Script generated by TTT

Title: Nipkow: Theo (22.07.2019)

Date: Mon Jul 22 14:13:42 CEST 2019

Duration: 71:54 min

Pages: 43

7. Automaten, Berechenbarkeit, und Logik

7.1 Die Unvollständigkeit der Arithmetik

Kurt Gödel. *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.* 1931.

7.1 Die Unvollständigkeit der Arithmetik

Kurt Gödel. *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.* 1931.

Kurt Gödel
1906 (Brünn) –
1978 (Princeton)

Syntax der Arithmetik:

Variablen:	V	$\to$	$x \mid y \mid z \mid \ldots$
Zahlen:	N	$\to$	$0 \mid 1 \mid 2 \mid \ldots$

Syntax der Arithmetik:

Variablen:	V	$\to$	$x \mid y \mid z \mid \ldots$
Zahlen:	N	$\to$	$0 \mid 1 \mid 2 \mid \ldots$
Terme:	T	$\to$	$V \mid N \mid (T + T) \mid (T * T)$
Formeln:	F	$\to$	$(T = T) \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid \exists V.\, F$

Syntax der Arithmetik:

Variablen:	V	$\to$	$x \mid y \mid z \mid \ldots$
Zahlen:	N	$\to$	$0 \mid 1 \mid 2 \mid \ldots$
Terme:	T	$\to$	$V \mid N \mid (T + T) \mid (T * T)$
Formeln:	F	$\to$	$(T = T) \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid \exists V.\, F$

Wir betrachten $\forall x.\, F$ als Abk. für $\neg\exists x.\, \neg F$.

Syntax der Arithmetik:

$$\begin{array}{rlcl} \text{Variablen:} & V & \to & x \mid y \mid z \mid \ldots \\ \text{Zahlen:} & N & \to & 0 \mid 1 \mid 2 \mid \ldots \\ \text{Terme:} & T & \to & V \mid N \mid (T + T) \mid (T * T) \\ \text{Formeln:} & F & \to & (T = T) \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid \exists V.\, F \end{array}$$

Wir betrachten $\forall x.\, F$ als Abk. für $\neg\exists x.\, \neg F$.

Definition 7.1

Ein Vorkommen einer Variablen x in einer Formel F ist gebunden gdw das Vorkommen in einer Teilformel der Form $\exists x.\, F'$ in der Teilformel F' liegt.
Ein Vorkommen ist frei gdw es nicht gebunden ist.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 7.2

$$F(x, y) \quad = \quad (x = y \;\wedge\; \exists x.\, x = y)$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 7.2

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 7.2

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Ein Satz ist eine Formel ohne freie Variablen.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 7.2

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Ein Satz ist eine Formel ohne freie Variablen.

Beispiel 7.3

$$\exists x.\, \exists y.\, x = y \qquad \exists y.\, \exists x.\, x = y$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k \in \mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 7.2

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Ein Satz ist eine Formel ohne freie Variablen.

Beispiel 7.3

$$\exists x.\, \exists y.\, x = y \qquad \exists y.\, \exists x.\, x = y$$

Mit S bezeichnen wir die Menge der arithmetischen Sätze.

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$ gdw t_1 und t_2 den selben Wert haben.

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$ gdw t_1 und t_2 den selben Wert haben.

$\neg F \in W$ gdw $F \notin W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$ gdw t_1 und t_2 den selben Wert haben.

$\neg F \in W$ gdw $F \notin W$

$(F \wedge G) \in W$ gdw $F \in W$ und $G \in W$

$(F \vee G) \in W$ gdw $F \in W$ oder $G \in W$

$\exists x.\, F(x) \in W$ gdw es $n \in \mathbb{N}$ gibt, so dass $F(n) \in W$

Fakt 7.5

Für jeden Satz F gilt entweder $F \in W$ oder $\neg F \in W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$ gdw t_1 und t_2 den selben Wert haben.

$\neg F \in W$ gdw $F \notin W$ ✗

$(F \wedge G) \in W$ gdw $F \in W$ und $G \in W$

$(F \vee G) \in W$ gdw $F \in W$ oder $G \in W$

$\exists x.\, F(x) \in W$ gdw es $n \in \mathbb{N}$ gibt, so dass $F(n) \in W$

Fakt 7.5

Für jeden Satz F gilt entweder $F \in W$ oder $\neg F \in W$

$\neg F \in W$ ✓

1. $F \notin W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F \in W$	gdw	$F \notin W$
$(F \wedge G) \in W$	gdw	$F \in W$ und $G \in W$
$(F \vee G) \in W$	gdw	$F \in W$ oder $G \in W$
$\exists x.\, F(x) \in W$	gdw	es $n \in \mathbb{N}$ gibt, so dass $F(n) \in W$

Fakt 7.5

Für jeden Satz F gilt entweder $F \in W$ oder $\neg F \in W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F \in W$	gdw	$F \notin W$
$(F \wedge G) \in W$	gdw	$F \in W$ und $G \in W$
$(F \vee G) \in W$	gdw	$F \in W$ oder $G \in W$
$\exists x.\, F(x) \in W$	gdw	es $n \in \mathbb{N}$ gibt, so dass $F(n) \in W$

Fakt 7.5

Für jeden Satz F gilt entweder $F \in W$ oder $\neg F \in W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

$$\exists x.\, x + x = y$$

Daher haben wir Wahrheit nur für Sätze definiert.

Formeln können Rel. repr.

$\exists z.\ x + y + z + 1 =: \phi(x, y)$

repr die Rel $x > y$

Formeln können Fkt. repr.:

$\exists r.\ (r < x_2 \wedge x_1 = y * x_2 + r) = \psi(x_1, x_2, y)$

repr $y = x_1 \text{ DIV } x_2$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 7.4

$(t_1 = t_2) \in W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F \in W$	gdw	$F \notin W$
$(F \wedge G) \in W$	gdw	$F \in W$ und $G \in W$
$(F \vee G) \in W$	gdw	$F \in W$ oder $G \in W$
$\exists x.\, F(x) \in W$	gdw	es $n \in \mathbb{N}$ gibt, so dass $F(n) \in W$

Fakt 7.5

Für jeden Satz F gilt entweder $F \in W$ oder $\neg F \in W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

$$\exists x.\, x + x = y$$

Daher haben wir Wahrheit nur für Sätze definiert.

Definition 7.6

Eine partielle Funktion $f : \mathbb{N}^k \to \mathbb{N}$ ist arithmetisch repräsentierbar gdw es eine Formel $F(x_1, \ldots, x_k, y)$ gibt, so dass für alle $n_1, \ldots, n_k, m \in \mathbb{N}$ gilt:

$$f(n_1, \ldots, n_k) = m \quad \text{gdw} \quad F(n_1, \ldots, n_k, m) \in W$$

Satz 7.7

Jede WHILE-berechenbare Funktion ist arithmetisch repräsentierbar.

Formeln können Rel. repr.

$\exists z.\ x = y + z + 1 =: \phi(x, y)$

repr die Rel $x > y$

Formeln können Fkt. repr.:

$\exists r.\ (r < x_2 \wedge x_1 = y * x_2 + r) = \psi(x_1, x_2, y)$

repr $y = x_1 \text{ DIV } x_2$

WHILE-program $P(x_0, \ldots, x_k) \mapsto F_P(x_0, \ldots, x_k, y_0, \ldots, y_k)$

so daß für alle $n_0, \ldots, n_k \in \mathbb{N}$, $m_0, \ldots, m_k \in \mathbb{N}$

$P(n_0, \ldots, n_k)$ term mit $x_0 = m_0, x_1 = m_1, \ldots$

$\iff F_P(m_0, \ldots, m_k, n_0, \ldots, n_k) \in W$ (*)

Bew. mit Ind. über P

$P = (x_i := x_j + n) \mapsto F_P(\bar{x}_k, \bar{y}_k) =$

$(y_i = x_j + n \wedge \bigwedge_{r \neq i} y_r = x_r)$

$P = Q; R \mapsto F_P(\bar{x}_k, \bar{y}_k) =$

$(\exists \bar{z}_k.\ F_Q(\bar{x}_k, \bar{z}_k) \wedge F_R(\bar{z}_k, \bar{y}_k))$

$P =$ WHILE $x_i \neq 0$ DO $Q \mapsto F_P(\bar{x}_k, \bar{y}_k) =$

$\exists t.\ \exists \bar{x}^0, \ldots, \bar{x}^t.$

$\bar{x}^0_k = \bar{x}_k \wedge x_i^t = 0 \wedge \bar{x}^t_k = \bar{y}_k \wedge$

$\forall j < t.\ x_i^j \neq 0 \wedge F_Q(\underbrace{x_0^j, \ldots, x_k^j}, \underbrace{x_0^{j+1}, \ldots, x_k^{j+1}})$

Definition 7.6

Eine partielle Funktion $f : \mathbb{N}^k \to \mathbb{N}$ ist arithmetisch repräsentierbar gdw es eine Formel $F(x_1, \ldots, x_k, y)$ gibt, so dass für alle $n_1, \ldots, n_k, m \in \mathbb{N}$ gilt:

$$f(n_1, \ldots, n_k) = m \quad \text{gdw} \quad F(n_1, \ldots, n_k, m) \in W$$

Satz 7.7

Jede WHILE-berechenbare Funktion ist arithmetisch repräsentierbar.

Stattdessen: Kodiere $x_r^0, \ldots, x_r^t$ in zwei Zahlen a_r, b_r

Details in Schöning

Satz 7.8

W ist nicht entscheidbar.

$P = \text{WHILE } x_i \neq 0 \text{ DO } Q \mapsto F_P(\bar{x}_u, \bar{y}_u) =$

$\exists t.\ \exists x_0^0, \ldots, x_0^t, \ldots, x_u^0, \ldots, x_u^t.$

$\bar{x}_u^0 = \bar{x}_u \wedge x_i^t = 0 \wedge \bar{x}_u^t = \bar{y}_u \wedge$

$\forall j < t.\ x_i^j \neq 0 \wedge F_Q(x_0^j, \ldots, x_u^j, x_0^{j+1}, \ldots, x_u^{j+1})$

Stattdessen: Kodiere $x_r^0, \ldots, x_r^t$ in zwei Zahlen a_r, b_r

Details in Schöning

Satz 7.8

W ist nicht entscheidbar.

Sei $U \subseteq \mathbb{N}$ semi-entsch., aber unentscheidbar

$\Rightarrow \chi'_U$ ist WHILE ber.

$\Rightarrow \chi'_U$ ist arith. repr. durch $F(x,y)$

$\Rightarrow [n \in U \Leftrightarrow \chi'_U(n) = 1 \Leftrightarrow F(n,1) \in W]$

$\Rightarrow U \leq W \Rightarrow W$ unentscheidbar

Anforderung an ein Beweissystem:

Wäre W s-e, dann wäre W auch ent.:

F: berechne $\chi'_W(F)$ und $\chi'_W(\neg F)$ parallel

Fakt: $F \in W$ oder $\neg F \in W$

Anforderung an ein Beweissystem:
Es muss entscheidbar sein, ob ein gegebener Text ein Beweis einer gegebenen Formel ist.

Anforderung an ein Beweissystem:
Es muss entscheidbar sein, ob ein gegebener Text ein Beweis einer gegebenen Formel ist.

Wir kodieren Beweise als Zahlen.

Anforderung an ein Beweissystem:
Es muss entscheidbar sein, ob ein gegebener Text ein Beweis einer gegebenen Formel ist.

Wir kodieren Beweise als Zahlen.

Definition 7.10
Ein Beweissystem für die Arithmetik ist ein entscheidbares Prädikat

$$Bew : \mathbb{N} \times \text{Satz} \rightarrow \{0, 1\}$$

wobei wir $Bew(b, F)$ lesen als „b ist Beweis für Formel F".

Anforderung an ein Beweissystem:
Es muss entscheidbar sein, ob ein gegebener Text ein Beweis einer gegebenen Formel ist.

Wir kodieren Beweise als Zahlen.

Definition 7.10
Ein Beweissystem für die Arithmetik ist ein entscheidbares Prädikat

$$Bew : \mathbb{N} \times \text{Satz} \rightarrow \{0, 1\}$$

wobei wir $Bew(b, F)$ lesen als „b ist Beweis für Formel F".
Ein Beweissystem Bew ist korrekt gdw

$$Bew(b, F) \implies F \in W.$$

Ein Beweissystem Bew ist vollständig gdw

$$F \in W \implies \text{es gibt } b \text{ mit } Bew(b, F).$$

Satz 7.11 (Gödel)

Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.

Satz 7.11 (Gödel)

Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.

Beweis:

Denn mit jedem korrekten und vollständigen Beweissystem kann man $\chi'_W(F)$ programmieren:

Satz 7.11 (Gödel)

Es gibt kein korrektes und vollständigen Beweissystem für die Arithmetik.

Beweis:

Denn mit jedem korrekten und vollständigen Beweissystem kann man $\chi'_W(F)$ programmieren:

$b := 0$
while $Bew(b, F) = 0$ **do** $b := b + 1$
output(1)

□

7.2 Die Entscheidbarkeit der Presburger Arithmetik

Satz 7.11 (Gödel)

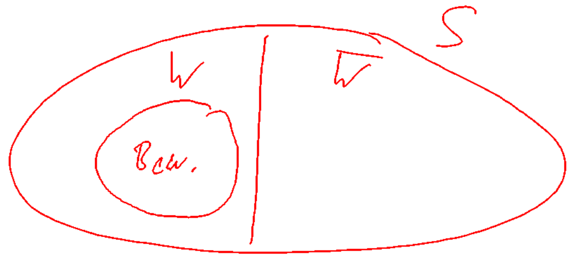
Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.

Beweis:

Denn mit jedem korrekten und vollständigen Beweissystem kann man $\chi'_W(F)$ programmieren:

Satz 7.11 (Gödel)

Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.



7.2 Die Entscheidbarkeit der Presburger Arithmetik

7.2 Die Entscheidbarkeit der Presburger Arithmetik

Sei $U \subseteq \mathbb{N}$ semi-entsch., aber unentscheidbar

$\Rightarrow \chi'_U$ ist WHILE ber.

$\Rightarrow \chi'_U$ ist arith. repr. durch $F(x,y)$

$\Rightarrow [n \in U \Leftrightarrow \chi'_U(n) = 1 \Leftrightarrow F(n,1) \in W]$

$\Rightarrow U \leq W \Rightarrow W$ unentscheidbar