

PS Grenzen der Berechenbarkeit - 5. Vortrag

David Asher

15. Juni 2007

Gliederung des Vortrags

- ▶ Das Axiomensystem P.E.
- ▶ Arithmetisierung des P.E.-Systems

Erinnerung: Beweissysteme

Ein Axiomensystem (Beweissystem) besteht aus

- ▶ Einer Menge aus (allgemeingültigen) Axiomen
- ▶ Einer Menge (korrekter) Ableitungsregeln

Unterteilung der Axiome

Die Axiome des P.E.-Systems lassen sich in vier Gruppen unterteilen

- ▶ Logische Axiome (Gruppe 1 + 2)
- ▶ Arithmetische Axiome (Gruppe 3 + 4)

Gruppe 1 - Axiome der Aussagenlogik

- ▶ $(F \supset (G \supset F))$
- ▶ $(F \supset (G \supset H)) \supset ((F \supset G) \supset (F \supset H))$
- ▶ $((\sim F \supset \sim G) \supset (G \supset F))$

Gruppe 2 - Axiome der Prädikatenlogik

- ▶ $(\forall v_i(F \supset G) \supset (\forall v_i F \supset \forall v_i G))$
- ▶ $(F \supset \forall v_i F)$
 v_i kommt nicht frei in F vor
- ▶ $\exists v_i(v_i = t)$
 v_i kommt nicht in t vor
- ▶ $(v_i = t \supset (X_1 v_i X_2 \supset X_1 t X_2))$
 X_1 und X_2 so gewählt, dass $X_1 v_i X_2$ atomare Formel

Gruppe 3 - Arithmetische Axiome

- ▶ $v_1' = v_2' \supset v_1 = v_2$
- ▶ $\sim \bar{0} = v_1'$
- ▶ $(v_1 + \bar{0}) = v_1$
- ▶ $(v_1 + v_2') = (v_1 + v_2)'$
- ▶ $(v_1 \cdot \bar{0}) = \bar{0}$
- ▶ $(v_1 \cdot v_2') = ((v_1 \cdot v_2) + v_1)$
- ▶ $(v_1 \leq \bar{0} \equiv v_1 = \bar{0})$
- ▶ $(v_1 \leq v_2' \equiv (v_1 \leq v_2 \vee v_1 = v_2'))$
- ▶ $((v_1 \leq v_2) \vee (v_2 \leq v_1))$
- ▶ $(v_1 \mathbf{E} \bar{0}) = \bar{0}'$
- ▶ $(v_1 \mathbf{E} v_2') = ((v_1 \mathbf{E} v_2) \cdot v_1)$

Gruppe 4 - Induktionsaxiome (Hilfsdefinition)

- ▶ $F[v'_1] := \forall v_i (v_i = v'_1 \supset \forall v_1 (v_1 = v_i \supset F))$
Wobei $F(v_1)$ Formel mit freier Variable v_1
- ▶ D.h. jedes Auftreten von v_1 als freie Variable in F wird durch v'_1 ersetzt

Gruppe 4 - Induktionsaxiome

$$\blacktriangleright \underbrace{(F[\bar{0}])}_{IA} \supset \underbrace{(\forall v_1 (F(v_1) \supset F[v'_1]))}_{IS} \supset \forall v_1 F(v_1))$$

Ableitungsregeln von P.E.

- ▶ Regel 1 - Modus Ponens
Aus F , $(F \supset G)$ folgt G .
- ▶ Regel 2 - Generalisation
Aus F folgt $\forall v_i F$.

Hinweis zur Korrektheit

- ▶ Wegen Regel 2 (Aus F folgt $\forall v_i F$), gilt Korrektheit in P.E. nur für Formeln ohne freie Variablen.
- ▶ Beispiel: Wenn $F := v_i \leq 0$, dann ist $(\forall v_i F)$ falsch.

Beweis in P.E.

- ▶ Beweis Ein *Beweis* in System ist eine endliches Tupel (Sequenz) aus Formeln, so dass jede Formel
 - ▶ Ein Axiom
 - ▶ Eine Ableitung mit Regel 1 aus zwei früheren Formeln
 - ▶ Eine Ableitung mit Regel 2 aus einer früheren Formelist.

Beweisbarkeit in P.E.

- ▶ Beweisbarkeit

Eine Formel F ist (in P.E.) *beweisbar*, wenn es einen Beweis gibt, in der F vorkommt.

Arithmetisierung des P.E. Systems

- ▶ Ziel: Zeigen, dass P (Gödelnrm. der beweisbaren Sätze) Arithmetische Menge

Die Relationen B, E und P

Wir definieren uns drei Hilfsrelationen

- ▶ $xB_b y$ wenn x mit y beginnt (Notation zur Basis b)
- ▶ $xE_b y$ wenn x mit y endet
- ▶ $xP_b y$ wenn x ein Teil von y ist

Kleines Beispiel

- ▶ 54300166
- ▶ 54 B_b 54300166
- ▶ 66 E_b 54300166
- ▶ 43 P_b 54300166
- ▶ Auch: 543 B_b 543 und 543 E_b 543

Spezialfall $0 \leq B_b \leq y$

- ▶ $0 \leq B_b \leq y$ soll nur gelten wenn $y = 0$.
- ▶ Es gilt also nicht $0 \leq B_b \leq 543$

Hinweis

- ▶ Im Folgendem verwenden wir oft $(\exists x \leq y)$ auch wenn $(\exists x)$ reichen würde.

Nachweis: Relationen Arithmetisch

- ▶ $x B_b y \leftrightarrow x = y \vee (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_b(w) \wedge (x \cdot w) *_b z = y))$
- ▶ $x E_b y \leftrightarrow x = y \vee (\exists z \leq y)(z *_b x = y)$
- ▶ $x P_b y \leftrightarrow (\exists z \leq y)(z E_b y \wedge x B_b z)$
- ▶ $x_1 *_b x_2 *_b \dots *_b x_n P_b y \leftrightarrow (\exists z \leq y)x_1 *_b \dots *_b x_n = z \wedge z P_b y$

Notation

- ▶ Da wir Basis 13 verwenden, schreiben wir ab sofort B , E , P anstelle von B_b , E_b , P_b .
- ▶ $x_1x_2 \dots x_n$ ist die Kurzschreibweise von $x_1 * x_2 * \dots * x_n$.
- ▶ $x\tilde{P}y$ bedeutet x kommt nicht in y vor (äquivalent zu $\sim xPy$).

Sequenzen (Definitionen)

- ▶ Ein n -Tupel (X_1, \dots, X_n) wird in \mathcal{L}_E mit $\#X_1\#X_2\#\dots\#X_n\#$ bezeichnet.
- ▶ K_{11} Menge aller Ausdrücke ohne δ (Gödelnr. von $\#$).
- ▶ $\delta a_1\delta a_2\delta \dots \delta a_n\delta$ heißt Sequenznummer der Sequenz (a_1, \dots, a_n) .
Wobei $a_i \in K_{11}, i = (1 \dots n)$.

Definitionen (Forts.)

- ▶ $\text{Seq}(x) \leftrightarrow x$ ist eine Sequenznr.
- ▶ $x \in y \leftrightarrow y$ ist eine Sequenznr. von einer Sequenz, die x enthält.
- ▶ $x \prec_z y \leftrightarrow z$ ist eine Sequenznr. von einer Sequenz, so dass x vor y in z vorkommt.

Nachweis: Relationen Arithmetisch

- ▶ $Seq\ x \leftrightarrow \delta Bx \wedge \delta Ex \wedge \delta \neq x \wedge \delta \delta \tilde{P}_x \wedge (\forall y \leq x)(\delta 0y P_x \supset \delta By)$
- ▶ $x \in y \leftrightarrow Seq\ y \wedge \delta x \delta P_y \wedge \delta \tilde{P}_x$
- ▶ $x \prec_z y \leftrightarrow x \in z \wedge y \in z \wedge (\exists w \leq z)(wBz \wedge x \in w \wedge \sim y \in w)$

Noch zwei Abkürzungen

- ▶ $(\forall x \in y)(\text{---})$ ist die Abkürzung für $\forall x(x \in y \supset (\text{---}))$
- ▶ $(\exists x, y \prec_w z)(\text{---})$ ist die Abkürzung für $\exists x \exists y(x \prec_w z \wedge y \prec_w z \wedge (\text{---}))$

Formationssequenzen (Erinnerung)

- ▶ Rekursive Definition für Terme in \mathcal{L}_E
 - ▶ Alle Variablen v_i sind Terme
 - ▶ Alle Zahlen sind Terme
 - ▶ Wenn t_1 und t_2 Terme sind dann sind auch
 - ▶ $(t_1 + t_2)$
 - ▶ $(t_1 \cdot t_2)$
 - ▶ $(t_1 \mathbf{E} t_2)$
 - ▶ t_1'

Terme.

Formationssequenzen (Ziel)

- ▶ Ziel: Ersetzen der rekursiven Definition (für Terme und Formeln) durch explizite

Formationssequenzen ($\mathcal{R}_t(X, Y, Z)$)

- ▶ $\mathcal{R}_t(X, Y, Z) \leftrightarrow Z = (X * Y)$ bzw. $Z = X'$
Wobei $* \in \{+, \cdot, \mathbf{E}\}$
- ▶ Beispiel: $X := (v_1 + 3)$, $Y := v_4$, $Z := (v_1 + 3) \cdot v_4$
Dann ist $\mathcal{R}_t(X, Y, Z)$ wahr

Formationssequenzen (Definition)

- ▶ **Formationssequenz (für Terme)**
Eine *Formationssequenz* ist eine endl. Sequenz (X_1, \dots, X_n) , so dass für alle X_i gilt:
 - ▶ X_i Variable
 - ▶ X_i Zahl
 - ▶ oder es gibt zwei frühere Terme X_j, X_k ($j, k < i$), so dass $\mathcal{R}_t(X_j, X_k, X_i)$ gilt.
- ▶ **Beispiel:** $(v_1, 3, (v_1 + 3), v_4, (v_1 + 3) \cdot v_4)$
ist eine Formationssequenz für den Term $(v_1 + 3) \cdot v_4$

Terme (Redefinition)

- ▶ X ist ein Term \leftrightarrow ex. Formationssequenz, in der X vorkommt.

Formationssequenzen $(\mathcal{R}_f(X, Y, Z))$

- ▶ $\mathcal{R}_f(X, Y, Z) \leftrightarrow$
 - ▶ $Z = \sim X$
 - ▶ $Z = (X \supset Y)$
 - ▶ $Z = \forall v_i X$

Formationssequenzen (Definition)

- ▶ **Formationsssequenz (für Formeln)**

Eine *Formationssequenz* ist eine endl. Sequenz (X_1, \dots, X_n) , so dass für alle X_i gilt:

- ▶ X_i atomare Formel
- ▶ oder es gibt zwei frühere Formeln X_j, X_k ($j, k < i$), so dass $\mathcal{R}_f(X_j, X_k, X_i)$ gilt.

- ▶ **Beispiel:** $((v_i \leq v_i), (v'_i \leq v'_j), ((v_i \leq v_j) \supset (v'_i \leq v'_j)))$
ist eine *Formationssequenz* für die Formel
 $(v_i \leq v_j) \supset (v'_i \leq v'_j)$

Formeln (Redefinition)

- ▶ X ist ein Formel \leftrightarrow ex. Formationssequenz, in der X vorkommt.