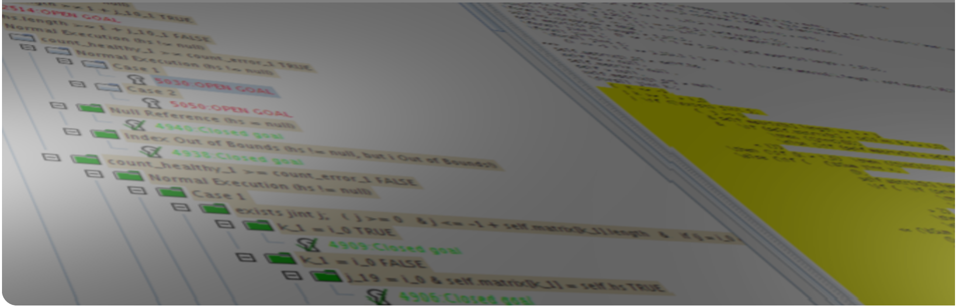
Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2017/2018

Peano-Arithmetik

KIT – Institut für Theoretische Informatik



Guiseppe (Ioseph) Peano

- Geboren 1858 in Spinetta
- Gestorben 1932 in Turin
- Beiträge zur Mathematik und Linguistik
- Eine zentrale Publikation:
  Arithmetices principia: nova methodo exposita
  erschienen 1889 im Verlag Augustae Taurinorum
  online Version `http://www.archive.org/stream/arithmeticespri00peangoog#page/n6/mode/2up`

Signatur Σ_{PA}

- Konstantensymbole $0, 1$ für *Null* und *Eins*
- zweistelliges Funktionszeichen für $+$ für Addition
- zweistelliges Funktionszeichen für $*$ für Multiplikation

Die Peano Axiome *PA* (prädikatenlogische Version)

1. $\forall x(x + 1 \not\doteq 0)$
2. $\forall x \forall y(x + 1 \doteq y + 1 \rightarrow x \doteq y)$
3. $\forall x(x + 0 \doteq x)$
4. $\forall x \forall y(x + (y + 1) \doteq (x + y) + 1)$
5. $\forall x(x * 0 \doteq 0)$
6. $\forall x \forall y(x * (y + 1) \doteq (x * y) + x)$
7. Für jede Σ_{PA}-Formel ϕ
   $\forall \bar{z}((\phi(0) \land \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x(\phi))$

Induktionsaxiom

Axiom 7 ist ein Axiomenschema.

Beispiel

Für die Formel $\phi = x + z \doteq z + x$ ergibt sich die Instanziierung des Induktionsschemas:

$$
\begin{array}{l}
\forall z(\\
0 + z \doteq z + 0 \wedge \\
\forall x(x + z \doteq z + x \rightarrow (x + 1) + z \doteq z + (x + 1)) \\
\rightarrow \forall x(x + z \doteq z + x))
\end{array}
$$

- Induktionsvariable x
- Parameter z
- Induktionsanfang $x = 0$
- Induktionsschritt $x \rightsquigarrow x + 1$

Erste Folgerungen aus *PA*

Die folgenden beiden Formeln sind aus *PA* ableitbar:

1. $\forall w(w + 0 \doteq 0 + w)$
2. $0 \neq 1$

Folgerung von 2. aus 1.

	Aus Axiom 3 $\forall x(x + 0 \doteq x)$	
1	folgt für $x \rightsquigarrow 1$	$1 + 0 \doteq 1$
2	Teil 1 mit $w \rightsquigarrow 1$	$0 + 1 \doteq 1$
	Axiom 1 $\forall x(x + 1 \not\doteq 0)$	
3	mit $x \rightsquigarrow 0$	$0 + 1 \neq 0$
4	aus 2 und 3 folgt	$1 \neq 0$

Ein erster Induktionsbeweis

$PA \vdash \forall w(w + 0 \doteq 0 + w)$

Induktionsanfang

$$0 + 0 \doteq 0 + 0 \quad \text{Gleichheitsaxiom der Logik}$$

Induktionsschritt

$$\begin{array}{rcll}
(w+1)+0 & \doteq & w+1 & \text{Axiom 3 von links nach rechts} \\
 & & & \text{mit } x \rightsquigarrow (w+1) \\
 & \doteq & (w+0)+1 & \text{Axiom 3 von rechts nach links} \\
 & & & \text{mit } x \rightsquigarrow w \\
 & \doteq & (0+w)+1 & \text{Induktionsvoraussetzung} \\
 & \doteq & 0+(w+1) & \text{Axiom 4 von rechts nach links} \\
 & & & \text{mit } x \rightsquigarrow 0, y \rightsquigarrow w
\end{array}$$

Assoziativität der Addition

$PA \vdash \forall u \forall v \forall w((u+v)+w \doteq u+(v+w))$

Induktion nach w Induktionsanfang: $(u+v)+0 \doteq u+(v+0)$

$$
\begin{array}{lcll}
(u+v)+0 & \doteq & u+v & \text{Ax 3} \\
 & & & x \rightsquigarrow (u+v) \\
v+0 & \doteq & v & \text{Ax 3} \\
 & & & x \rightsquigarrow v
\end{array}
$$

Induktionshypothese $(u+v)+w \doteq u+(v+w)$
Induktionsbehauptung $(u+v)+(w+1) \doteq u+(v+(w+1))$

$$
\begin{array}{lcll}
(u+v)+(w+1) & \doteq & ((u+v)+w)+1 & \text{Ax 4} \\
 & & & x,y \rightsquigarrow (u+v), w \\
 & \doteq & (u+(v+w))+1 & \text{IndHyp} \\
 & \doteq & (u+((v+w)+1) & \text{Ax 4} \\
 & & & x,y \rightsquigarrow u, v+w
\end{array}
$$

Vollständigkeit von *PA*?

Kann man alle wahren Aussagen über die Struktur $\mathcal{N} = \langle \mathbb{N}, +, *, 0, 1 \rangle$ aus den Axiomen *PA* herleiten?

Notation:

$$\begin{array}{rcl} Th(\mathcal{N}) & = & \{\phi \in Fml_{\Sigma_{PA}} \mid \mathcal{N} \models \phi\} \\ Cn(PA) & = & \{\phi \in Fml_{\Sigma_{PA}} \mid PA \vdash \phi\} \end{array}$$

Fakten:

1. $Cn(PA) \subseteq Th(\mathcal{N})$
2. $Cn(PA)$ ist rekursiv aufzählbar

Frage: $Cn(PA) = Th(\mathcal{N})$

Anwort: Nein. Denn:
$Th(\mathcal{N})$ ist nicht rekursiv aufzählbar (nicht axiomatisierbar)
1. Gödelscher Unvollständigkeitssatz

Unentscheidbarkeit

Bemerkung

Für alle $\phi \in \mathit{Fml}_{\Sigma_{PA}}$ gilt:

$$\phi \in \mathit{Th}(\mathcal{N}) \text{ oder } \neg\phi \in \mathit{Th}(\mathcal{N})$$

Darum:
Wäre $\mathit{Th}(\langle \mathbb{N}, +, *, 0, 1 \rangle)$ rekursiv aufzählbar,
dann wäre $\mathit{Th}(\langle \mathbb{N}, +, *, 0, 1 \rangle)$ auch entscheidbar.

Presburger Arithmetik

$\mathit{Th}(\langle \mathbb{N}, +, 0, 1 \rangle)$ (ohne Multiplikation)
ist rekursiv aufzählbar und entscheidbar

Nichtaxiomatisierbarkeit von $Th(\mathcal{N})$

$$Cn(PA) \subsetneq Th(\mathcal{N})$$

Bedeutung der Lücke zwischen $Cn(PA)$ und $Th(\mathcal{N})$ für die Praxis? **Gering!**

- Wenig relevante/verständliche Beispiele für ϕ mit

  $$\phi \in Th(\mathcal{N}) \text{ und } \phi \notin Cn(PA)$$

- Nichtstandardmodelle von *PA* sind alle „seltsam“ (Modelle, die nicht isomorph zu $\mathcal{N}$ sind)

  Satz von Tennenbaum:
  In allen Nichtstandardmodellen von PA sind Addition und Multiplikation nicht-berechenbare Funktionen.