Das zehnte Hilbertsche Problem und die Gödelschen Sätze

Peter Koepke, Mathematisches Institut, Universität Bonn

Cusanuswerk, Fachschaftstagung Mathematik-Informatik, Uder, 1.-4. Mai 2008

Mathematische Probleme

Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900

Von David Hilbert

Wer von uns würde nicht gern den Schleier lüften, unter dem die Zukunft verborgen liegt, um einen Blick zu werfen auf die bevorstehenden Fortschritte unsrer Wissenschaft und in die Geheimnisse ihrer Entwickelung während der künftigen Jahrhunderte! Welche besonderen Ziele werden es sein, denen die führenden mathematischen Geister der kommenden Geschlechter nachstreben? welche neuen Methoden und neuen Thatsachen werden die neuen Jahrhunderte entdecken - auf dem weiten und reichen Felde mathematischen Denkens?

Die Geschichte lehrt die Stetigkeit der Entwickelung der Wissenschaft. Wir wissen, daß jedes Zeitalter eigene Probleme hat, die das kommende Zeitalter löst oder als unfruchtbar zur Seite schiebt und durch neue Probleme ersetzt. Wollen wir eine Vorstellung gewinnen von der muthmaßlichen Entwickelung mathematischen Wissens in der nächsten Zukunft, so müssen wir die offenen Fragen vor unserem Geiste passiren lassen und die Probleme überschauen, welche die gegenwärtige Wissenschaft stellt, und deren Lösung wir von der Zukunft erwarten. Zu einer solchen Musterung der Probleme scheint mir der heutige Tag, der an der Jahrhundertwende liegt, wohl geeignet; denn die großen Zeitabschnitte fordern uns nicht blos auf zu Rückblicken in die Vergangenheit, sondern sie lenken unsere Gedanken auch auf das unbekannte Bevorstehende.

Die hohe Bedeutung bestimmter Probleme für den Fortschritt der mathematischen Wissenschaft im Allgemeinen und die wichtige Rolle, die sie bei der Arbeit des einzelnen Forschers spielen, ist unleugbar. Solange ein Wissenszweig Ueberfluß an Problemen bietet, ist er lebenskräftig; Mangel an Problemen bedeutet Absterben oder Aufhören der selbstständigen Entwickelung. Wie überhaupt jedes menschliche Unternehmen Ziele verfolgt, so braucht die mathematische Forschung Probleme. Durch die Lösung, von Problemen stählt sich die Kraft des Forschers; er findet neue Methoden und Ausblicke, er gewinnt einen weiteren und freieren Horizont.

...

Unermeßlich ist die Fülle von Problemen in der Mathematik, und sobald ein Problem gelöst ist, tauchen an dessen Stelle zahllose neue Probleme auf. Gestatten Sie mir im Folgenden, gleichsam zur Probe, aus verschiedenen mathematischen Disciplinen einzelne bestimmte Probleme zu nennen, von deren Behandlung eine Förderung der Wissenschaft sich erwarten läßt.

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Eine diophantische Gleichung ist von der Form

$$P(x_1, ..., x_k) = 0$$

wobei P ein Polynom in den Variablen $x_1, ..., x_k$ bezeichnet, das nur ganzzahlige Koeffizienten besitzt.

Martin Davis, Yuri Matiyasevich, Hilary Putnam, Julia Robinson

Es gibt kein Entscheidungsverfahren für die Lösbarkeit diophantischer Gleichungen (1970)

- Mathematische Logik: Lehre von allgemeiner mathematischer Formalisierbarkeit, Beweisbarkeit, Berechenbarkeit

- Allgemeine Formalisierung von Entscheidungsverfahren durch Turingmaschinen

- Halteproblem für Turingmaschinen: es gibt Turing-aufzählbare Mengen natürlicher Zahlen, die nicht Turing-entscheidbar sind

- Turing-aufzählbare Mengen $A \subseteq \mathbb{N}$ lassen sich durch diophantische Gleichungen $P = 0$ darstellen als

$$A = \{n \in \mathbb{N} | \text{ es gibt } x_2, ..., x_k \text{ mit } P(n, x_2, ..., x_k) = 0\}$$

- Kodierung von logischen Eigenschaften durch diophantische Gleichungen

- Also gibt es kein allgemeines Entscheidungsverfahren für die Lösbarkeit diophantischer Gleichungen

Gliederung der Vorträge

1. Logik mit exponentiell diophantischen Gleichungen

2. Kodierung von Turing-Maschinen mit exponentiell diophantischen Gleichungen

3. Exponentiell diophantische Mengen sind diophantische Mengen

4. Anwendungen

5. Die Gödelschen Sätze

Literatur

1900: David Hilbert, Mathematische Probleme. Nachgedruckt in David Hilbert, *Gesammelte Abhandlungen*, Springer-Verlag, 1935, 290-329.

1950: Martin Davis, Arithmetical problems and recursively enumerable predicates (abstract). *Journal of Symbolic Logic* 15, 77-78

1953: Martin Davis, Arithmetical problems and recursively enumerable predicates. *Journal of Symbolic Logic* 18, 33-41

1958: Martin Davis und Hilary Putnam, Reductions of Hilbert's tenth problem. *Journal of Symbolic Logic* 23, 183-187

1960: Julia Robinson, The undecidability of exponential Diophantine equations. *Notices of the American Mathematical Society* 7, 75

1962: Julia Robinson, The undecidability of exponential Diophantine equations. In *Logic, Methodology and Philosophy of Science: Proceedings of the 1960 International Congress*, Stanford University Press, 12-13.

1970: Yuri Matiyasevich, Enumerable sets are Diophantine (Übersetzung). *Soviet Mathematics. Doklady* 11, 354-358

1993: Yuri Matiyasevich, *Hilbert's Tenth Problem* (Übersetzung), The MIT Press

1997: Heiko Goeman, Diplomarbeit Bonn

1. Logik mit exponentiell diophantischen Gleichungen

Natürliche Zahlen

$\mathbb{N} = \{0, 1, 2, \ldots\}$

Außer als Kardinal- und Ordinalzahlen können die natürlichen Zahlen auch zur Kodierung von Informationen benutzt werden:

20080501 kann als 1. Mai 2008 gelesen werden; Zahlen in Stellenzahldarstellung (binär/dezimal), Folgen von Bits/Symbolen.

Zur Verarbeitung von Folgen von Bits/Symbolen werden Operationen wie aussagenlogische Verknüpfungen (und, oder, nicht) verwendet.

Kann man solche Verarbeitungen auch mit den arithmetischen Operationen $+$ und $\times$ durchführen?

Diophantische Gleichungen

- Polynome
  - Jede Variable x und jede ganze Zahl $z \in \mathbb{Z}$ is ein Polynom
  - Sind P und Q Polynome, so auch $P+Q$ und $P \cdot Q$
- Eine diophantische Gleichung ist eine Gleichung der Form $P=0$
- $P=0$ ist lösbar, wenn es natürliche Werte der Variablen gibt, für die $P=0$ ist
- $R \subseteq \mathbb{N}^n$ ist *diophantisch*, wenn es ein Polynom $P_R(x_1, ..., x_m, a_1, ..., a_n)$ gibt mit

$$R = \{(a_1, ..., a_n) \in \mathbb{N}^n | \text{ es gibt } x_1, ..., x_m \in \mathbb{N} \text{ mit } P_R(x_1, ..., x_m, a_1, ..., a_m) = 0\}$$

$$[R = \{(a_1, ..., a_n) \in \mathbb{N}^n | \exists x_1, ..., x_m \in \mathbb{N}\colon P_R(x_1, ..., x_m, a_1, ..., a_m) = 0\}]$$

Exponentiell diophantische Gleichungen

- exponentielle Polynome
  - Jede Variable x und jede ganze Zahl $z \in \mathbb{Z}$ is ein exponentielles Polynom
  - Ist n eine natürliche Zahl, und sind x, y Variablen, so sind n^y und x^y exponentielle Polynome
  - Sind P und Q exponentielle Polynome, so auch $P+Q$ und $P \cdot Q$
- Eine exponentiell diophantische Gleichung ist eine Gleichung der Form $P=0$
- $R \subseteq \mathbb{N}^n$ ist *exponentiell diophantisch*, wenn es ein exponentielles Polynom $P_R(x_1,...,x_m,a_1,...,a_m)$ gibt mit

$$R=\{(a_1,...,a_n)\in\mathbb{N}^n|\text{ es gibt } x_1,...,x_m\in\mathbb{N} \text{ mit } P_R(x_1,...,x_m,a_1,...,a_m)=0\}$$

$$[R=\{(a_1,...,a_n)\in\mathbb{N}^n|\exists x_1,...,x_m\in\mathbb{N}\colon P_R(x_1,...,x_m,a_1,...,a_m)=0\}]$$

Exponentiell diophantische Mengen (e.d. Mengen)

– Die Vereinigung e.d. Mengen ist eine e.d. Menge:

$$
\begin{aligned}
& \vec{a} \in \{\vec{a} \,|\exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0\} \cup \{\vec{a} \,|\exists \vec{x}\, Q(\vec{x}\,,\vec{a}\,)=0\} \\
\leftrightarrow\ & \vec{a} \in \{\vec{a} \,|\exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0\} \cup \{\vec{a} \,|\exists \vec{y}\, Q(\vec{y}\,,\vec{a}\,)=0\} \\
\leftrightarrow\ & \exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0 \text{ oder } \exists \vec{y} Q(\vec{y}\,,\vec{a}\,)=0 \\
\leftrightarrow\ & \exists \vec{x}\,, \vec{y}\,(\, P(\vec{x}\,,\vec{a}\,)=0 \text{ oder } \ Q(\vec{y}\,,\vec{a}\,)=0) \\
\leftrightarrow\ & \exists \vec{x}\,, \vec{y}\,(\, P(\vec{x}\,,\vec{a}\,) \cdot Q(\vec{y}\,,\vec{a}\,)=0)
\end{aligned}
$$

– Der Durchschnitt e.d. Mengen ist eine e.d. Menge:

$$
\begin{aligned}
& \vec{a} \in \{\vec{a} \,|\exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0\} \cap \{\vec{a} \,|\exists \vec{x}\, Q(\vec{x}\,,\vec{a}\,)=0\} \\
\leftrightarrow\ & \vec{a} \in \{\vec{a} \,|\exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0\} \cap \{\vec{a} \,|\exists \vec{y}\, Q(\vec{y}\,,\vec{a}\,)=0\} \\
\leftrightarrow\ & \exists \vec{x}\, P(\vec{x}\,,\vec{a}\,)=0 \text{ und } \exists \vec{y} Q(\vec{y}\,,\vec{a}\,)=0 \\
\leftrightarrow\ & \exists \vec{x}\,, \vec{y}\,(\, P(\vec{x}\,,\vec{a}\,)=0 \text{ und } \ Q(\vec{y}\,,\vec{a}\,)=0) \\
\leftrightarrow\ & \exists \vec{x}\,, \vec{y}\,(\, P^2(\vec{x}\,,\vec{a}\,) + Q^2(\vec{y}\,,\vec{a}\,)=0)
\end{aligned}
$$

– Eine Projektion einer e.d. Menge ist eine e.d. Menge:

$$\begin{aligned} & \{\vec{a}\,|\exists\vec{b}\;(\vec{a}\,,\vec{b}\,)\in\{(\vec{a}\,,\vec{b}\,)|\exists\vec{x}\,P(\vec{x}\,,\vec{a}\,,\vec{b}\,)=0\}\} \\ = \;& \{\vec{a}\,|\exists\vec{b}\,\exists\vec{x}\,P(\vec{x}\,,\vec{a}\,,\vec{b}\,)=0\} \end{aligned}$$

– Die Komposition e.d. Mengen (Funktionen) ist e.d.:

$$\begin{aligned} & (\vec{a}\,,b)\in R\circ S \\ \leftrightarrow\; & \exists c((\vec{a}\,,c)\in S \text{ und } (c,b)\in R) \end{aligned}$$

– Ist das Komplement einer e.d. Menge e.d.? I.a. Nein! Folgt aus dem Satz von Davis, Matiyasevich, Putnam, Robinson.

Beispiele exponentiell diophantischer Relationen

- $x = y \leftrightarrow x - y = 0$
- $x \geqslant y \leftrightarrow \exists z\colon x - y - z = 0$
- $x > y \leftrightarrow \exists z\colon x - y - z - 1 = 0$
- $z = x + y \leftrightarrow x + y - z = 0$
- $z = x - y \leftrightarrow x - y - z = 0$
- $z = x \cdot y \leftrightarrow x \cdot y - z = 0$
- $z = x/y \leftrightarrow \exists r\colon r < y \wedge x - yz - r = 0$
- $r = \mathrm{Mod}(x, y) \leftrightarrow \exists z\colon r < y \wedge x - yz - r = 0$
- $x \,|\, y \leftrightarrow \exists z\colon y - x\,z = 0$
- x ist ungerade $\leftrightarrow \exists y\colon x = 2y + 1$

Der Binomialkoeffizient ist exponentiell diophantisch

$$(u+1)^n = \sum_{j=0}^{n} \binom{n}{j} u^j$$

$\binom{n}{j} \leqslant (1+1)^j = 2^j$, und damit ist für $u = 2^n + 1$, $\binom{n}{j}$ die j-te Ziffer von $(u+1)^n$ in der Darstellung zur Basis u. Also

$$y = \binom{n}{k} \Longleftrightarrow \exists u, x, z \colon u = 2^n + 1 \wedge (u+1)^n = x u^{k+1} + y u^k + z \wedge y < u \wedge z < u^k$$

Die binäre Dominanz ist exponentiell diophantisch

Für binär dargestellte Zahlen

$$r = \sum_{i=0}^{n} r_i \, 2^i \text{ und } s = \sum_{i=0}^{n} s_i \, 2^i$$

definiere die binäre Dominanz

$$r \preceq s \leftrightarrow \forall i \colon r_i \leqslant s_i$$

Simulation von Kopfbewegungen auf einem Turing-Band:

$s =$	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
$r =$	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1

Lemma 1. $r+1 \preceq s+1 \Leftrightarrow (r \preceq s \wedge r+1 \not\preceq s) \vee (r \not\preceq s \wedge r+1 \preceq s)$

Satz 2. *$m \preceq s \iff \exists k\colon k = \binom{s}{m} \wedge k$ is ungerade. Also ist $\preceq$ exponentiell diophantisch.*

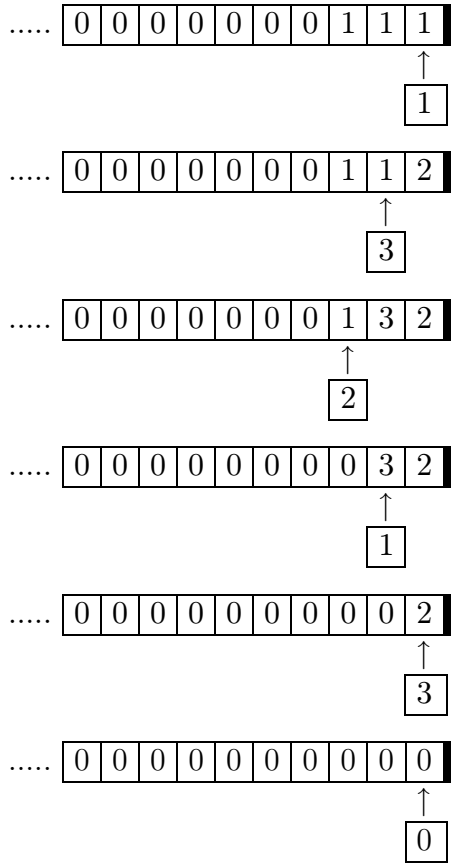
Beweis. Induktion über s.

$s = 0$: Dann ist $m = 0$, und $m \preceq s$ und $\binom{0}{0} = 1$.

$s+1 > 0$: $0 \preceq s+1$ und $\binom{s+1}{0} = 1$. Sei also $m = r+1$. Dann

$$
\begin{aligned}
& r+1 \preceq s+1 \\
\iff\ & (r \preceq s \wedge r+1 \not\preceq s) \vee (r \not\preceq s \wedge r+1 \preceq s) \\
\iff\ & [\tbinom{s}{r} \text{ ungerade } \wedge \tbinom{s}{r+1} \text{ gerade}] \vee [\tbinom{s}{r} \text{ gerade } \wedge \tbinom{s}{r+1} \text{ ungerade}] \\
\iff\ & \tbinom{s}{r} + \tbinom{s}{r+1} \text{ ungerade} \\
\iff\ & \tbinom{s+1}{r+1} \text{ ungerade}
\end{aligned}
$$

□



$\delta(1,1) = (3,2,-1)$

$\delta(3,1) = (2,3,-1)$

$\delta(2,1) = (1,0,1)$

$\delta(1,3) = (3,0,1)$

$\delta(3,2) = (0,0,0)$

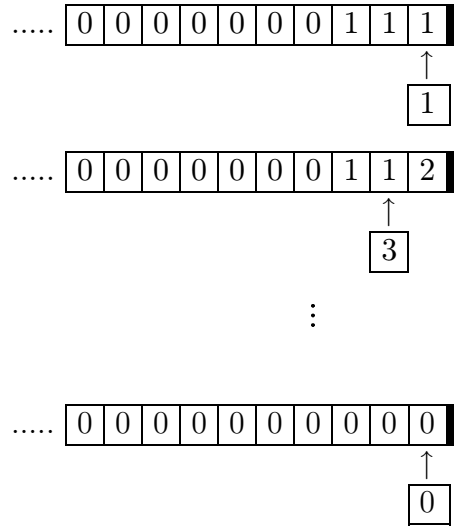
STOP: die Eingabe 3=1 1 1 ist akzeptiert

- Unendliches, nach rechts beschränktes Turing-Band
- Zustände $0, 1, ..., m$, Startzustand 1, Stopzustand 0
- Bandsymbole $0, 1, ..., l$, Leerzeichen 0, Eingabesymbol 1
- Eingabe der natürlichen Zahl n in der Form $\underbrace{1\,1\,1 \ldots 1}_{n}$
- Turing-Programm ist eine endliche Funktion

$$\delta\colon \text{Zustände} \times \text{Symbole} \longrightarrow \text{Zustände} \times \text{Symbole} \times \{-1, 0, +1\}$$

- $-1 \approx$ Kopf links, $0 \approx$ Kopf bewegt sich nicht, $+1 \approx$ Kopf rechts
- Akzeptanzbedingung: Stopzustand 0 und leerer Bandinhalt

Kodierung von Berechnungen



$\delta(1,1) = (3,2,-1)$

$\delta(3,1) = (2,3,-1)$

STOP: die Eingabe 3=1 1 1 ist akzeptiert

wird durch die Bandfolge T und die Zustands-Positionsfolge SP kodiert:

0	0	0	0	0	0	0	0	0	2	0	0	0	3	2	0	0	1	3	2	0	0	1	1	2	0	0	1	1	1

0	0	0	0	0	0	0	0	0	3	0	0	0	1	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	1

Kodierung durch natürliche Zahlen

Diese Berechnung der Länge 5

0	0	0	0	0	0	0	0	0	2	0	0	0	3	2	0	0	1	3	2	0	0	1	1	2	0	0	1	1	1

0	0	0	0	0	0	0	0	0	3	0	0	0	1	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	1

wird durch Zahlen zur Basis b kodiert:

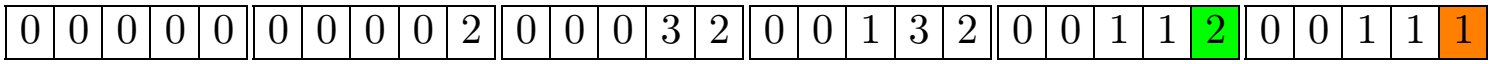
$$\begin{aligned} T &= 000000000200032001320011200111_b = 2000320013200112001 11_b \\ SP &= 000000000300010002000003000001_b = 300010002000003000001_b \end{aligned}$$

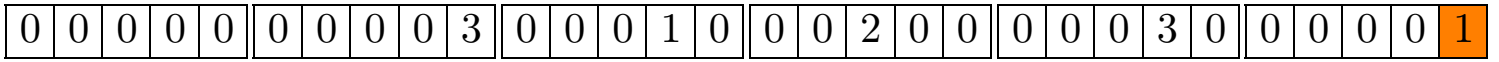
$$n \text{ wird von } \delta \text{ akzeptiert} \Longleftrightarrow \exists b, s, T, SP, \ldots : \ldots \wedge \ldots \wedge \ldots$$

wobei $\ldots \wedge \ldots \wedge \ldots$ exponentiell diophantische Bedingungen an $b, s, T, SP, \ldots$ sind, die die Struktur der Band- und Kopf-Historie beschreiben.

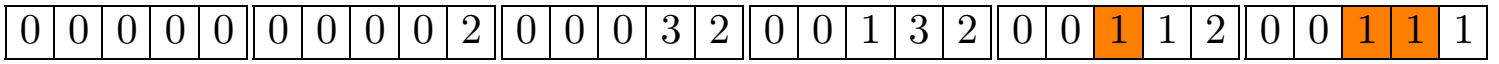
Exponentiell diophantische Bedingungen an T und SP

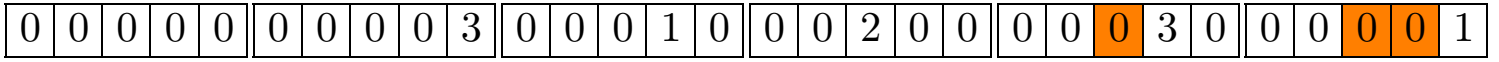
Die grüne 2 wird durch die orangenen 1, 1 impliziert

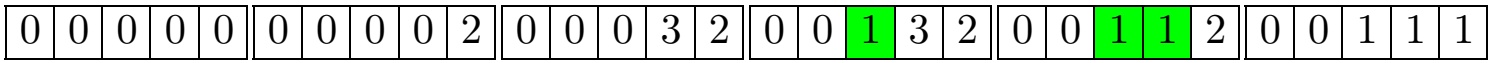




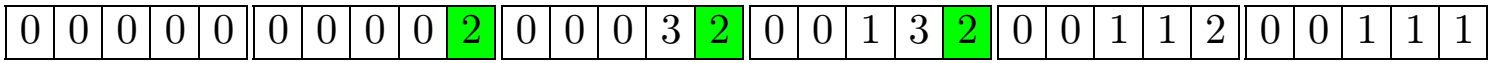
Die grünen 1 werden durch die orangenen 1, 0 impliziert







Die grünen 2 werden durch die orangenen 2, 0 impliziert



.....

$$
\begin{aligned}
T &= \text{Orange}_{1,1} + \text{Orange}_{1,0} + \text{Orange}_{2,0} + \ldots + \text{Orange}_{2,3} \\
&= \text{Grün}_{1,1} + \text{Grün}_{1,0} + \text{Grün}_{2,0} + \ldots + \text{Grün}_{2,3} + \text{Eingabe}
\end{aligned}
$$

wobei

$$
\begin{aligned}
\text{Orange}_{2,0} &= 2000020000200000_b \\
&= 2 \times 1000010000100000_b \\
&= 2 \times \text{Indikator}_{2,0}
\end{aligned}
$$

und

$$
\begin{aligned}
\text{Grün}_{2,0} &= 2000020000200000000000_b \\
&= 200000 \times 1000010000100000_b \\
&= 200000 \times \text{Indikator}_{2,0}
\end{aligned}
$$

T, SP kodieren eine akzeptierende Berechnung für das Turing-Programm

$$\delta\colon \{\ldots,(1,1),\ldots\} \to \{\ldots,(3,2,-1),\ldots\}$$

mit Eingabe e genau dann, wenn

$$\exists\,\text{Basis}\,b\,\exists s \ldots \text{Indikator}_{1,1}\ldots$$

so dass: $b = 2^i$

$$\begin{aligned} T &= \ldots + 1_b \times \text{Indikator}_{1,1} + \ldots + 2_b \times \text{Indikator}_{2,0} + \ldots \\ &= \ldots. + 200000_b \times \text{Indikator}_{1,1} + \ldots + 200000_b \times \text{Indikator}_{2,0} + \ldots + \frac{b^e - 1}{b-1} \\ SP &= \ldots + 1_b \times \text{Indikator}_{1,1} + \ldots + 0_b \times \text{Indikator}_{2,0} + \ldots \\ &= \ldots + 3000000_b \times \text{Indikator}_{1,1} + \ldots + \ldots + 1 \end{aligned}$$

und für die Indikatoren gilt

$$\begin{aligned} \text{Indikator}_{1,1} &\preceq 111101111011110111101111_b \\ &= 1111_b \times 1000010000100001000001_b \end{aligned}$$

- Eine Menge $A \subseteq \mathbb{N}$ ist Turing-aufzählbar (semi-entscheidbar), wenn es ein Turing-Programm δ gibt, so dass

$$A = \{n | \text{ die Berechnung mit Programm } \delta \text{ akzeptiert die Eingabe } n\}$$

- Eine Menge $A \subseteq \mathbb{N}$ ist Turing-berechenbar (entscheidbar), wenn A und $\mathbb{N} \setminus A$ Turing-aufzählbar sind

- Halteproblem: Es gibt eine Turing-aufzählbare Menge HALT $\subseteq \mathbb{N}$, die nicht Turing-entscheidbar ist

- A ist Turing-aufzählbar $\leftrightarrow A$ is exponentiell diophantisch

- HALT ist exponentiell diophantisch

- Davis-Putnam-Robinson: Das 10. Hilbertsche Problem für exponentiell diophantische Gleichungen ist unlösbar: es gibt kein Verfahren, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob eine exponentiell diophantische Gleichung in ganzen rationalen Zahlen lösbar ist.

3. Eine diophantische Kodierung der Exponentiation

Ziel: die dreistellige Relation

$$z = x^y$$

ist diophantisch (entspricht der „Julia-Robinson-Bedingung“, „JR“).

Matiyasevich: die Relation

$$z \text{ ist die } y\text{-te Fibonacci-Zahl } F(y)$$

ist diophantisch, wobei die Fibonacci-Zahlen durch folgende Rekursion

$$F(y+1) = F(y) + F(y-1)$$

definiert sind. Die Fibonacci-Zahlen wachsen exponentiell, die Folge erfüllt viele Gesetzmäßigkeiten, mit deren Hilfe $z = F(y)$ identifiziert werden kann.

Kodierung mit Hilfe der Pellschen Gleichung

Definition 3. *Sei* $a \geqslant 2$. *Für* $n \in \mathbb{N}$ *definiere ganze Zahlen* $X_a(n)$ *und* $Y_a(n)$ *durch*

$$X_a(n) + Y_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$$

Lemma 4. *Es gelten die Rekursionsgleichungen* $X_a(0) = 1$, $Y_a(0) = 0$, *und*

$$\begin{aligned} X_a(n+1) &= aX_a(n) + (a^2-1)Y_a(n) \\ Y_a(n+1) &= X_a(n) + aY_a(n) \end{aligned}$$

Beweis.

$$\begin{aligned} &(X_a(n) + Y_a(n)\sqrt{a^2-1})(a+\sqrt{a^2-1}) = \\ &aX_a(n) + X_a(n)\sqrt{a^2-1} + (a^2-1)Y_a(n) + aY_a(n)\sqrt{a^2-1} = \\ &[aX_a(n) + (a^2-1)Y_a(n)] + [X_a(n) + aY_a(n)]\sqrt{a^2-1} \end{aligned}$$

□

Lemma 5. *$X_a(n)$, $Y_a(n)$ sind (genau die) Lösungen der Pellschen Gleichung*

$$x^2 - (a^2-1)\,y^2 = 1\,.$$

Beweis. Durch Induktion über n. □

Lemma 6. $Y_a(n+1) \geqslant (2a-1)^n$.

Satz 7. *Für $a \geqslant 2$ gilt $y = Y_a(x)$ genau dann, wenn es Zahlen b, s, t, u, v, w gibt mit*

i:	$2x \leqslant y$	vii:	$u \mid t - y$
ii:	$w^2 - (a^2-1)y^2 = 1$	viii:	$y \mid t - x$
iii:	$u^2 - (a^2-1)v^2 = 1$	ix:	$y^2 \mid v$
iv:	$s^2 - (b^2-1)t^2 = 1$	x:	$v > 0$
v:	$u \mid b - a$	xi:	$b \geqslant 2$
vi:	$y \mid b - 1$		

$(\Rightarrow)$ Wähle sukzessive: $w = X_a(x)$, $m = xY_a(x)$, $u = X_a(m)$, $v = Y_a(m)$, b, so dass v, vi erfüllt sind, $s = X_b(x)$, $t = Y_b(x)$. Gleichung ix wird zu

$$Y_a(x)^2 \mid Y_a(xY_a(x))$$

und gilt nach den Teilbarkeitsgesetzen für die Lösungen der Pellschen Gleichung.

Folgerung 8. *Die Relationen $y = Y_a(x)$ und $y = X_a(x)$ sind diophantisch.*

Lemma 9. $2ax - x^2 - 1 \,|\, X_a(y) - (a-x)Y_a(y) - x^y$.

Beweis. Induktion über y.

$$X_a(0) - (a-x)Y_a(0) - x^0 = 1 - (a-x)0 - 1 = 0\,.$$

$$\begin{aligned}
& 2ax - x^2 - 1 \,|\, X_a(y) - (a-x)Y_a(y) - x^y \\
\Rightarrow\ & 2ax - x^2 - 1 \,|\, x(X_a(y) - (a-x)Y_a(y) - x^y) + (2ax - x^2 - 1)Y_a(y) \\
\Leftrightarrow\ & 2ax - x^2 - 1 \,|\, xX_a(y) + (ax - 1)Y_a(y) - xx^y \\
\Leftrightarrow\ & 2ax - x^2 - 1 \,|\, (a - a + x)X_a(y) + (a^2 - 1 - a^2 + ax)Y_a(y) - x^{y+1} \\
\Leftrightarrow\ & 2ax - x^2 - 1 \,|\, aX_a(y) + (a^2 - 1)Y_a(y) - (X_a(y) + aY_a(y))(a-x) - x^{y+1} \\
\Leftrightarrow\ & 2ax - x^2 - 1 \,|\, X_a(y+1) - Y_a(y+1)(a-x) - x^{y+1}
\end{aligned}$$

□

Satz 10. *Die Relation $z = x^y$ ist diophantisch.*

Beweis. Für $a = Y_{2x}(y+2)$ gilt

$$2ax - x^2 - 1 = 2Y_{2x}(y+2)x - x^2 - 1 > x^y.$$

Dann gilt für den Rest

$$\mathrm{Mod}(X_a(y) - (a-x)Y_a(y), 2ax - x^2 - 1) = x^y.$$

Dann ist $z = x^y$ diophantisch mit der Aussage

$$\begin{aligned} \exists a \quad [\quad & (x = 0 \wedge y > 0 \wedge z = 0) \\ \vee \quad & (x > 0 \wedge a = Y_{2x}(y+2) \wedge z = \mathrm{Mod}(X_a(y) - (a-x)Y_a(y), 2ax - x^2 - 1)]. \end{aligned}$$

□

Satz 11. *Das 10. Hilbertsche Problem für diophantische Gleichungen hat keine Lösung.*

4. Anwendungen

1. Ein Polynom, dessen posiiven Werte genau die Primzahlen sind.

2. Ein Polynom, dass genau dann eine Lösung hat, wenn die Peano-Arithmetik inkonsistent ist.

5. Die Gödelschen Sätze

Kurt Gödel, geboren 28. April 1906 in Brünn, Mähren

1924 Studium Universität Wien

1928 Dissertation *Über die Vollständigkeit des Logikkalküls*

1930 Habilitationsschrift *Über formal unentscheidbare Sätze der Principia mathematica und verwandter Systeme I*

1938 Mengentheoretische Konsistenzresultate

1940 Mitglied des *Institute for Advanced Study*, Princeton

gestorben 14. Januar 1978 in Princeton

Kurt Gödel

ca. 1929

Über die Vollständigkeit des Logikkalküls

"Dabei soll "Vollständigkeit" bedeuten, daß jede im engeren Funktionenkalkül ausdrückbare allgemein giltige Formel (...) sich durch eine endliche Reihe formaler Schlüsse aus den Axiomen deduzieren lässt."

Kürzer:

Jede allgemeingültige Aussage ist formal beweisbar.

Satz (Pythagoras?) $\sqrt{2}$ ist eine irrationale Zahl

Beweis Sei $\sqrt{2}$ ist rational, d.h. ein Bruch.
Sei $\sqrt{2} = \frac{a}{b}$, und a ungerade oder b ungerade.
$2 = \frac{a}{b} \cdot \frac{a}{b} = \frac{a \cdot a}{b \cdot b}$.
$2 \cdot b \cdot b = a \cdot a$.
Fall 1. Sei a ungerade.
Dann ist $2 \cdot b \cdot b$ gerade und $a \cdot a$ ungerade. Widerspruch.
Also: Wenn a ungerade ist, folgt ein Widerspruch.
Fall 2. Sei a gerade.
Dann ist b ungerade. $b \cdot b = \frac{a}{2} \cdot a$.
$b \cdot b$ ist ungerade, $\frac{a}{2} \cdot a$ gerade. Widerspruch.
Also: Wenn a gerade ist, folgt ein Widerspruch.
Widerspruch. Also ist $\sqrt{2}$ nicht rational. Qed

Endliche Liste allgemeiner Schlussregeln für formale Beweise

$$\frac{A(x) \quad x = T}{A(T)}$$

$$\frac{\text{Aus } A \text{ folgt } B \qquad \text{Aus nicht } A \text{ folgt } B}{B} \quad \text{Fallunterscheidung}$$

$$\frac{\text{Sei } A \ \ldots\ldots\ldots\ldots\ldots\ B}{\text{Also: Aus } A \text{ folgt } B}$$

$$\frac{A(x)}{\text{Für alle } x \text{ gilt } A}$$

usw.

Die Frage nach der Vollständigkeit

Hilbert und Ackermann 1928:

"Whether the axiom system is complete in the sense that from it all logical formulas that are correct for each domain of individuals can be derived is still an unsolved question. It is only known purely empirically that this axiom system suffices for all applications."

Satz 12. (Gödelscher Vollständigkeitssatz, 1928) *Jede allgemeingültige Formel des engeren Funktionenkalküls ist beweisbar.*

Beweis. Sei B nicht beweisbar. Es genügt, eine Struktur zu konstruieren, in der B falsch ist ..... □

Der erste Gödelsche Unvollständigkeitssatz

Satz 13. *Die Menge* $\mathrm{PA}^+ = \{\varphi | \varphi$ *folgt aus der Theorie* PA$\}$ *ist Turing-aufzählbar.*

Beweis. Folgt aus dem Gödelschen Vollständigkeitssatz. □

Satz 14. *Sei die Theorie* PA *widerspruchsfrei. Dann ist* PA *unvollständig, d.h. es gibt eine zahlentheoretische Aussage* φ*, so dass weder* φ *noch* $\neg\varphi$ *aus* PA *folgen.*

Beweis. Angenommen, PA wäre vollständig. Dann können wir die Lösbarkeit diophantischer Gleichungen $P(\vec{x}) = 0$ folgendermaßen entscheiden. Zähle die Menge PA^+ auf. Wegen der Vollständigkeit von PA kommt mindestens eine der Aussagen

$$\exists \vec{x}\, P(\vec{x}) = 0 \text{ oder } \neg\exists \vec{x}\, P(\vec{x}) = 0$$

in der Aufzählung vor. Wegen der Widerspruchsfreiheit von PA kommt genau eine dieser Aussagen in der Aufzählung vor. Dementsprechend kann man nach endlicher Zeit „Ja“ oder „Nein“ ausgeben. □

Auch die Zermelo-Fraenkelsche Mengenlehre ist unvollständig: *Ignorabimus!*

Der zweite Gödelsche Unvollständigkeitssatz

Diagonalisierung: „dieser Satz ist falsch“, „dieser Satz hat keine Begründung“, „dieser Satz ist nicht in PA beweisbar“.

Formalisiere die Eigenschaft $\gamma \in \mathrm{PA}^+$ diophantisch durch

$$\mathrm{Bew}(\gamma) = (\exists \vec{w}\, P(\gamma, \vec{w}) = 0)$$

Die Formel $\varphi(x) := \neg\mathrm{Bew}(x(x))$ ist eine zahlentheoretische Aussage. Für den Gödel-Satz $\gamma = \varphi(\varphi)$ gilt in der Theorie PA

$$\gamma \leftrightarrow \varphi(\varphi) \leftrightarrow \neg\mathrm{Bew}(\varphi(\varphi)) \leftrightarrow \neg\mathrm{Bew}(\gamma). \tag{1}$$

Lemma 15. a) *Angenommen* PA *impliziert den Gödel-Satz* γ. *Dann impliziert* PA $0=1$, *d.h.* PA *ist inkonsistent.* b) *In* PA *ist beweisbar:* $\mathrm{Bew}(\gamma) \to \mathrm{Bew}(0=1)$.

Beweis. a) Der Beweis von γ in PA kann innerhalb von PA formalisiert werden. In der Theorie PA gilt dann $\mathrm{Bew}(\gamma)$, und nach (1) $\neg\gamma$. Damit ist PA inkonsistent. b) ist die Formalisierung von a) innerhalb von PA. □

Satz 16. (Zweiter Gödelscher Unvollständigkeitssatz) *Wenn* PA *konsistent ist, dann beweist* PA *nicht „die eigene Konsistenz". D.h.* PA *beweist nicht die Aussage* $\neg\mathrm{Bew}(0=1)$.

Beweis. Angenommen PA beweist $\neg\mathrm{Bew}(0=1)$.

Nach Lemma 15b beweist PA die Aussage $\neg\mathrm{Bew}(\gamma)$.

Nach der charakteristischen Eigenschaft des Gödel-Satzes beweist PA die Aussage γ.

Nach Lemma 15a ist PA inkonsistent. □

.