Düstere Ecken der Logik

Ingo Blechschmidt

Curry Club Augsburg

7. September 2017 und 5. Oktober 2017

1. Gödels Unvollständigkeitssatz
   - Beweisbarkeit und Wahrheit
   - Quines
   - Undefinierbarkeit von Wahrheit
   - Konsistenzreflektion
2. Das Halteproblem
   - Unentscheidbarkeit des Halteproblems
   - Unabhängigkeit
   - Das universelle Programm
   - Die universelle Gleichung
3. Randomisierte Strategien

Abschnitt 0

Der effektive Topos

Es gibt ein mathematisches Alternativuniversum, in dem …

1. es nicht trivial ist, dass jede Zahl prim oder nicht prim ist,
2. nicht jede Menge leer ist oder nicht leer ist,
3. jede Funktion $\mathbb{N} \to \mathbb{N}$ berechenbar ist und
4. jede Funktion $\mathbb{R} \to \mathbb{R}$ stetig ist.

Abschnitt 0

Der effektive Topos

Es gibt ein mathematisches Alternativuniversum, in dem …

1. es nicht trivial ist, dass jede Zahl prim oder nicht prim ist,
2. nicht jede Menge leer ist oder nicht leer ist,
3. jede Funktion $\mathbb{N} \to \mathbb{N}$ berechenbar ist und
4. jede Funktion $\mathbb{R} \to \mathbb{R}$ stetig ist.

Zu jedem Modell von Berechenbarkeit, wie etwa Turingmaschinen oder dem Lambda-Kalkül, gibt es eine Variante des „effektiven Topos“. Man kann sogar Maschinen der realen Welt als Grundlage verwenden; dann verlässt man die rigorose Mathematik, erhält aber philosophisch/physikalisch interessante Aussagen.

Turingmaschinen und das Lambda-Kalkül liefern zwar denselben Berechenbarkeitsbegriff für Funktionen $\mathbb{N} \to \mathbb{N}$, sie unterscheiden sich aber in Fragen der Berechenbarkeit von Funktionen höherer Ordnung. Daher sind auch die entstehenden Topoi unterschiedlich.

Mehr zum Thema:

- https://rawgit.com/iblech/mathezirkel-kurs/master/superturingmaschinen/slides.pdf
- https://rawgit.com/iblech/mathezirkel-kurs/master/superturingmaschinen/slides-warwick2017.pdf

Abschnitt I

Gödels Unvollständigkeitssatz

Es gibt wahre Aussagen, die nicht beweisbar sind.

Abschnitt I

Gödels Unvollständigkeitssatz

Es gibt wahre Aussagen, die nicht beweisbar sind.

Zum Beispiel folgende:
„Diese Aussage ist nicht beweisbar.“

Abschnitt I

Gödels Unvollständigkeitssatz

Es gibt wahre Aussagen, die nicht beweisbar sind.

Zum Beispiel folgende:
„Diese Aussage ist nicht beweisbar.“

Currys Paradoxon mahnt zur Vorsicht:
„Sollte diese Aussage stimmen, so ist der Mond aus Käse.“

Abschnitt I

Gödels Unvollständigkeitssatz

Es gibt wahre Aussagen, die nicht beweisbar sind.

Zum Beispiel folgende:
„Diese Aussage ist nicht beweisbar."

Currys Paradoxon mahnt zur Vorsicht:
„Sollte diese Aussage stimmen, so ist der Mond aus Käse."

Wie kann es konzeptionell sein, dass es unbeweisbare wahre Aussagen gibt? Woher können wir von einer Aussage wissen, dass sie wahr ist, wenn nicht durch einen Beweis? Dieser Scheinwiderspruch wird auf den nächsten Folien aufgeklärt.

Wie die Wikipedia- und SEP-Artikel zu Currys Paradoxon erklären, lässt sich nicht jeder grammatikalisch korrekte Aussagesatz menschlicher Sprache als formale Aussage im Sinne der Logik interpretieren.

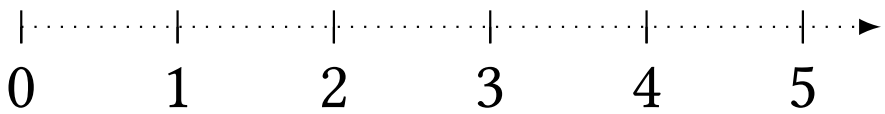
Deswegen ist die Beweisskizze von Gödels Unvollständigkeitssatz auf der vorherigen Folie unvollständig: Es ist korrekt, aber nicht klar, dass die Aussage „Diese Aussage ist unbeweisbar" formal verstanden werden kann.

Das Problem bei Currys Paradoxon liegt übrigens nicht an der Selbstbezüglichkeit, sondern am Wort „stimmen".

Vereinbarungen zur Metaebene

Auf der Metaebene wissen wir, …

1. wie man mit endlichen syntaktischen Objekten operiert,
2. was die natürlichen Zahlen sind,

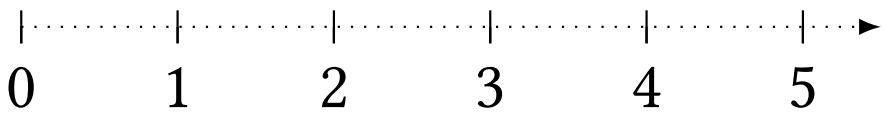


3. was es bedeutet, dass eine Zahl mit einer gewissen Eigenschaft existiert oder dass eine Behauptung für alle Zahlen stimmt.

Vereinbarungen zur Metaebene

Auf der Metaebene wissen wir, …

1. wie man mit endlichen syntaktischen Objekten operiert,
2. was die natürlichen Zahlen sind,



3. was es bedeutet, dass eine Zahl mit einer gewissen Eigenschaft existiert oder dass eine Behauptung für alle Zahlen stimmt.

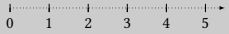
Mögliche Wahlen der Metaebene:

- gesunder Menschenverstand mit Platonismus
- gesunder Menschenverstand mit Formalismus
- diverse formale Systeme

Vereinbarungen zur Metaebene

Auf der Metaebene wissen wir, …

1. wie man mit endlichen syntaktischen Objekten operiert,
2. was die natürlichen Zahlen sind,



3. was es bedeutet, dass eine Zahl mit einer gewissen Eigenschaft existiert oder dass eine Behauptung für alle Zahlen stimmt.

Mögliche Wahlen der Metaebene:

- gesunder Menschenverstand mit Platonismus
- gesunder Menschenverstand mit Formalismus
- diverse formale Systeme

Wenn man sich entscheidet, die Metaebene formal zu halten, verwendet man oft sehr schwache Systeme wie etwa PRA, die sowohl von ihren sprachlichen Mitteln als auch den erlaubten logischen Schlüsseln sehr eingeschränkt sind. (PRA ist so schwach, dass es noch nicht einmal einen Unterschied zwischen klassischem und intuitionistischem PRA gibt. In PRA gibt es auch keine Realisierung der aktual unendlichen Menge der natürlichen Zahlen.)

Das macht man aus zwei Gründen: Zum einen möchte man in diesem Geschäft unter anderem die Konsistenz von gewissen logischen Systemen untersuchen. Um sicher zu gehen, dass solche Untersuchungen aussagekräftig sind, sollten sie selbst keine mächtigen logischen Prinzipien verwenden.

Zum anderen möchte man Argumente auf der Metaebene gelegentlich auch in anderen Systemen internalisieren. Dazu ist es hilfreich, auf der Metaebene ein System zu verwenden, dass als größter gemeinsamer Nenner aller relevanten anderen Systeme fungieren kann. PRA ist ein solches System.

Oft verwendet man aber auch starke Systeme wie Zermelo–Fraenkel-Mengenlehre mit Auswahlaxiom und großen Kardinalzahlaxiomen als Metaebene, um interessante modelltheoretische Aussagen treffen zu können.

Peano-Arithmetik

Die Schlussregeln und Axiome von PA sind:

- die üblichen Schlussregeln von Logik erster Ordnung
- $\neg(\exists n.\ 0 = S(n))$
- $\forall n.\ \forall m.\ (S(n) = S(m) \to n = m)$
- $\forall n.\ n + 0 = n$
- $\forall n.\ \forall m.\ n + S(m) = S(n + m)$
- $\forall n.\ n \cdot 0 = 0$
- $\forall n.\ \forall m.\ n \cdot S(m) = n \cdot m + n$
- Für jede Aussageform $A(n)$ je ein Induktionsaxiom:

$$(A(0) \land (\forall n.\ (A(n) \to A(n+1)))) \to \forall n.\ A(n).$$

Peano-Arithmetik

Die Schlussregeln und Axiome von PA sind:

- die üblichen Schlussregeln von Logik erster Ordnung
- $\neg(\exists n.\ 0 = S(n))$
- $\forall n.\ \forall m.\ (S(n) = S(m) \to n = m)$
- $\forall n.\ n + 0 = n$
- $\forall n.\ \forall m.\ n + S(m) = S(n + m)$
- $\forall n.\ n \cdot 0 = 0$
- $\forall n.\ \forall m.\ n \cdot S(m) = n \cdot m + n$
- Für jede Aussageform $A(n)$ je ein Induktionsaxiom:

$$(A(0) \land (\forall n.\ (A(n) \to A(n+1)))) \to \forall n.\ A(n).$$

Im Folgenden studieren wir *Peano-Arithmetik* (PA), ein wichtiges formales System in Logik erster Ordnung. Genauso gut könnten wir eine Formalisierung von Mengenlehre in Logik erster Ordnung oder diverse andere Systeme verwenden.

Die Terme von PA werden induktiv aus der Konstante 0, der Nachfolgeroperation S und Funktionssymbolen für jede primitiv-rekursive Funktion zusammengesetzt. Etwa ist $4 := S(S(S(S(0))))$ ein Term in PA.

Aussagen in PA werden induktiv aus folgenden Zutaten zusammengesetzt:

- $s = t$, wobei s und t beliebige Terme sind
- $\top$ („truthhood“) und $\bot$ („falsehood“)
- $A \land B$, $A \lor B$, $A \to B$ und $\neg A$ als Abkürzung für $A \to \bot$
- $\forall n.\ A(n)$ und $\exists n.\ A(n)$

Beweisbarkeit und Wahrheit

Syntaktische Qualität

Eine Aussage A heißt genau dann **beweisbar**, wenn es in einem fixierten formalen System einen **formalen Beweis** von A gibt:

$$\mathrm{PA} \vdash A$$

Semantische Qualität

Eine Aussage A heißt genau dann **wahr**, wenn sie im **Standardmodell** gilt: $\mathbb{N} \models A$

Beweisbarkeit und Wahrheit

Syntaktische Qualität

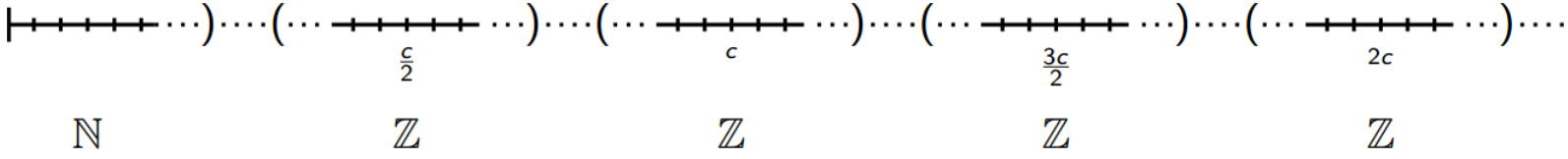
Eine Aussage A heißt genau dann **beweisbar**, wenn es in einem fixierten formalen System einen **formalen Beweis** von A gibt:

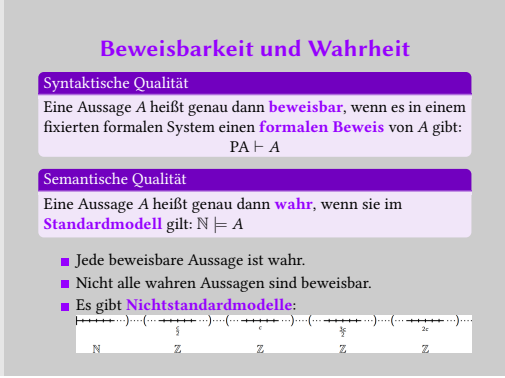
$$\mathrm{PA} \vdash A$$

Semantische Qualität

Eine Aussage A heißt genau dann **wahr**, wenn sie im **Standardmodell** gilt: $\mathbb{N} \models A$

- Jede beweisbare Aussage ist wahr.
- Nicht alle wahren Aussagen sind beweisbar.
- Es gibt **Nichtstandardmodelle**:





Die Axiome von Peano-Arithmetik sind so konzipiert, dass sie genau das Wesen der natürlichen Zahlen einfangen. Dieses Ziel wurde aber nicht erreicht: Nicht nur die üblichen natürlichen Zahlen, das Standardmodell, erfüllen die Peano-Axiome, auch die diversen Nichtstandardmodelle tun es.

Das ist ein grundsätzliches Phänomen an Logik erster Ordnung; mit Logik zweiter Ordnung, bei der nicht nur über Elemente, sondern auch über Teilmengen quantifiziert werden kann, kann man Axiome formulieren, die nur von den üblichen natürlichen Zahlen und nicht von weiteren Strukturen erfüllt werden. Vorteile an Logik erster Ordnung sind Einfachheit und die Existenz von Vollständigkeitssätzen: Gilt eine Aussage in *allen* Modellen, so ist sie beweisbar.

Nur wenig Leute möchten nicht unterstellen, dass die Metaebene die Schlussregeln von Peano-Arithmetik mitmacht und in der $\mathbb{N}$ die Peano-Axiome erfüllt. Unterstellt man das, so sind beweisbare Aussagen auch wahr. Überdies sind beweisbare Aussagen auch in allen Nichtstandardmodellen wahr.

Es wird niemals eine Haskell-Bibliothek zum Umgang mit Nichtstandardzahlen geben: Tennenbaum bewies 1959, dass es kein Nichtstandardmodell gibt, dessen Elemente man als Bitfolgen kodieren könnte, sodass Addition oder Multiplikation berechenbar sind.

Mehr zu Nichtstandardmodellen steht auf dem Blog von Victoria Gitman.

Beweisbarkeit und Wahrheit

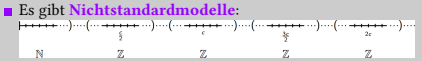
Syntaktische Qualität

Eine Aussage A heißt genau dann **beweisbar**, wenn es in einem fixierten formalen System einen **formalen Beweis** von A gibt:
$\mathrm{PA} \vdash A$

Semantische Qualität

Eine Aussage A heißt genau dann **wahr**, wenn sie im **Standardmodell** gilt: $\mathbb{N} \models A$

- Jede beweisbare Aussage ist wahr.
- Nicht alle wahren Aussagen sind beweisbar.
- Es gibt **Nichtstandardmodelle**:



Sei A etwa die formale Aussage $\forall n.\ \forall m.\ (n+m)^2 = n^2+2nm+m^2$. Dann bedeutet $\mathbb{N} \models A$, dass für alle gewöhnlichen Zahlen die binomische Formel gilt. Ist M irgendein Nichtstandardmodell, so bedeutet $M \models A$, dass für alle Zahlen des Nichtstandardmodells die binomische Formel gilt. (Die Aussage A ist übrigens beweisbar und daher in allen Modellen gültig.)

Die meisten Leute erachten PA als *konsistent*, d. h. die Aussage $\bot$ (oder äquivalent die Aussage $0 = 1$) als nicht beweisbar. Denn wenn $0 = 1$ beweisbar wäre, so wäre auch $0 = 1$ im Standardmodell $\mathbb{N}$ (wenn man akzeptiert, dass $\mathbb{N}$ die Peano-Axiome erfüllt); dem ist aber nicht so.

Ein rein syntaktischer und finitistisch zulässiger Beweis der Konsistenz von PA wurde aber noch nicht erbracht. Es macht Spaß, die Inkonsistenz von PA in Betracht zu ziehen; die wenigsten Leute machen das ernsthaft, aber ein paar schon (Nelson, Voevodsky, …).

Quines

Wir schreiben $\ulcorner A \urcorner$ für die **Gödelnummer** einer Aussage A.

Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\text{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A beweisbar ist:

$$\mathbb{N} \models \text{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \text{PA} \vdash A.$$

Quines

Wir schreiben $\ulcorner A \urcorner$ für die **Gödelnummer** einer Aussage A.

Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\text{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A beweisbar ist:

$$\mathbb{N} \models \text{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \text{PA} \vdash A.$$

Mit dem **Diagonallemma** gibt es eine Aussage G mit

$$\text{PA} \vdash (G \leftrightarrow \neg(\text{Prov}(\ulcorner G \urcorner))).$$

Quines

Wir schreiben $\ulcorner A \urcorner$ für die **Gödelnummer** einer Aussage A.

Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\text{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A beweisbar ist:

$$\mathbb{N} \models \text{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \text{PA} \vdash A.$$

Mit dem **Diagonallemma** gibt es eine Aussage G mit

$$\text{PA} \vdash (G \leftrightarrow \neg(\text{Prov}(\ulcorner G \urcorner))).$$

1. Angenommen $\text{PA} \vdash G$. Dann $\text{PA} \vdash \neg(\text{Prov}(\ulcorner G \urcorner))$, also $\mathbb{N} \models \neg(\text{Prov}(\ulcorner G \urcorner))$, also nicht $\mathbb{N} \models \text{Prov}(\ulcorner G \urcorner)$, also ist G nicht beweisbar, also folgt ein Widerspruch.
2. Also ist G nicht beweisbar, somit $\mathbb{N} \models \neg\text{Prov}(\ulcorner G \urcorner)$.
3. Also $\mathbb{N} \models G$, d. h. G ist wahr.

Quines

Wir schreiben $\ulcorner A \urcorner$ für die Gödelnummer einer Aussage A.

Reflektion von Beweisbarkeit

Es gibt eine Aussageform $\mathrm{Prov}(n)$, sodass für jede Aussage A genau dann $\mathrm{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A beweisbar ist:

$$\mathbb{N} \models \mathrm{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \mathrm{PA} \vdash A.$$

Mit dem Diagonallemma gibt es eine Aussage G mit

$$\mathrm{PA} \vdash (G \leftrightarrow \neg(\mathrm{Prov}(\ulcorner G \urcorner))).$$

1. Angenommen $\mathrm{PA} \vdash G$. Dann $\mathrm{PA} \vdash \neg(\mathrm{Prov}(\ulcorner G \urcorner))$, also $\mathbb{N} \models \neg(\mathrm{Prov}(\ulcorner G \urcorner))$, also nicht $\mathbb{N} \models \mathrm{Prov}(\ulcorner G \urcorner)$, also ist G nicht beweisbar, also folgt ein Widerspruch.
2. Also ist G nicht beweisbar, somit $\mathbb{N} \models \neg\mathrm{Prov}(\ulcorner G \urcorner)$.
3. Also $\mathbb{N} \models G$, d. h. G ist wahr.

Die mit dem Diagonallemma konstruierte Aussage G drückt umgangssprachlich aus: „Aussage G ist nicht beweisbar.“ Der auf der vorhergehenden Folie gegebene Beweis von Gödels Unvollständigkeitssatz ist also eine Ausformalisierung der anfangs gegebenen Beweisskizze. Das Diagonallemma ermöglicht, Selbstbezüglichkeit zu elimieren.

Dieser (Meta-)Beweis von Gödels Unvollständigkeitssatz liefert ein explizites Beispiel für eine Aussage, die im Standardmodell wahr ist, aber keinen formalen Beweis in PA besitzt. Die so erhaltene Aussage wurde aber speziell für diese Argumentation konstruiert. Es gibt viele weitere Beispiele für unbeweisbare wahre Aussagen, die inhaltlich viel interessanter sind und auf den ersten Blick keinerlei Verbindungen zur mathematischen Logik aufzuweisen scheinen, insbesondere nicht Selbstbezüglichkeit oder Begriffe wie „Beweisbarkeit“ enthalten.

Das Argument auf der vorhergehenden Folie für $\mathrm{PA} \nvdash G$ war semantisch: Es verwendete, dass $\mathbb{N}$ ein Modell von PA ist. Ein rein syntaktischer Beweis, der nur die Annahme der Konsistenz von PA verwendet, ist auch möglich: Angenommen, es gibt einen formalen Beweis von G. Dieser hat eine Gödelnummer, sodass man ihn in das formale System bringen kann: Es folgt $\mathrm{PA} \vdash \mathrm{Prov}(\ulcorner G \urcorner)$. Zugleich gilt $\mathrm{PA} \vdash \neg(\mathrm{Prov}(\ulcorner G \urcorner))$. Also $\mathrm{PA} \vdash \bot$. Widerspruch.

Die Negation von G ist in PA ebenfalls nicht beweisbar: Wenn doch, wäre sie wahr, ist sie aber nicht. Ein syntaktischer Beweis ist nicht bekannt, aber *Rossers Trick* liefert eine leichte Variante G', von der syntaktisch $\mathrm{PA} \nvdash G'$ und $\mathrm{PA} \nvdash \neg G'$ nachweisbar sind (nur unter der Konsistenzannahme).

Quines

Wir schreiben $\ulcorner A \urcorner$ für die **Gödelnummer** einer Aussage A.

Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\text{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A beweisbar ist:

$$\mathbb{N} \models \text{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \text{PA} \vdash A.$$

Mit dem **Diagonallemma** gibt es eine Aussage G mit

$$\text{PA} \vdash (G \leftrightarrow \neg(\text{Prov}(\ulcorner G \urcorner))).$$

1. Angenommen $\text{PA} \vdash G$. Dann $\text{PA} \vdash \neg(\text{Prov}(\ulcorner G \urcorner))$, also $\mathbb{N} \models \neg(\text{Prov}(\ulcorner G \urcorner))$, also nicht $\mathbb{N} \models \text{Prov}(\ulcorner G \urcorner)$, also ist G nicht beweisbar, also folgt ein Widerspruch.
2. Also ist G nicht beweisbar, somit $\mathbb{N} \models \neg\text{Prov}(\ulcorner G \urcorner)$.
3. Also $\mathbb{N} \models G$, d. h. G ist wahr.

Die Aussage G, die das Diagonallemma liefert, lautet ins Deutsche übersetzt wie folgt:

„Die Aussage, die man erhält, wenn man in der Aussage ‚Die Aussage, die man erhält, wenn man in der Aussage x die vorkommende Variable durch die Gödelnummer dieser Aussage ersetzt, ist nicht beweisbar.‘ die vorkommende Variable durch die Gödelnummer dieser Aussage ersetzt, ist nicht beweisbar.“

Das Diagonallemma sagt aus: Sei $F(n)$ eine Aussageform. Dann gibt es eine Aussage D mit

$$\text{PA} \vdash (D \leftrightarrow F(\ulcorner D \urcorner)).$$

Der Beweis ist konstruktiv und gibt die Aussage D explizit an. Für den Fall, dass man nicht glaubt, dass beweisbare Aussagen wahr sind – etwa weil man als Ultrafinitist nicht vom Induktionsaxiom für natürliche Zahlen überzeugt ist –, so ist es noch hilfreich zu wissen, dass für die vom Diagonallemma konstruierte Aussage sogar gilt: Genau dann ist D wahr, wenn $F(\ulcorner D \urcorner)$ wahr ist.

Das ist noch aus einem anderen Grund gut zu wissen: Argumentationen, die nicht die Wahrheit von beweisbaren Aussagen unterstellen, können *internalisiert* werden. Das wird auf späteren Folien diskutiert.

Goodsteinsche Folgen

Beginne etwa mit 35. Schreibe die Zahl in **hereditary base 2**:

$$\begin{aligned} 35 &= 1 \cdot 2^5 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 2^{1 \cdot 2^2 + 1 \cdot 2^0} + 1 \cdot 2^1 + 1 \cdot 2^0. \end{aligned}$$

Ersetze alle Vorkommen von 2 durch 3:

$$\begin{aligned} & 1 \cdot 3^{1 \cdot 3^3 + 1 \cdot 3^0} + 1 \cdot 3^1 + 1 \cdot 3^0 \\ &= 1 \cdot 3^{28} + 3 + 1 \\ &= 22876792454965. \end{aligned}$$

Ziehe dann 1 ab:

$$22876792454964.$$

Mach immer so weiter.

Goodsteinsche Folgen

Beginne etwa mit 35. Schreibe die Zahl in **hereditary base 2**:

$$\begin{aligned} 35 &= 1 \cdot 2^5 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 2^{1 \cdot 2^2 + 1 \cdot 2^0} + 1 \cdot 2^1 + 1 \cdot 2^0. \end{aligned}$$

Ersetze alle Vorkommen von 2 durch 3:

$$\begin{aligned} & 1 \cdot 3^{1 \cdot 3^3 + 1 \cdot 3^0} + 1 \cdot 3^1 + 1 \cdot 3^0 \\ &= 1 \cdot 3^{28} + 3 + 1 \\ &= 22876792454965. \end{aligned}$$

Ziehe dann 1 ab:

$$22876792454964.$$

Mach immer so weiter.

- Schlussendlich ist das Ergebnis 0.
- PA kann nicht beweisen, dass dem immer so ist.

Immunität gegen Gödel

Wir sahen: Im Standardmodell wahre Aussagen besitzen nicht unbedingt einen formalen Beweis.

Für Aussagen, die nur aus folgenden Zutaten zusammengesetzt sind, passiert das nicht:

- Gleichheit: $s = t$
- Konjunktion: $\top$ und $\wedge$
- Disjunktion: $\bot$ und $\vee$
- Existenzquantifikation: $\exists$
- Beschränkte Allquantifikation: $\forall n.\ (n \leq t \to \cdots)$

Nicht vorkommen dürfen: $\to$, $\neg$, $\forall$. Solche Aussagen heißen **Σ-Aussagen** oder **geometrische Aussagen**.

Undefinierbarkeit von Wahrheit

Erinnerung: Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\mathrm{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A **beweisbar** ist:

$$\mathbb{N} \models \mathrm{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \mathrm{PA} \vdash A.$$

Nun: Kann man auch Wahrheit reflektieren?

Gibt es eine Aussageform **True(n)**, sodass für jede Aussage A genau dann $\mathrm{True}(\ulcorner A \urcorner)$ wahr ist, wenn A **wahr** ist?

$$\mathbb{N} \models \mathrm{True}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \mathbb{N} \models A$$

Undefinierbarkeit von Wahrheit

Erinnerung: Reflektion von Beweisbarkeit

Es gibt eine Aussageform **Prov(n)**, sodass für jede Aussage A genau dann $\mathrm{Prov}(\ulcorner A \urcorner)$ wahr ist, wenn A **beweisbar** ist:

$$\mathbb{N} \models \mathrm{Prov}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \mathrm{PA} \vdash A.$$

Nun: Kann man auch Wahrheit reflektieren?

Gibt es eine Aussageform **True(n)**, sodass für jede Aussage A genau dann $\mathrm{True}(\ulcorner A \urcorner)$ wahr ist, wenn A **wahr** ist?

$$\mathbb{N} \models \mathrm{True}(\ulcorner A \urcorner) \quad \text{genau dann, wenn} \quad \mathbb{N} \models A$$

Nein: Mit dem Diagonallemma gäbe es eine Aussage A mit

$$\mathrm{PA} \vdash (A \leftrightarrow \neg(\mathrm{True}(\ulcorner A \urcorner))).$$

Zu deutsch besagte A: „Aussage A ist nicht wahr.“
Diese Aussage wäre genau dann wahr, wenn sie nicht wahr ist.

Konsistenzreflektion

Sei wie vorher G die Aussage „Aussage G ist nicht beweisbar“.
Wir wissen: Ist PA konsistent (d. h. ist $1 = 0$ nicht beweisbar), so stimmt G.

Konsistenzreflektion

Sei wie vorher G die Aussage „Aussage G ist nicht beweisbar“.
Wir wissen: Ist PA konsistent (d. h. ist $1 = 0$ nicht beweisbar), so stimmt G.

Das dafür präsentierte Argument könnten wir formalisieren.
Daher folgt:

$$\mathrm{PA} \vdash (\neg(\mathrm{Prov}(\ulcorner 1 = 0 \urcorner)) \to G).$$

Konsistenzreflektion

Sei wie vorher G die Aussage „Aussage G ist nicht beweisbar“. Wir wissen: Ist PA konsistent (d. h. ist $1 = 0$ nicht beweisbar), so stimmt G.

Das dafür präsentierte Argument könnten wir formalisieren. Daher folgt:

$$\mathrm{PA} \vdash (\neg(\mathrm{Prov}(\ulcorner 1 = 0 \urcorner)) \to G).$$

Ist PA konsistent, so folgt:

PA kann die Konsistenz von PA nicht beweisen.

Denn aus $\mathrm{PA} \vdash \neg(\mathrm{Prov}(\ulcorner 1 = 0 \urcorner))$ folgte $\mathrm{PA} \vdash G$, was unter der Konsistenzannahme falsch ist.

Going deeper

Wir schreiben „Con“ für „$\neg(\mathrm{Prov}(\ulcorner 1 = 0 \urcorner))$“.

Wir wissen: Genau dann ist PA konsistent, wenn PA die Konsistenz von PA nicht beweisen kann.

Das dafür präsentierte Argument könnten wir formalisieren. Daher folgt:

$$\mathrm{PA} \vdash (\mathrm{Con} \leftrightarrow \neg(\mathrm{Prov}(\ulcorner \mathrm{Con} \urcorner))).$$

Übungsaufgaben

1. Sei A eine Aussage. Sei B eine vom Diagonallemma gelieferte Aussage mit

$$\mathrm{PA} \vdash (B \leftrightarrow (\mathrm{Prov}(\ulcorner B \urcorner) \to A)).$$

   Zeige: Sollte aus Beweisbarkeit von A Wahrheit von A folgen, so ist B wahr. Internalisiere anschließend dein Argument, um zu zeigen, dass

$$\mathrm{PA} \vdash ((\mathrm{Prov}(\ulcorner A \urcorner) \to A) \to B).$$

   Tipp. Dass B wahr ist, bedeutet, dass aus Beweisbarkeit von B Wahrheit von A folgt.

2. Sei H eine ihre eigene Beweisbarkeit behauptende Aussage:

$$\mathrm{PA} \vdash (H \leftrightarrow \mathrm{Prov}(\ulcorner H \urcorner)).$$

   Zeige, dass H beweisbar ist.

3. Zeige: Ist $\mathrm{Prov}(\ulcorner A \urcorner) \to A$ beweisbar, so ist schon A beweisbar.

4. Sei n eine große Zahl. Sei L eine Aussage, die ausdrückt, dass kein Beweis von ihr kürzere Länge als 2^n hat. Zeige, dass L unter Annahme der Konsistenz wahr ist. Internalisiere dein Argument, um zu zeigen, dass es in PA einen kurzen Beweis von $(\mathrm{Con} \to L)$ gibt.

Übungsaufgaben

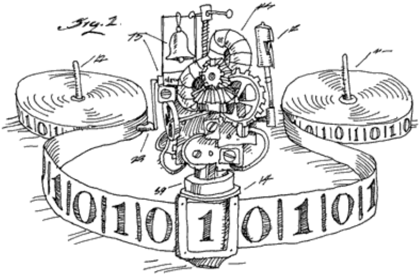
1. Sei A eine Aussage. Sei B eine vom Diagonallemma gelieferte Aussage mit
$$\mathrm{PA} \vdash (B \leftrightarrow (\mathrm{Prov}(\ulcorner B \urcorner) \to A)).$$
Zeige: Sollte aus Beweisbarkeit von A Wahrheit von A folgen, so ist B wahr. Internalisiere anschließend dein Argument, um zu zeigen, dass
$$\mathrm{PA} \vdash ((\mathrm{Prov}(\ulcorner A \urcorner) \to A) \to B).$$
Tipp. Dass B wahr ist, bedeutet, dass aus Beweisbarkeit von B Wahrheit von A folgt.
2. Sei H eine ihre eigene Beweisbarkeit behauptende Aussage:
$$\mathrm{PA} \vdash (H \leftrightarrow \mathrm{Prov}(\ulcorner H \urcorner)).$$
Zeige, dass H beweisbar ist.
3. Zeige: Ist $\mathrm{Prov}(\ulcorner A \urcorner) \to A$ beweisbar, so ist schon A beweisbar.
4. Sei n eine große Zahl. Sei L eine Aussage, die ausdrückt, dass kein Beweis von ihr kürzere Länge als 2^n hat. Zeige, dass L unter Annahme der Konsistenz wahr ist. Internalisiere dein Argument, um zu zeigen, dass es in PA einen kurzen Beweis von $(\mathrm{Con} \to L)$ gibt.

Punkt 3 drückt ein Theorem von Löb aus. Es gibt einen Beweis in Cartoonform von Eliezier Yudkowsky.

Punkt 4 zeigt: Die Annahme der Konsistenz kann Beweise deutlich verkürzen: Der kürzeste Beweis von L hat mindestens Länge 2^n; von $(\mathrm{Con} \to L)$ dagegen gibt es kurze Beweise.

Abschnitt II

Spiel und Spaß mit Berechenbarkeitstheorie



Unentscheidbarkeit des Halteproblems

Ein **Halteorakel** ist ein Programm, das ein Programm P als Eingabe liest und korrekt ausgibt: „P hält“ oder „P hält nicht“.

Unentscheidbarkeit des Halteproblems

Ein **Halteorakel** ist ein Programm, das ein Programm P als Eingabe liest und korrekt ausgibt: „P hält“ oder „P hält nicht“.

Wenn es ein Halteorakel gäbe, könnte man auch folgendes Programm Q entwickeln:

> Befrage das Halteorakel, ob Programm Q hält.
> Falls ja: Gehe in eine Endlosschleife.
> Falls nein: Halte.

Unentscheidbarkeit des Halteproblems

Ein **Halteorakel** ist ein Programm, das ein Programm P als Eingabe liest und korrekt ausgibt: „P hält“ oder „P hält nicht“.

Wenn es ein Halteorakel gäbe, könnte man auch folgendes Programm Q entwickeln:

> Befrage das Halteorakel, ob Programm Q hält.
> Falls ja: Gehe in eine Endlosschleife.
> Falls nein: Halte.

Das Programm Q hält genau dann, wenn es nicht hält.

Ein Halteorakel gibt es nicht.

Unentscheidbarkeit des Halteproblems

Ein **Halteorakel** ist ein Programm, das ein Programm P als Eingabe liest und korrekt ausgibt: „P hält“ oder „P hält nicht“.

Wenn es ein Halteorakel gäbe, könnte man auch folgendes Programm Q entwickeln:

> Befrage das Halteorakel, ob Programm Q hält.
> Falls ja: Gehe in eine Endlosschleife.
> Falls nein: Halte.

Das Programm Q hält genau dann, wenn es nicht hält.

Ein Halteorakel gibt es nicht.

Ein praktisch verwendbares Halteorakel wäre extrem nützlich, da man mit ihm auf einen Schlag unzählige offene mathematische Vermutungen klären könnte. Etwa ist momentan noch unbekannt, ob es ungerade perfekte Zahlen gibt. Hätte man ein Halteorakel, könnte man diese Frage sofort klären, indem man es befragt, ob ein Programm, dass alle ungeraden natürlichen Zahlen abläuft und genau dann abbricht, wenn es eine perfekte Zahl gefunden hat, hält.

Chaitinsche Haltewahrscheinlichkeit

Sei Ω die Zahl

$$\Omega = \sum_p 2^{-|p|} = c_0 \cdot 1 + c_1 \cdot \frac{1}{2} + c_2 \cdot \frac{1}{4} + c_3 \cdot \frac{1}{8} + \cdots,$$

wobei c_n die Anzahl derjenigen Programme der Länge n ist, welche halten.

- Ω ist eine wohldefinierte Zahl zwischen 0 und 1.
- Sind die ersten N Nachkommaziffern von Ω bekannt, so lässt sich das Halteproblem für alle Programme der Länge $\leq N$ lösen.

Chaitinsche Haltewahrscheinlichkeit

Sei Ω die Zahl

$$\Omega = \sum_p 2^{-|p|} = c_0 \cdot 1 + c_1 \cdot \frac{1}{2} + c_2 \cdot \frac{1}{4} + c_3 \cdot \frac{1}{8} + \cdots,$$

wobei c_n die Anzahl derjenigen Programme der Länge n ist, welche halten.

- Ω ist eine wohldefinierte Zahl zwischen 0 und 1.
- Sind die ersten N Nachkommaziffern von Ω bekannt, so lässt sich das Halteproblem für alle Programme der Länge $\leq N$ lösen.
- Ω ist nicht berechenbar.

Chaitinsche Haltewahrscheinlichkeit

Sei Ω die Zahl

$$\Omega = \sum_p 2^{-|p|} = c_0 \cdot 1 + c_1 \cdot \frac{1}{2} + c_2 \cdot \frac{1}{4} + c_3 \cdot \frac{1}{8} + \cdots,$$

wobei c_n die Anzahl derjenigen Programme der Länge n ist, welche halten.

- Ω ist eine wohldefinierte Zahl zwischen 0 und 1.
- Sind die ersten N Nachkommaziffern von Ω bekannt, so lässt sich das Halteproblem für alle Programme der Länge $\leq N$ lösen.
- Ω ist nicht berechenbar.
- Es gibt eine konkrete Zahl N, sodass PA keine Vermutung über mehr als N Nachkommaziffern beweisen kann.

Chaitinsche Haltewahrscheinlichkeit

Sei Ω die Zahl

$$\Omega = \sum_P 2^{-|p|} = c_0 \cdot 1 + c_1 \cdot \frac{1}{2} + c_2 \cdot \frac{1}{4} + c_3 \cdot \frac{1}{8} + \cdots,$$

wobei c_n die Anzahl derjenigen Programme der Länge n ist, welche halten.

- Ω ist eine wohldefinierte Zahl zwischen 0 und 1.
- Sind die ersten N Nachkommaziffern von Ω bekannt, so lässt sich das Halteproblem für alle Programme der Länge $\leq N$ lösen.
- Ω ist nicht berechenbar.
- Es gibt eine konkrete Zahl N, sodass PA keine Vermutung über mehr als N Nachkommaziffern beweisen kann.

Der amerikanische Physiker und Informatiker Charles Bennet (* 1943) und der berühmte Wissenschaftsjournalist Martin Gardner (* 1914, † 2010) schrieben Folgendes über Ω:

„Die Konstante Ω verkörpert eine enorme Menge an Wissen auf sehr kleinem Raum. Die ersten paar Tausend Ziffern, die problemlos auf einem kleinen Stück Papier Platz finden könnten, enthalten die Antworten auf mehr mathematische Fragen, als man im ganzen Universum aufschreiben könnte.

Im Laufe der Menschheitsgeschichte strebten Mystiker und Philosophen stets nach einem kompakten Schlüssel zu universeller Weisheit, einer endlichen Formel oder einem Text, der, wenn bekannt und verstanden, Antworten auf alle Fragen liefern würde; man denke nur an die Versuche, der Bibel, dem Koran oder dem I Ging Weissagungen zu entlocken [...].

Solche Quellen universeller Weisheit sind herkömmlicherweise vor beiläufigem Zugriff geschützt: indem sie schwer zu finden, wenn gefunden schwierig zu verstehen und gefährlich zu benutzen sind, dazu neigend, mehr und tiefere Fragen zu beantworten als sich der Suchende wünschte. Das esoterische Buch ist, wie Gott, einfach und dennoch unbeschreibbar. Es ist allwissend, und verändert alle, die es kennen.

Ω ist in vielerlei Hinsicht eine kabbalistische Zahl. Dem menschlichen Verstand ist sie bekannt, aber unkennbar. Um sie im Detail zu erfahren, müsste man ihre unberechenbare Ziffernfolge als Glaubensgrundsatz einfach hinnehmen, genau wie die Worte eines heiligen Texts."

Ein Programm mit unbeweisbarem Halteverhalten

Wir betrachten folgendes Programm P:

> Laufe systematisch alle formalen Beweise ab. Sobald ein Beweis von $1 = 0$ gefunden wurde, halte.

Ein Programm mit unbeweisbarem Halteverhalten

Wir betrachten folgendes Programm P:

> Laufe systematisch alle formalen Beweise ab. Sobald ein Beweis von $1 = 0$ gefunden wurde, halte.

Ist PA konsistent, so gilt:

- Das Programm P hält nicht.
- Die Aussage, dass P nicht halte, ist in PA nicht beweisbar.
- Sei n die Anzahl Zustände, die eine Umsetzung von P als Turingmaschine benötigt. Dann entzieht sich jede Vermutung über $\mathrm{BB}(n)$ der Beweisbarkeit in PA.

Das universelle Programm

Wir betrachten folgendes Programm P:

> Laufe systematisch alle formalen Beweise ab. Sobald ein Beweis einer Aussage der Form „Die Ausgabe von Programm P ist nicht die Liste $x_1, \ldots, x_n$“ gefunden wurde, gib die Liste $x_1, \ldots, x_n$ aus und halte.

1. PA beweist, dass P eine endliche Liste von Zahlen ausgibt (vielleicht die leere Liste, falls P nicht halten sollte).
2. Für jede endliche Liste von Zahlen gibt es ein Universum U, sodass P genau diese Liste ausgibt, wenn man es in U ausführt.

Das universelle Programm

Wir betrachten folgendes Programm P:

> Laufe systematisch alle formalen Beweise ab. Sobald ein Beweis einer Aussage der Form „Die Ausgabe von Programm P ist nicht die Liste $x_1, \ldots, x_n$“ gefunden wurde, gib die Liste $x_1, \ldots, x_n$ aus und halte.

1. PA beweist, dass P eine endliche Liste von Zahlen ausgibt (vielleicht die leere Liste, falls P nicht halten sollte).
2. Für jede endliche Liste von Zahlen gibt es ein Universum U, sodass P genau diese Liste ausgibt, wenn man es in U ausführt.

In $\mathbb{N}$ ausgeführt, wird P nie halten.

In geeigneten Nichtstandardmodellen dagegen wird P nach einer Nichtstandardzahl von Schritten halten.

Mehr dazu steht auf dem Blog der MathOverflow-Legende und Mengentheoretikers Joel David Hamkins.

Ein Rosetta-Stein

Sei M eine Menge natürlicher Zahlen. Dann sind äquivalent:

1. Die Menge M ist **rekursiv aufzählbar**.
2. Es gibt eine Aussageform $A(n, m)$, in der nur beschränkte Quantifikation vorkommt, sodass

$$M = \{n \in \mathbb{N} \mid \text{es gibt } m \in \mathbb{N} \text{ mit } A(n, m)\}.$$

3. Es gibt eine **diophantische Gleichung** „$f(n, x_1, \ldots, x_k) = 0$“ mit

$$M = \{n \in \mathbb{N} \mid \text{es gibt } x_1, \ldots, x_k \in \mathbb{N} \text{ mit } f(n, x_1, \ldots, x_k) = 0\}$$

Eine der Konsequenzen: Es gibt eine diophantische Gleichung, die genau dann eine Lösung hat, wenn PA inkonsistent ist.

Abschnitt III

Zufall als wertvolle Ressource

Abschnitt III

Zufall als wertvolle Ressource

Alice versteckt zwei verschiedene reelle Zahlen in Boxen. Bob darf in eine der Boxen hineinschauen und dann einen Tipp abgeben, welche der Zahlen größer sei.

Es gibt eine **randomisierte Strategie**, mit der Bobs Gewinnwahrscheinlichkeit bei jeder Wahl von x und y mehr als $50\,\%$ beträgt.

Abschnitt III

Zufall als wertvolle Ressource

Alice versteckt zwei verschiedene reelle Zahlen in Boxen. Bob darf in eine der Boxen hineinschauen und dann einen Tipp abgeben, welche der Zahlen größer sei.

Es gibt eine **randomisierte Strategie**, mit der Bobs Gewinnwahrscheinlichkeit bei jeder Wahl von x und y mehr als 50 % beträgt.