

Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2014/2015

Prädikatenlogik: Semantik

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK

Ist die Formel

$$q(x) \rightarrow \exists y(in(y, x) \wedge kl(y)),$$

wahr?

Die Signatur $\Sigma = \{k(), q(), d(), kl(), gr(), in(,)\}$ liegt fest.

Die Wahrheit ist abhängig von

- ▶ einer Interpretation $\mathcal{D} = (D, I)$
- ▶ einer Variablenbelegung β

Einführendes Beispiel 2

```

1      int max = 0;
2      if ( a.length > 0 ) max = a[0];
3      int i = 1;
4      while ( i < a.length ) {
5          if ( a[i] > max ) max = a[i];
6          ++i;
7      }
  
```

Nachbedingung:

$(\forall \text{ forall int } j; (j \geq 0 \ \& \ j < a.length \rightarrow \text{max} \geq a[j]))$

&
 $(a.length > 0 \rightarrow$
 $\quad \exists \text{ exists int } j; (j \geq 0 \ \& \ j < a.length \ \& \ \text{max} = a[j]))$
 $)$

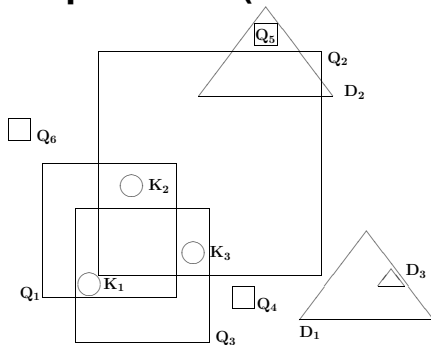
Definition

Es sei Σ eine Signatur der PL1.

Eine *Interpretation* $\mathcal{D}$ von Σ ist ein Paar (D, I) mit

1. D ist eine beliebige, nichtleere Menge
2. I ist eine Abbildung der Signatursymbole, die
 - ▶ jeder Konstanten c ein Element $I(c) \in D$
 - ▶ für $n \geq 1$: jedem n -stelligen Funktionssymbol f eine Funktion $I(f) : D^n \rightarrow D$
 - ▶ jedem 0-stelligen Prädikatsymbol P einen Wahrheitswert $I(P) \in \{\mathbf{W}, \mathbf{F}\}$
 - ▶ für $n \geq 1$: jedem n -stelligen Prädikatsymbol p eine n -stellige Relation $I(p) \subseteq D^n$ zuordnet.

Beispiel-Interpretation (Tarski's World)



$$P_{\Sigma} = \{k(), q(), d(), kl(), gr(), in(,)\}$$

$$D_{Bsp} = \{Q_1, \dots, Q_6\} \cup \{K_1, K_2, K_3, D_1, D_2, D_3\}$$

$$I_{Bsp}(q) = \{Q_1, \dots, Q_6\}, \quad I_{Bsp}(k) = \{K_1, K_2, K_3\}, \quad I_{Bsp}(d) = \{D_1, D_2, D_3\}$$

$$I_{Bsp}(in) = \{(K_1, Q_1), (K_1, Q_3), (K_2, Q_1), (K_2, Q_2), (K_3, Q_2), (K_3, Q_3), (D_3, D_1), (Q_5, D_2)\}$$

Definition

Es sei (D, I) eine Interpretation von Σ .

Eine *Variablenbelegung* (oder kurz *Belegung* über D) ist eine Funktion

$$\beta : \text{Var} \rightarrow D.$$

Zu β , $x \in \text{Var}$ und $d \in D$ definieren wir die *Modifikation* von β an der Stelle x zu d :

$$\beta_x^d(y) = \begin{cases} d & \text{falls } y = x \\ \beta(y) & \text{falls } y \neq x \end{cases}$$

Definition Auswertungsfunktion

Sei (D, I) Interpretation von Σ , β Variablenbelegung über D .
Wir definieren eine Funktion $val_{D,I,\beta}$, mit

$$\begin{aligned} val_{D,I,\beta}(t) &\in D && \text{für } t \in Term_{\Sigma} \\ val_{D,I,\beta}(A) &\in \{\mathbf{W}, \mathbf{F}\} && \text{für } A \in For_{\Sigma} \end{aligned}$$

Definition Auswertung von Termen

$$\begin{aligned} val_{D,I,\beta}(x) &= \beta(x) \text{ für } x \in Var \\ val_{D,I,\beta}(f(t_1, \dots, t_n)) &= (I(f))(val_{D,I,\beta}(t_1), \dots, val_{D,I,\beta}(t_n)) \end{aligned}$$

Definition

- $val_{D,I,\beta}(1) = \mathbf{W}$
 $val_{D,I,\beta}(0) = \mathbf{F}$
 $val_{D,I,\beta}(s \doteq t) := \begin{cases} \mathbf{W} & \text{falls } val_{D,I,\beta}(s) = val_{D,I,\beta}(t) \\ \mathbf{F} & \text{sonst} \end{cases}$
 $val_{D,I,\beta}(P) \quad \quad \quad := I(P) \text{ für 0-stellige Prädikate } P$
 $val_{D,I,\beta}(p(t_1, \dots, t_n)) :=$
 $\begin{cases} \mathbf{W} & \text{falls } (val_{D,I,\beta}(t_1), \dots, val_{D,I,\beta}(t_n)) \in I(p) \\ \mathbf{F} & \text{sonst} \end{cases}$

Definition

2. $val_{D,I,\beta}(X)$ für $X \in \{\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B\}$ wie in der Aussagenlogik.
3. $val_{D,I,\beta}(\forall x A) :=$
$$\begin{cases} \mathbf{W} & \text{falls für alle } d \in D : val_{D,I,\beta_x^d}(A) = \mathbf{W} \\ \mathbf{F} & \text{sonst} \end{cases}$$
4. $val_{D,I,\beta}(\exists x A) :=$
$$\begin{cases} \mathbf{W} & \text{falls ein } d \in D \text{ existiert mit } val_{D,I,\beta_x^d}(A) = \mathbf{W} \\ \mathbf{F} & \text{sonst} \end{cases}$$

Beispiel für Auswertung

Sei die Interpretation $\mathcal{D}_{Bsp} = (D_{Bsp}, I_{Bsp})$ und die Variablenbelegung $\beta(x) = Q_1$. Werte darin die Formel aus:

$$q(x) \rightarrow \exists y(in(y, x) \wedge kl(y))$$

$$val_{\mathcal{D}_{Bsp}, \beta}(x) = Q_1 \in I(q),$$

also

$$val_{\mathcal{D}_{Bsp}, \beta}(q(x)) = \mathbf{W}.$$

Wähle K_1 als Belegung für y .

$$(K_1, Q_1) \in I_{Bsp}(in) \text{ und}$$

$$K_1 \in I_{Bsp}(kl),$$

also

$$val_{\mathcal{D}_{Bsp}, \beta_y^{K_1}}((in(y, x) \wedge kl(y))) = \mathbf{W},$$

also

$$val_{\mathcal{D}_{Bsp}, \beta}(\exists y(in(y, x) \wedge kl(y))) = \mathbf{W}$$

Insgesamt

$$val_{\mathcal{D}_{Bsp}, \beta}(q(x) \rightarrow \exists y(in(y, x) \wedge kl(y))) = \mathbf{W}$$

Theorem

$\mathcal{D}$ sei Interpretation, β, γ Variablenbelegungen

1. Gilt für den Term t $\beta(x) = \gamma(x)$ für alle $x \in \text{Var}(t)$, dann $\text{val}_{\mathcal{D},\beta}(t) = \text{val}_{\mathcal{D},\gamma}(t)$.
2. Gilt für die Formel A $\beta(x) = \gamma(x)$ für alle $x \in \text{Frei}(A)$, dann $\text{val}_{\mathcal{D},\beta}(A) = \text{val}_{\mathcal{D},\gamma}(A)$.
3. Ist $A \in \text{For}_{\Sigma}$ geschlossen, dann gilt $\text{val}_{\mathcal{D},\beta}(A) = \text{val}_{\mathcal{D},\gamma}(A)$

Beweis: Durch strukturelle Induktion unter Ausnutzung der Definition von val .

Konsequenz: Ist $A \in \text{For}_{\Sigma}$ geschlossen, schreiben wir $\text{val}_{\mathcal{D}}(A)$ statt $\text{val}_{\mathcal{D},\beta}(A)$.

Notation: $\mathcal{D} \models A$ bedeutet $\text{val}_{\mathcal{D}}(A) = \mathbf{W}$.

Signatur $\Sigma_{arith} = \{0, 1, +, *, <\}$

Struktur 1: Die mathematischen ganzen Zahlen

$$\mathcal{Z} = (\mathbb{Z}, \overset{\mathbb{Z}}{+}, \overset{\mathbb{Z}}{*}, \overset{\mathbb{Z}}{<}).$$

Struktur 2: Die ganzen Zahlen in Java (int)

$$\mathcal{Z}_{Jint} = (\mathbb{Z}_{Jint}, \overset{J}{+}, \overset{J}{*}, \overset{J}{<}).$$

$$\mathbb{Z}_{Jint} := [int_MIN, int_MAX] = [-2^{31}, 2^{31} - 1]$$

wobei: $\overset{J}{n} + m :=$ nächste Folie

$\overset{J}{n} * m :=$ nächste Folie

$\overset{J}{n} < m :\Leftrightarrow n <^{\mathbb{Z}} m$

Für $n, m \in [int_MIN, int_MAX]$ definiere

$$n \overset{J}{+} m := int_MIN \overset{\mathbb{Z}}{+} (int_HALFRANGE \overset{\mathbb{Z}}{+} (n \overset{\mathbb{Z}}{+} m)) \overset{\mathbb{Z}}{\%} int_RANGE$$

$$n \overset{J}{*} m := int_MIN \overset{\mathbb{Z}}{+} (int_HALFRANGE \overset{\mathbb{Z}}{+} (n \overset{\mathbb{Z}}{*} m)) \overset{\mathbb{Z}}{\%} int_RANGE$$

wobei $int_HALFRANGE = 2^{31}$ und $int_RANGE = 2^{32}$.

Dann gilt z.B.

$$int_MAX \overset{J}{+} 1 = int_MIN \quad \text{und} \quad int_MIN \overset{J}{+} (-1) = int_MAX$$

Vergleich von $\mathcal{Z}$ und $\mathcal{Z}_{Jint}$

Formel ϕ	$\mathcal{Z} \models \phi$	$\mathcal{Z}_{jint} \models \phi$
$\forall x \exists y (x < y)$	ja	nein
$\forall x \forall y ((x + 1) * y = x * y + y)$	ja	ja
$\exists x (0 < x \wedge x + 1 < 0)$	nein	ja

Theorem

Σ sei eine Signatur,
 $\mathcal{D}$ eine Interpretation für Σ ,
 β, β' Belegungen,
 σ eine Substitution und $t \in \text{Term}_{\Sigma}$.

Dann gilt

$$\text{val}_{\mathcal{D},\beta}(\sigma(t)) = \text{val}_{\mathcal{D},\beta'}(t).$$

wobei

$$\beta'(x) = \text{val}_{\mathcal{D},\beta}(\sigma(x))$$

für alle $x \in \text{Var}$.

Strukturelle Induktion nach t .

Fall $t = x \in \text{Var}$:

$$\begin{aligned} \text{val}_{\mathcal{D},\beta}(\sigma(x)) &= \beta'(x) && \text{Def. von } \beta' \\ &= \text{val}_{\mathcal{D},\beta'}(x) && \text{Def. von } \text{val}(x) \end{aligned}$$

Fall $t = f(t_1, \dots, t_n)$:

$$\begin{aligned} & \text{val}_{\mathcal{D},\beta}(\sigma(f(t_1, \dots, t_n))) \\ &= \text{val}_{\mathcal{D},\beta}(f(\sigma(t_1), \dots, \sigma(t_n))) \\ &= l(f)(\text{val}_{\mathcal{D},\beta}(\sigma(t_1)), \dots, \text{val}_{\mathcal{D},\beta}(\sigma(t_n))) \\ &= l(f)(\text{val}_{\mathcal{D},\beta'}(t_1), \dots, \text{val}_{\mathcal{D},\beta'}(t_n)) \\ &\quad \text{(nach Induktionsannahme)} \\ &= \text{val}_{\mathcal{D},\beta'}(f(t_1, \dots, t_n)) \end{aligned}$$

Kollisionsfreie Substitutionen

Es bezeichne F die Formel

$$p(x, z) \wedge \exists y(p(x, y) \wedge p(z, y) \rightarrow p(x, y))$$

Welche der folgenden Substitutionen ist kollisionsfrei für F ?

- | | | |
|------------|------------------------|-----------------------|
| σ_1 | $\{x/a, z/b\}$ | <i>kollisionsfrei</i> |
| σ_2 | $\{x/(x+z), z/(x+z)\}$ | <i>kollisionsfrei</i> |
| σ_3 | $\{x/(x+y), z/a\}$ | <i>Kollision</i> |
| σ_4 | $\{y/(x+y)\}$ | <i>kollisionsfrei</i> |
| σ_5 | $\{x/z\}$ | <i>kollisionsfrei</i> |

Theorem

Σ sei eine Signatur, $\mathcal{D}$ eine Interpretation für Σ ,
 β, β' Belegungen, $A \in \text{For}_\Sigma$ und
 σ eine für A **kollisionsfreie** Substitution.

Dann gilt:

$$\text{val}_{\mathcal{D},\beta}(\sigma(A)) = \text{val}_{\mathcal{D},\beta'}(A),$$

wobei

$$\beta'(x) = \text{val}_{\mathcal{D},\beta}(\sigma(x))$$

für alle $x \in \text{Var}$.

Induktion nach A .

Exemplarisch: Schritt von A nach $\exists xA$.

Notation: val_{β} abkürzend für $val_{\mathcal{D},\beta}$.

Außerdem: $\sigma_x(x) = x$, $\sigma_x(y) = \sigma(y)$ für $y \neq x$.

$$val_{\beta}(\sigma(\exists xA)) = \mathbf{W}$$

$$\text{gdw } val_{\beta}(\exists x\sigma_x(A)) = \mathbf{W}$$

Anwendung von σ

$$\text{gdw } val_{\beta_x^d}(\sigma_x(A)) = \mathbf{W} \text{ für ein } d \in D$$

Def. von val

$$\text{gdw } val_{(\beta_x^d)''}(A) = \mathbf{W}$$

Ind.-Vor.

$$\text{wo } (\beta_x^d)''(y) = val_{\beta_x^d}(\sigma_x(y)) \text{ für alle } y.$$

$$\text{gdw } val_{(\beta')_x^d}(A) = \mathbf{W}$$

Lücke

$$\text{gdw } val_{\beta'}(\exists xA) = \mathbf{W}$$

Def. von val

Beweis

Schließen der Lücke

Der Beweis wird vollständig geführt sein, wenn wir die Lücke

$$(\beta_x^d)'' = (\beta')_x^d$$

schließen können. Wir müssen für jede Variable $y \in \text{Frei}(A)$ zeigen $(\beta_x^d)''(y) = (\beta')_x^d(y)$.

$y = x$:

$$\begin{aligned}
 (\beta_x^d)''(x) &= \text{val}_{\beta_x^d}(\sigma_x(x)) && \text{Def. von } (\beta_x^d)'' \\
 &= \text{val}_{\beta_x^d}(x) && \text{Def. von } \sigma_x \\
 &= \beta_x^d(x) && \text{Def. von } \text{val} \text{ für Variable} \\
 &= d && \text{Def. der modifizierten Belegung} \\
 &= (\beta')_x^d(x) && \text{Def. der modifizierten Belegung}
 \end{aligned}$$

Beweis (Forts.)

Schließen der Lücke $(\beta_x^d)'' = (\beta')_x^d$

$y \neq x$, y frei in A :

$$\begin{aligned}
 (\beta_x^d)''(y) &= \text{val}_{\beta_x^d}(\sigma_x(y)) && \text{Def. von } (\beta_x^d)'' \\
 &= \text{val}_{\beta_x^d}(\sigma(y)) && \text{Def. von } \sigma_x \\
 &= \text{val}_{\beta}(\sigma(y)) && \text{da } x \text{ nicht in } \sigma(y) \text{ vorkommt} \\
 &&& \text{Kollisionsfreiheit von } \sigma \\
 &= \beta'(y) && \text{Def. von } \beta' \\
 &= (\beta')_x^d(y) && \text{Def. der modifizierten Belegung}
 \end{aligned}$$

Sir Anthony „Tony“ Hoare



Sir C.A.R. Hoare

Studied philosophy at Oxford U.

Graduated from Moscow State U., 1959

Programmer for Elliott Brothers, 1960

Prof. of CS at Queen's U. Belfast, 1968

*An axiomatic basis for computer
programming*

Communications ACM, 1969

Oxford U. Programming Research, 1977

Microsoft Research, Cambridge, now

Zuweisungsregel im Hoare-Kalkül

$$\{\{x/s\}A\} x := s \{A\}$$

wobei die Substitution $\{x/s\}$ kollisionsfrei sein muß.

Die Zuweisungsregel besagt, daß

- ▶ ausgehend von einem Zustand, in dem die Formel $\{x/s\}A$ wahr ist,
- ▶ nach Ausführung der Programmstücks $x := s$
- ▶ ein Zustand erreicht wird, in dem die Formel A gilt.

Hintergrund-Interpretation $\mathcal{H}$.

Programmzustand = Variablenbelegung β .

Gelte $val_{\mathcal{H},\beta}(\{x/s\}A) = W$

Nach der Zuweisung $x := s$ wird ein Zustand β' erreicht

$$\beta'(x) := val_{\mathcal{H},\beta}(s)$$

$$\beta'(y) := \beta(y) \text{ für } y \neq x$$

Die Regel behauptet $val_{\mathcal{H},\beta'}(A) = W$.

Das ist gerade die Aussage des Substitutionslemmas für die Formel A ist und die Substitution $\sigma = \{x/s\}$.

Theorem

*Sei Σ eine Signatur,
 $\mathcal{D}$ eine Interpretation für Σ ,
 β eine Belegung und
 σ eine für A kollisionsfreie Substitution
mit $\sigma(y) = y$ für alle Variablen $y \neq x$,
dann gilt:*

- ▶ $val_{\mathcal{D},\beta}(\forall xA \rightarrow \sigma(A)) = W$
- ▶ $val_{\mathcal{D},\beta}(\sigma(A) \rightarrow \exists xA) = W.$

Wir nehmen an, daß $val_{\mathcal{D},\beta}(\forall xA) = W$ gilt, d.h.

$$val_{\mathcal{D},\beta_x^d}(A) = W \text{ für alle } d \in D.$$

Zu zeigen ist

$$val_{\mathcal{D},\beta}(\sigma(A)) = W$$

Nach dem Substitutionslemma ist das gleichbedeutend mit

$$val_{\mathcal{D},\beta'}(A) = W$$

wobei

$$\beta'(y) = val_{\mathcal{D},\beta}(\sigma(y)) = \begin{cases} \beta(y) & \text{falls } x \neq y \\ val_{\mathcal{D},\beta}(\sigma(x)) & \text{falls } y = x \end{cases}$$

Also $\beta' = \beta_x^d$, wenn man $d = val_{\mathcal{D},\beta}(\sigma(x))$ wählt.

Die zweite Aussage läßt sich analog beweisen.

Den Modell- und Folgerungsbegriff definieren wir nur für Formeln und Formelmengen ohne freie Variablen. Das ist mit Abstand der häufigste Anwendungsfall. Der Fall mit freien Variablen wird ausführlich in den Übungsaufgaben im Skript behandelt.

Definition

- ▶ Eine Interpretation $\mathcal{D}$ über Σ nennen wir ein **Modell** einer Formel A ohne freie Variablen über Σ , wenn $val_{\mathcal{D}}(A) = W$.
- ▶ $\mathcal{D}$ heißt **Modell** einer Formelmenge M ohne freie Variablen, wenn für jede Formel $B \in M$ gilt $val_{\mathcal{D}}(B) = W$.

Definition

Es sei $M \subseteq \text{For}_\Sigma$, $A \in \text{For}_\Sigma$, beide ohne freie Variablen.

$$M \models_\Sigma A \quad :\Leftrightarrow$$

Jedes Modell von M ist auch Modell von A .

Lies: **Aus M folgt A** (über Σ).

Kurznotationen:

$$\models \text{ statt } \models_\Sigma, \quad \models A \text{ für } \emptyset \models A, \quad B \models A \text{ für } \{B\} \models A.$$

$$M \models A \quad \text{gdw} \quad M \cup \{\neg A\} \\ \text{hat kein Modell}$$

Definition

$A \in \text{For}_\Sigma$ heißt

- ▶ **allgemeingültig** gdw $\models A$
- ▶ **erfüllbar** gdw $\neg A$ ist nicht allgemeingültig.

Theorem

1. *Die folgenden Aussagen sind äquivalent:*
 - 1.1 *A allgemeingültig*
 - 1.2 *Jede Interpretation $\mathcal{D}$ ist Modell von A.*
 - 1.3 *$\text{val}_{\mathcal{D}}(A) = W$ für alle $\mathcal{D}$.*
2. *Die folgenden Aussagen sind äquivalent:*
 - 2.1 *A erfüllbar*
 - 2.2 *Es gibt $\mathcal{D}$ mit $\text{val}_{\mathcal{D}}(A) = W$*

Beispiele für allgemeingültige Formeln

1. $\neg \forall x A \leftrightarrow \exists x \neg A$,
2. $\neg \exists x A \leftrightarrow \forall x \neg A$
3. $\forall x \forall y A \leftrightarrow \forall y \forall x A$,
4. $\exists x \exists y A \leftrightarrow \exists y \exists x A$
5. $\forall x (A \wedge B) \leftrightarrow \forall x A \wedge \forall x B$
6. $\exists x (A \vee B) \leftrightarrow \exists x A \vee \exists x B$
7. $\forall \vec{y} (A \wedge Qx B \leftrightarrow Qx (A \wedge B))$,
falls $x \notin \text{Frei}(A)$ und $\vec{y}$ alle freie Variablen in $A \wedge Qx B$ sind.
8. $\forall \vec{y} (A \vee Qx B \leftrightarrow Qx (A \vee B))$,
falls $x \notin \text{Frei}(A)$ und $\vec{y}$ alle freie Variablen in $A \wedge Qx B$ sind.

Zeige

Für alle $\mathcal{D}, \beta$ gilt $val_{\mathcal{D}, \beta}(A \rightarrow \forall x B) = val_{\mathcal{D}, \beta}(\forall x(A \rightarrow B))$
Voraussetzung: $x \notin \text{Frei}(A)$.

Falls $val_{\mathcal{D}, \beta}(A \rightarrow \forall x B) = W$, dann folgt unmittelbar aus der Definition von val $val_{\mathcal{D}, \beta}(\forall x(A \rightarrow B)) = W$ (Übung).

Sei jetzt $val_{\mathcal{D}, \beta}(\forall x(A \rightarrow B)) = W$, d. h. für alle $d \in D$:
 $(val_{\mathcal{D}, \beta_x^d}(A) = W \Rightarrow val_{\mathcal{D}, \beta_x^d}(B) = W)$. (*)

Angenommen, es wäre $val_{\mathcal{D}, \beta}(A \rightarrow \forall x B) = F$. Dann gilt also
 $val_{\mathcal{D}, \beta}(A) = W$ und $val_{\mathcal{D}, \beta}(\forall x B) = F$
es gibt also ein $e \in D$ mit $val_{\mathcal{D}, \beta_x^e}(B) = F$.

Wegen $x \notin \text{Frei}(A)$ gilt auch $val_{\mathcal{D}, \beta_x^e}(A) = W$. Aus (*) folgt somit der Widerspruch: $val_{\mathcal{D}, \beta_x^e}(B) = W$.

Gilt folgendes?

$$\left. \begin{array}{l} \forall x \forall y \forall z (r(x, y) \wedge r(y, z) \rightarrow r(x, z)) \\ \forall x \forall y (r(x, y) \rightarrow r(y, x)) \\ \forall x \exists y (r(x, y)) \end{array} \right\} \models \forall x r(x, x)$$

Anders gesagt:

$$\left. \begin{array}{l} \text{Transitivität} \\ \text{Symmetrie} \\ \text{Endlosigkeit} \end{array} \right\} \models \text{Reflexivität}$$

Die Antwort ist

JA

2. Beispiel für ein Folgerbarkeitsproblem

Gilt folgendes?

$$\neg \exists x (a < x \wedge c(x) \wedge \forall y (a \leq y < x \rightarrow b(y)))$$

$\models$

$$\exists x (a < x \wedge \neg c(x) \wedge \forall y (a \leq y < x \rightarrow \neg b(y)))$$

Gegenbeispiel:

a		p_1		p_2
·	$<$	·	$<$	·
$b(a)$		$\neg b(p_1)$		$\neg b(p_2)$
$\neg c(a)$		$\neg c(p_1)$		$c(p_2)$