbf{1} \in s \\ & & \qquad\qquad \text{wenn } (C_1 \wedge C_2) \in s \text{ dann } C_1 \in s \text{ und } C_2 \in s \\ & & \qquad\qquad \text{wenn } (C_1 \vee C_2) \in s \text{ dann } C_1 \in s \text{ oder } C_2 \in s \;\} \\ S_0 & = & \{s \in S \mid \; B \in s\} \end{array}$$

$E_i = A_i \,\mathbf{U}\, B_i$ für $1 \leq i \leq k$ alle Fmln der Form $A \,\mathbf{U}\, B$ in $subF(B)$.

Beweis

Konstruktion

Gegeben: LTL-Formel B
P Menge der AL-Atome, B in Negationsnormalform
nur: $\neg$, $\wedge$, $\vee$, $\mathbf{U}$, $\mathbf{V}$, X in B

Gesucht: Büchi-Automat $\mathcal{A}_B = (V, S, S_0, \delta, \mathcal{F})$

$V = 2^P$
$subF(B)$ sei die Menge aller Teilformeln von B

$$\begin{array}{lcl} S & = & \{s \subseteq subF(B) \mid \mathbf{0} \notin s, \mathbf{1} \in s \\ & & \qquad \text{wenn } (C_1 \wedge C_2) \in s \text{ dann } C_1 \in s \text{ und } C_2 \in s \\ & & \qquad \text{wenn } (C_1 \vee C_2) \in s \text{ dann } C_1 \in s \text{ oder } C_2 \in s \ \} \\ S_0 & = & \{s \in S \mid \ B \in s\} \end{array}$$

$E_i = A_i \, \mathbf{U} \, B_i$ für $1 \leq i \leq k$ alle Fmln der Form $A \, \mathbf{U} \, B$ in $subF(B)$.

$\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$ mit

$$\mathcal{F}_i = \{s \in S \mid E_i \notin s \text{ oder } E_i \in s \text{ und } B_i \in s\}$$

Konstruktion

Die Übergangsfunktion δ

Für $s, t \in S$ und $a \in 2^P$ gilt $t \in \delta(s, a)$ wenn alle folgenden Bedingungen erfüllt sind

1. Für alle $p \in P$ mit $p \in s$ gilt $p \in a$.

Konstruktion

Die Übergangsfunktion δ

Für $s, t \in S$ und $a \in 2^P$ gilt $t \in \delta(s, a)$ wenn alle folgenden Bedingungen erfüllt sind

1. Für alle $p \in P$ mit $p \in s$ gilt $p \in a$.
2. Für alle $p \in P$ mit $\neg p \in s$ gilt $p \notin a$.

Konstruktion

Die Übergangsfunktion δ

Für $s, t \in S$ und $a \in 2^P$ gilt $t \in \delta(s, a)$ wenn alle folgenden Bedingungen erfüllt sind

1. Für alle $p \in P$ mit $p \in s$ gilt $p \in a$.
2. Für alle $p \in P$ mit $\neg p \in s$ gilt $p \notin a$.
3. Falls $X\ A \in s$ dann $A \in t$.

Konstruktion

Die Übergangsfunktion δ

Für $s, t \in S$ und $a \in 2^P$ gilt $t \in \delta(s, a)$ wenn alle folgenden Bedingungen erfüllt sind

1. Für alle $p \in P$ mit $p \in s$ gilt $p \in a$.
2. Für alle $p \in P$ mit $\neg p \in s$ gilt $p \notin a$.
3. Falls $X\ A \in s$ dann $A \in t$.
4. Falls $A\ \mathbf{U}\ B \in s$, dann gilt $B \in s$ oder ($A \in s$ und $A\ \mathbf{U}\ B \in t$).

Konstruktion

Die Übergangsfunktion δ

Für $s, t \in S$ und $a \in 2^P$ gilt $t \in \delta(s, a)$ wenn alle folgenden Bedingungen erfüllt sind

1. Für alle $p \in P$ mit $p \in s$ gilt $p \in a$.
2. Für alle $p \in P$ mit $\neg p \in s$ gilt $p \notin a$.
3. Falls $X\ A \in s$ dann $A \in t$.
4. Falls $A\ \mathbf{U}\ B \in s$, dann gilt $B \in s$ oder ($A \in s$ und $A\ \mathbf{U}\ B \in t$).
5. Falls $A\ \mathbf{V}\ B \in s$, dann ($B \in s$ und $A \in s$) oder ($B \in s$ und $A\ \mathbf{V}\ B \in t$).

Beispiel

$B = \Diamond\Box p$

Beispiel

$B = \Diamond\Box p$
$B = 1 \; \mathbf{U} \; \Box p$

Beispiel

$B = \Diamond\Box p$
$B = 1 \mathbf{U} \Box p$
$B = 1 \mathbf{U} \neg(\neg 0 \mathbf{U} \neg p)$

Beispiel

$$B = \Diamond\Box p$$
$$B = 1 \;\mathbf{U}\; \Box p$$
$$B = 1 \;\mathbf{U}\; \neg(\neg 0 \;\mathbf{U}\; \neg p)$$
$$B = 1 \;\mathbf{U}\; (0 \;\mathbf{V}\; p)$$

Beispiel

$B = \Diamond\Box p$
$B = 1 \mathbf{U} \Box p$
$B = 1 \mathbf{U} \neg(\neg 0 \mathbf{U} \neg p)$
$B = 1 \mathbf{U} (0 \mathbf{V} p)$

$V = \{\{p\} \equiv p, \quad \{\} \equiv \neg p\}$

Beispiel

$B = \Diamond\Box p$
$B = 1 \; \mathbf{U} \; \Box p$
$B = 1 \; \mathbf{U} \; \neg(\neg 0 \; \mathbf{U} \; \neg p)$
$B = 1 \; \mathbf{U} \; (0 \; \mathbf{V} \; p)$

$V = \{\{p\} \equiv p, \quad \{\} \equiv \neg p\}$
$subFml(B) = \{B, B_0 = 0 \; \mathbf{V} \; p, p, \qquad \mathbf{1}, \mathbf{0}\}$

Beispiel

$$B = \Diamond\Box p$$
$$B = 1 \;\mathbf{U}\; \Box p$$
$$B = 1 \;\mathbf{U}\; \neg(\neg 0 \;\mathbf{U}\; \neg p)$$
$$B = 1 \;\mathbf{U}\; (0 \;\mathbf{V}\; p)$$

$$V = \{\{p\} \equiv p, \quad \{\} \equiv \neg p\}$$
$$subFml(B) = \{B, B_0 = 0 \;\mathbf{V}\; p, p, \qquad \mathbf{1}, \mathbf{0}\}$$
$$S = \{\{B\}, \{B_0\}, \{p\}, \{B, B_0, p\}, \{B, B_0\}\{B, p\}\{B_0, p\}\}$$

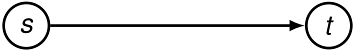
Beispiel

$B = \Diamond\Box p$
$B = 1 \ \mathbf{U} \ \Box p$
$B = 1 \ \mathbf{U} \ \neg(\neg 0 \ \mathbf{U} \ \neg p)$
$B = 1 \ \mathbf{U} \ (0 \ \mathbf{V} \ p)$

$V = \{\{p\} \equiv p, \quad \{\} \equiv \neg p\}$
$subFml(B) = \{B, B_0 = 0 \ \mathbf{V} \ p, p, \qquad \mathbf{1}, \mathbf{0}\}$
$S = \{\{B\}, \{B_0\}, \{p\}, \{B, B_0, p\}, \{B, B_0\}\{B, p\}\{B_0, p\}\}$
$E_1 = 1 \ \mathbf{U} \ B_0$ i.e. $A_1 = \mathbf{1}$, $B_1 = B_0$
$\mathcal{F} = \{F_1\}$
$F_1 = \{\{B_0\}, \{p\}, \{B_0, p\}, \{B, B_0\}, \{B, B_0, p\}\}$

Beispiel

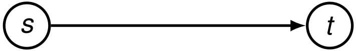
Übergangsfunktion



4. Falls $A\ \mathbf{U}\ B \in s$, dann gilt $B \in s$ oder ($A \in s$ und $A\ \mathbf{U}\ B \in t$).
5. Falls $A\ \mathbf{V}\ B \in s$, dann ($B \in s$ und $A \in s$) oder ($B \in s$ und $A\ \mathbf{V}\ B \in t$).

Beispiel

Übergangsfunktion



4. Falls $A\ \mathbf{U}\ B \in s$, dann gilt $B \in s$ oder ($A \in s$ und $A\ \mathbf{U}\ B \in t$).
5. Falls $A\ \mathbf{V}\ B \in s$, dann ($B \in s$ und $A \in s$) oder ($B \in s$ und $A\ \mathbf{V}\ B \in t$).

4. Falls $1\ \mathbf{U}\ B_0 \in s$, dann gilt $B_0 \in s$ oder ($1 \in s$ und $1\ \mathbf{U}\ B_0 \in t$).
5. Falls $0\ \mathbf{V}\ p \in s$, dann ($p \in s$ und $0 \in s$) oder ($p \in s$ und $0\ \mathbf{V}\ p \in t$).

Beispiel

Übergangsfunktion

$$s \longrightarrow t$$

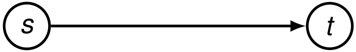
4. Falls $A\ \mathbf{U}\ B \in s$, dann gilt $B \in s$ oder ($A \in s$ und $A\ \mathbf{U}\ B \in t$).
5. Falls $A\ \mathbf{V}\ B \in s$, dann ($B \in s$ und $A \in s$) oder ($B \in s$ und $A\ \mathbf{V}\ B \in t$).

4. Falls $1\ \mathbf{U}\ B_0 \in s$, dann gilt $B_0 \in s$ oder ($1 \in s$ und $1\ \mathbf{U}\ B_0 \in t$).
5. Falls $0\ \mathbf{V}\ p \in s$, dann ($p \in s$ und $0 \in s$) oder ($p \in s$ und $0\ \mathbf{V}\ p \in t$).

4. Falls $B \in s$, dann gilt $B_0 \in s$ oder $B \in t$.
5. Falls $B_0 \in s$, dann ($p \in s$ und $B_0 \in t$).

Beispiel

Übergangsfunktion



$B \in s, B_0 \notin s$	$B \in t$
$B \in s, B_0 \in s$	keine Einschränkung
$B_0 \in s, p \in s$	$B_0 \in t$
$B_0 \in s, p \notin s$	nicht möglich

Beispiel

Übergangsfunktion

$$s \longrightarrow t$$

$B \in s, B_0 \notin s$	$B \in t$
$B \in s, B_0 \in s$	keine Einschränkung
$B_0 \in s, p \in s$	$B_0 \in t$
$B_0 \in s, p \notin s$	nicht möglich

$$S = \{\{B\}, \{B_0\}, \{p\}, \{B, B_0, p\}, \{B, B_0\}, \{B, p\}\{B_0, p\}\}$$

Beispiel

Übergangsfunktion

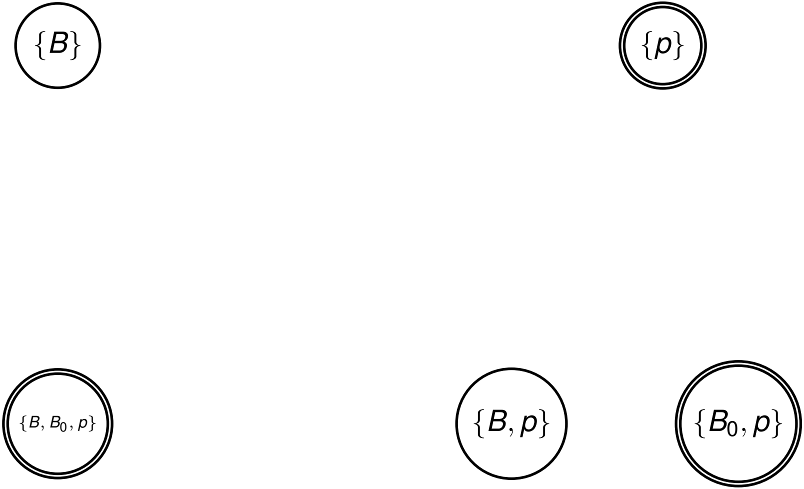
$$s \longrightarrow t$$

$B \in s, B_0 \notin s$	$B \in t$
$B \in s, B_0 \in s$	keine Einschränkung
$B_0 \in s, p \in s$	$B_0 \in t$
$B_0 \in s, p \notin s$	nicht möglich

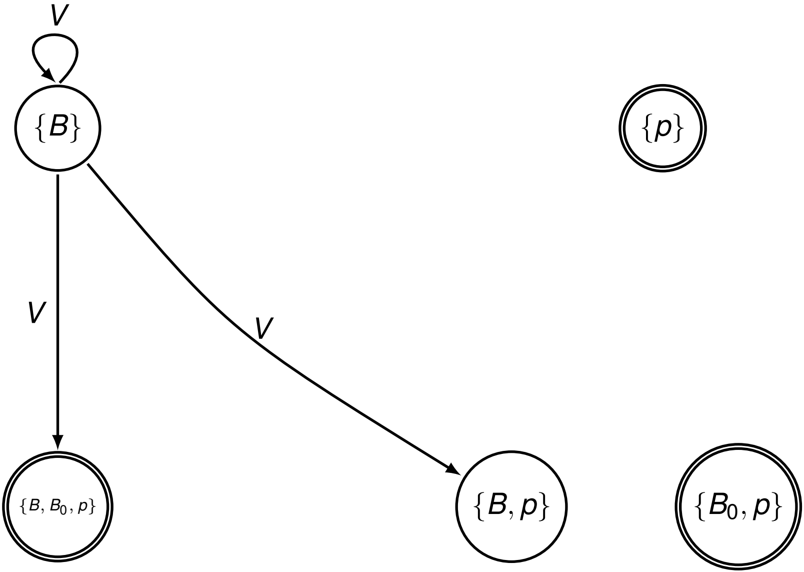
$$S = \{\{B\}, \{B_0\}, \{p\}, \{B, B_0, p\}, \{B, B_0\}, \{B, p\}\{B_0, p\}\}$$

Sackgassen

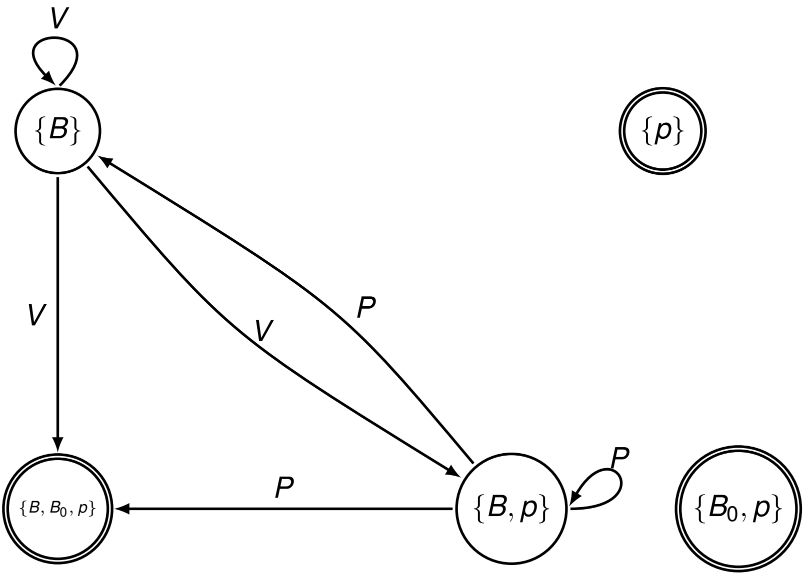
Beispiel



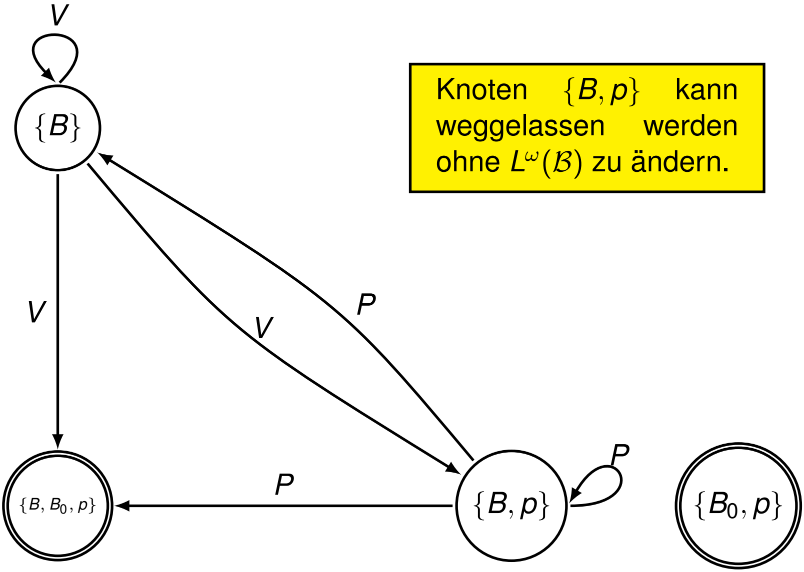
Beispiel



Beispiel

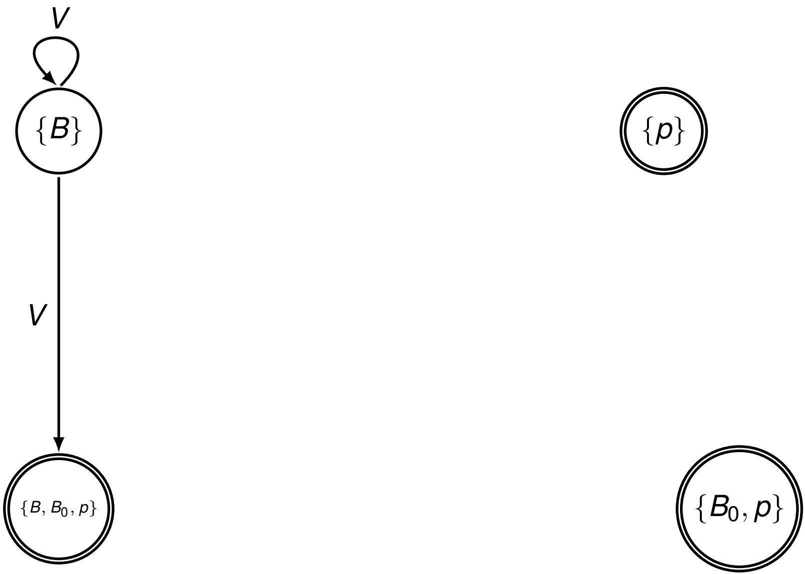


Beispiel

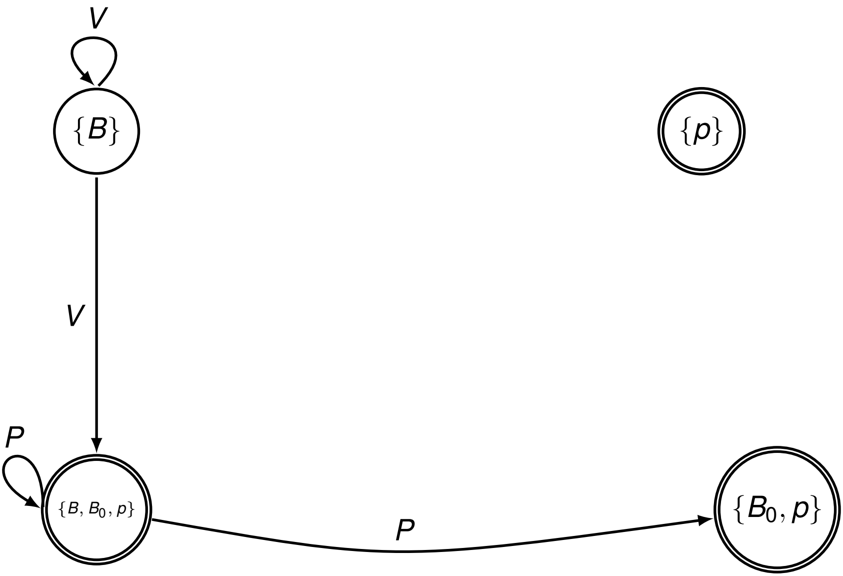


Knoten $\{B, p\}$ kann weggelassen werden ohne $L^\omega(\mathcal{B})$ zu ändern.

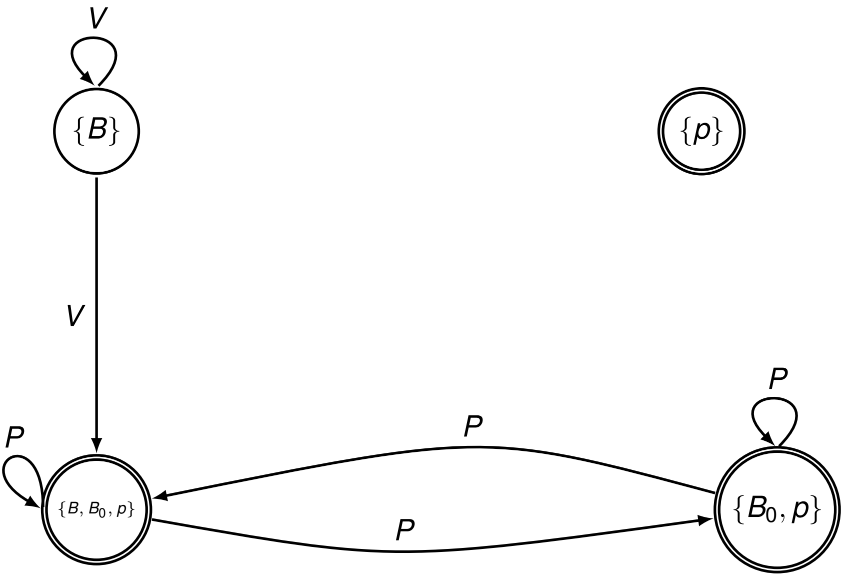
Beispiel



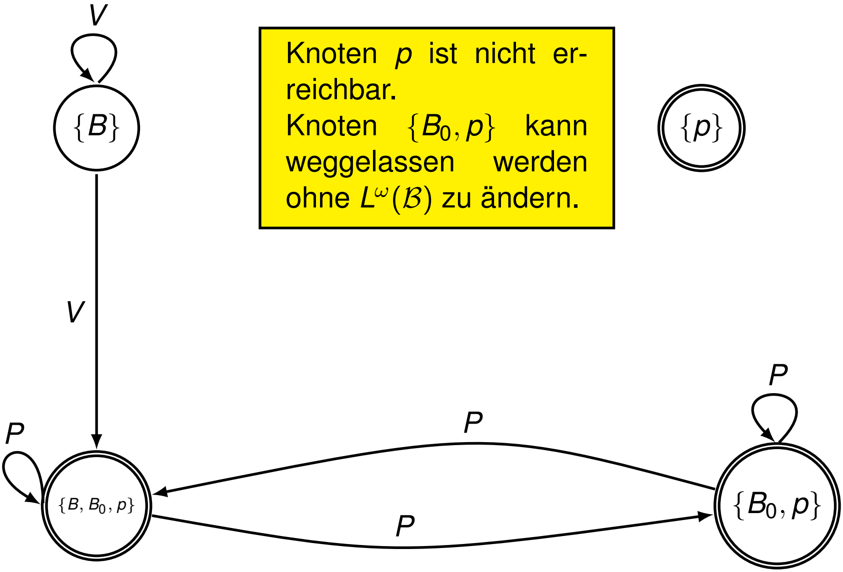
Beispiel



Beispiel



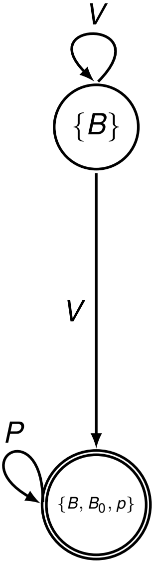
Beispiel



Knoten p ist nicht erreichbar.
Knoten $\{B_0, p\}$ kann weggelassen werden ohne $L^\omega(\mathcal{B})$ zu ändern.

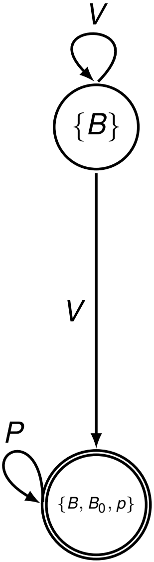
Beispiel

Endergebnis



Beispiel

Endergebnis



Beide verbleibenden Zustände sind Startzustände. Man sieht aber, daß es genügt $\{B\}$ als Startzustand zu haben.

Korollar

Erfüllbarkeit und Allgemeingültigkeit von LTL Formeln ist entscheidbar.

Korollar

Erfüllbarkeit und Allgemeingültigkeit von LTL Formeln ist entscheidbar.

Beweis:

Korollar

Erfüllbarkeit und Allgemeingültigkeit von LTL Formeln ist entscheidbar.

Beweis:

Man konstruiert die Büchi-Automaten $\mathcal{A}_B$ und $\mathcal{A}_{\neg B}$. Es gilt

$$\begin{array}{lcl} B \text{ ist erfüllbar} & \Leftrightarrow & L^\omega(\mathcal{A}_B) \neq \emptyset \\ B \text{ ist allgemeingültig} & \Leftrightarrow & L^\omega(\mathcal{A}_{\neg B}) = \emptyset \end{array}$$

Für jeden Büchi-Automaten $\mathcal{C}$ ist die Frage $L^\omega(\mathcal{C}) = \emptyset$? entscheidbar.

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Die LTL-beschreibbaren Mengen sind eine echte Teilklasse der durch Büchi-Automaten bescheibbaren.

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Die LTL-beschreibbaren Mengen sind eine echte Teilklasse der durch Büchi-Automaten bescheibbaren.
Äquivalent sind:

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Die LTL-beschreibbaren Mengen sind eine echte Teilklasse der durch Büchi-Automaten bescheibbaren.
Äquivalent sind:

- LTL

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Die LTL-beschreibbaren Mengen sind eine echte Teilklasse der durch Büchi-Automaten bescheibbaren.
Äquivalent sind:

- LTL
- Prädikatenlogik erster Stufe

Vergleich der Ausdrucksstärke

Zur Beschreibung von Mengen von Omega-Strukturen sind äquivalent:

- Büchi-Automaten
- ω-reguläre Mengen
- Monadische Logik zweiter Stufe

Die LTL-beschreibbaren Mengen sind eine echte Teilklasse der durch Büchi-Automaten bescheibbaren.
Äquivalent sind:

- LTL
- Prädikatenlogik erster Stufe
- stern-freie ω-reguläre Mengen