First-Order Logic: Theory and Practice

Christoph Benzmüller

Freie Universität Berlin

Block Lecture, WS 2012, October 1-12, 2012

Lügner Paradoxon (Eubulides aus Miletus, 4. Jh. v. Chr.)

Dieser Satz ist falsch. $\underbrace{\text{Dieser Satz}}$ ist falsch.

- Selbstreferenz
- Ist der Satz 'wahr' oder 'falsch'?
- Zusammenhang zu infiniter Rekursion

  ‘Dieser Satz ist falsch’ ist falsch.
  “Dieser Satz ist falsch’ ist falsch’ ist falsch.
  “‘Dieser Satz ist falsch’ ist falsch’ ist falsch’ ist falsch.
  etc.

Gödels Incompleteness Results

Ausdrucksstärke von Logiken versus Berechnungseigenschaften?

- Aussagenlogik

$$\begin{array}{ll} & itRains \wedge isCold \\ \wedge & (itRains \wedge isCold \Rightarrow slipperyRoad) \\ \Rightarrow & slipperyRoad \end{array}$$

- Logik erster Stufe

$$\begin{array}{ll} & isHuman(sokrates) \\ \wedge & (\forall x.isHuman(x) \Rightarrow isMortal(x)) \\ \Rightarrow & isMortal(sokrates) \end{array}$$

- Logik höherer Stufe

$$\begin{array}{ll} & (\forall F.isSurjective(F) \Leftrightarrow \forall y.\exists x.y = F(x)) \\ \Rightarrow & isSurjective(\lambda x.x) \end{array}$$

entscheidbar
unentscheidbar, unvollständig

unentscheidbar, vollständig

Lügner Paradoxon (Eubulides aus Miletus, 4. Jh. v. Chr.)

$\underbrace{\text{Dieser Satz}}$ ist falsch.

- Gödel's Arbeit ist inspiriert durch dieses Paradoxon.

Gödel's Unvollständigkeitssätze

"Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I", Monatshefte für Mathematik, 1931:

Theorem — Erster Unvollständigkeitssatz **1**

Jedes hinreichend mächtige formale System ist entweder widersprüchlich (inkonsistent) oder unvollständig.

Beweisskizze folgt.

Theorem — Zweiter Unvollständigkeitssatz **2**

Jedes hinreichend mächtige konsistente formale System kann die eigene Konsistenz nicht beweisen.

Beweisskizze folgt (Korollar aus 1. Unvollständigkeitssatz).

Beweisführung — eine “intellektuelle Sinfonie” —

1. Satz (Gödelisierung): *Abbildung von Termen, Formeln und Beweisen der PM auf natürliche Zahlen.*
2. Satz (Arithmetisierung der Meta-Mathematik): *Abbildung von Meta-Mathematischen Aussagen auf Eigenschaften von natürlichen Zahlen (bzw. Relationen zwischen natürlichen Zahlen). Diese Eigenschaften (bzw. Relationen) können also selbst wieder in PM kodiert werden.*
3. Satz (Entwicklung des Paradoxon): *Konstruktion einer widersprüchlichen, selbst-referentiellen Aussage und deren Kodierung in PM.*
4. Satz (Das Finale): *Analyse dieser Aussage und Implikationen.*

(Vorlesung beruht auf: E. Nagel, J.R. Newman, Gödel's Proof, NY Univ. Press, 2001)

Was meint Gödel mit hinreichend mächtig?

- umfasst die natürlichen Zahlen
- umfasst alle primitiv rekursiven Funktionen
  - k-stellige Nullfunktion, k-te Projektionen, Nachfolgefunktion
  - Komposition von Funktionen
  - Primitive Rekursion

(Addition und Multiplikation sind primitiv rekursiv)

Die Principia Mathematica (PM) ist ein Beispiel für ein hinreichend mächtiges System. Gödel's Beweis bezieht sich auf PM — ist aber keineswegs eingeschränkt auf PM!

Wichtiges Lemma in Gödel's Arbeit

Lemma (Korrespondenzlemma)

Sei T eine primitiv rekursive wahre Aussage (der Arithmetik) und sei S die Stringrepäsentation von T in der Sprache der PM. Dann ist S ein Theorem in PM (d.h. demonstrierbar/ableitbar in PM).

Beweis: nicht hier.

1. Satz: Gödelisierung

Schritt 1: Definition Gödelnummer Gn

Injektive Abbildung

$$Gn : \text{Terme, Formeln und Beweise in PM} \longrightarrow \mathbb{N}$$

- Terme, Formeln und Beweise der PM werden identifiziert mit Zahlen $n \in \mathbb{N}$.
- Umgekehrt gilt: gewisse Zahlen $n \in \mathbb{N}$ repräsentieren Terme, Formeln und Beweise der PM.

Freie Universität Berlin

Schritt 1(a): Gn für Elementare Zeichen

Symbol	*Gn*		*Symbol*	*Gn*	
$\sim$	1	*not*	s	7	*successor of ...*
$\vee$	2	*or*	(	8	*punctuation mark*
$\supset$	3	*if ... then ...*	)	9	*punctuation mark*
$\exists$	4	*there is an ...*	,	10	*punctuation mark*
$=$	5	*equals*	$+$	11	*plus*
0	6	*zero*	$\times$	12	*times*

Schritt 1(b): Gn für Variablensymbole

numerische Variablen	*Gn*	Beispiel-instanz
x	13	0
y	17	$s0$
z	19	y

Satz-variablen	*Gn*	Beispiel-instanz
p	13^2	$0 = 0$
q	17^2	$(\exists X)(x = y)$
r	19^2	$p \supset q$

Prädikats-variablen	*Gn*	Beispiel-instanz
P	13^3	$x = sy$
Q	17^3	$(x = ss0 \times y)$
R	19^3	$(\exists z)(x = y + sz)$

Schritt 1(c): Kodierung von Formeln am Beispiel

$$
\begin{array}{cccccccccc}
(& \exists & x &) & (& x & = & s & y &) \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
8 & 4 & 13 & 9 & 8 & 13 & 5 & 7 & 17 & 9 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
\end{array}
$$

$$m = 2^8 \times 3^4 \times 5^{13} \times 7^9 \times 11^8 \times 13^{13} \times 17^5 \times 19^7 \times 23^{17} \times 29^9$$

Das ist noch kein $n \in \mathbb{N}$ — es fehlt die Verknüpfung.

Primzahlen in aufsteigender Reihenfolge

Das k-te Symbol der Zeichenkette wird abgebildet auf

$(k\text{-te Primzahl})^{\mathrm{Gn}(k\text{-tes Symbol})}$

1. Satz: Gödelisierung

Schritt 1(d): Kodierung von Formelsequenzen und Beweisen

$$\begin{array}{lcl} (\exists x)(x = sy) & \longrightarrow & m \\ ------- & & & \longrightarrow \quad 2^m \times 3^n \\ (\exists x)(x = s0) & \longrightarrow & n \end{array}$$

Primzahlen in aufsteigender Reihenfolge

1. Satz: Gödelisierung

Beobachtung: Die Abbildung *Gn* ist nicht surjektiv (nicht jede Zahl $n \in \mathbb{N}$ ist Gödelnummer einer Zeichenkette).

Beispiel: 100

- Gn eines elementaren Symbols? Nein, da $100 > 12$.
- Gn einer num. Variablen? Nein, ungleich zu 13, 17, 19.
- Gn einer Satzvariablen? Nein, ungleich zu 13^2, 17^2, 19^2.
- Gn einer Prädikatsvariablen? Nein, ungleich zu 13^3, 17^3, 19^3.
- kanonische Primfaktorzerlegung: $100 = 2^2 \times 5^2$
  3 fehlt als Primfaktor, deshalb kann 100 keine Gn sein (für einen Term, Formel, Formelsequenz)

Freie Universität Berlin

Theorem 3

Sei $n \in \mathbb{N}$. Entweder ist n keine Gödelnummer oder es existiert eine eindeutige Zeichenkette Z (der PM), so dass $n = Gn(Z)$.

Proof.

Verwendet Fundamentalsatz der Arithmetik (kanonische Primfaktorzerlegung). $\square$

Beispiel:

Dekodierung

$$\begin{array}{ccc} & 243.000.000 & \\ 64 & \times\ 243\ \times & 15.625 \\ 2^6 & \times\ 3^5\ \times & 5^6 \\ 6 & 5 & 6 \\ \downarrow & \downarrow & \downarrow \\ 0 & = & 0 \end{array}$$

Kodierung

1. Satz: Gödelisierung

Zusammenfassung 1. Satz

Jedem Term, jeder Formel, und jedem Beweis in der Sprache der PM kann eine eindeutige Gödelnummer zugeordnet werden. Diese Abbildungsfunktion, sowie ihre Inverse, sind berechenbar.

2. Satz: Arithmetisierung der Meta-Mathematik

Beobachtung

- Terme T, Formeln F und Beweise B der PM korrespondieren also zu bestimmten Zahlen $n \in \mathbb{N}$ (und umgekehrt).
- Damit können wir aber noch nicht *über* T, F oder B reden in der Arithmetik. Dies ist aber das Ziel von Gödel.

Schritt 2: Kodierung von Meta-Mathematischen Aussagen

Aussagen *über* die Struktur von Termen, Formeln und Beweisen (in PM) können als arithmetische Formeln kodiert werden.

2. Satz: Arithmetisierung der Meta-Mathematik

Beispielformel (in PM): $\sim (0 = 0)$

Aussage: "Das erste Symbol dieser Formel ist die Tilde (Negation)."

$$a = Gn('\!\sim (0 = 0)') \quad = \quad 2^1 \times 3^8 \times 5^6 \times 7^5 \times 11^6 \times 13^9$$

Das erste Symbol ... ist eine Tilde (Negation).

$$(\exists z)(a = 2 \times z) \wedge \sim (\exists z)(a = (2 \times 2) \times z)$$

$$\overbrace{ss \ldots s0}$$

$$\overbrace{ss0}$$

2. Satz: Arithmetisierung der Meta-Mathematik

Beispielformel (in PM): $\sim (0 = 0)$

Aussage: "Das erste Symbol dieser Formel ist die Tilde (Negation)."

Kodierung (in PM) als Formel S:

$$(\exists z)(\underbrace{ss\ldots s0}_{a} = z \times \underbrace{ss0}_{2}) \wedge \ \sim (\exists z)(\underbrace{ss\ldots s0}_{a} = z \times (\underbrace{ss0}_{2} \times \underbrace{ss0}_{2}))$$

Diese Aussage ist eine 'primitiv rekursive Wahrheit'.

Anwendung Korrespondenzlemma:

Die Formel S ist demonstrierbar/ableitbar in PM!

2. Satz: Arithmetisierung der Meta-Mathematik

Zusammenfassung 2. Satz

Wir können über typographische und strukturelle Eigenschaften von Formeln der PM indirekt (aber präzise) reden, indem wir über Eigenschaften von Primfaktorzerlegungen reden. Dies können wir wiederum in der Sprache der PM tun.

3. Satz: Entwicklung des Paradoxon

Wir betrachten nun folgende Meta-Mathematische Aussage:
"Die Formelsequenz mit Gödelnummer x ist ein Beweis (in PM) für die Formel mit Gödelnummer y."

- Diese Aussage ist (im Sinne der Arithmetisierung der Meta-Mathematik) abbildbar auf eine numerische Beziehung zwischen den Zahlen x und y. Diese Beziehung bezeichnen wir mit $dem(x, y)$ — für y demonstriert x
(Bemerkung: Diese Beziehung ist abhängig von PM selbst.)
- Man kann zeigen:
  - Relation $dem(x, y)$ ist primitiv rekursiv.
  - Zu $dem(x, y)$ gibt es Stringrepräsentation $DEM(x, y)$ in PM.
- Aus dem Korrespondenzlemma folgt:
Falls $dem(x, y)$ gilt, dann ist $DEM(x, y)$ ein Theorem in PM.
Falls $\sim dem(x, y)$ gilt, dann ist $\sim DEM(x, y)$ Theorem in PM.

3. Satz: Entwicklung des Paradoxon

Was sagt uns das?

Meta-Mathematische Aussagen wie "das-und-das demonstriert dies-und-dies nach den Regeln der PM" (bzw. "das-und-das demonstriert dies-und-dies nicht in PM") werden wiederum reflektiert durch Theoreme von PM.

— PM kann über sich selbst reden! —

3. Satz: Entwicklung des Paradoxon

Noch ein Wort zu Substitutionen. Wir betrachten dazu die folgende Beispielformel mit der freien Variablen y:

$$(\exists x)(x = sy)$$

Diese Formel hat Gödelnummer m (siehe vorher).

Substitution von m (in PM Stringrepräsentation) für y liefert

$$(\exists x)(x = s\,\underbrace{ss\ldots s0}_{m})$$

Diese Formel hat wiederum eine (sehr grosse) Gödelnummer r.

3. Satz: Entwicklung des Paradoxon

Die Substitution korrespondiert zu einer arithmetischen Funktion *sub* (beachte: y hat Gödelnummer 17)

$$r = sub(m, 17, m)$$

Lese: "Die PM Formel mit Gödelnummer r ist das Resultat der Substitution aller Vorkommen der Variablen y in der PM Formel mit Gödelnummer m durch (die PM Stringrepräsentation) von m."

Man kann zeigen:

- $sub(x, 17, x)$ ist eine primitive rekursive arithmetische Funktion
- zu $sub(x, 17, x)$ gibt es wiederum eine korrespondierende Stringrepräsentation $SUB(x, 17, x)$ in PM

4. Satz: Das Finale

Gödel's Vorgehen:

- **A** Konstruiert PM Formel G für Meta-Mathematische Aussage: "Die Formel G is nicht demonstrierbar in PM"
- **B** Zeigt: G demonstrierbar gdw. $\sim G$ demonstrierbar. Also: Falls PM konsistent, dann ist G nicht demonstrierbar.

  Hinweis: Das ist eine Vereinfachung der ursprünglichen Argumentation von Gödel; dieses stärkere Resultat wurde von Barkley und Rosser 1936 gezeigt
- **C** Zeigt: Obwohl G nicht demonstrierbar ist in PM, so ist die durch G beschriebene arithmetische Eigenschaft dennoch wahr.
- **D** Verknüpft B und C: PM muss unvollständig sein, weil G wahr ist, aber nicht demonstrierbar. (Erster Unvollständigkeitssatz)
- **E** Konstruiert PM Formel A für Aussage: "PM ist konsistent" Konstruiert PM Formel $A \supset G$ und zeigt Demonstrierbarkeit in PM.

  Argumentiert: Annahme A demonstrierbar, dann auch G

4. Satz: Das Finale

Mehr Details zu

A Konstruiert PM Formel G für Meta-Mathematische Aussage:
"Die Formel G is nicht demonstrierbar in PM"

- Wir kennen bereits die PM Formel $DEM(x, z)$:
"Die Formelsequenz mit Gödelnummer x ist ein Beweis (in PM) für die Formel mit Gödelnummer z."
- $(\exists x) DEM(x, z)$:
"Die Formel mit Gödelnummer z ist demonstrierbar."
- $\sim (\exists x) DEM(x, z)$:
"Die Formel mit Gödelnummer z ist nicht demonstrierbar"
- Wir bilden nun eine sehr geschickt gewählte Instanz dieser Formel!

4. Satz: Das Finale

Mehr Details zu   Aussage ist noch nicht definit!

A Konstruiert PM Formel G für Meta-Mathematische Aussage: "Die Formel G is nicht demonstrierbar (in PM)"

- $\sim (\exists x) DEM(x, SUB(y, 17, y))$
  "Die Formel mit Gödelnummer $sub(y, 17, y)$ ist nicht demonstrierbar."
- Sei nun n die Gödelnummer obiger Formel
- Bilde dann Formel G: $\sim (\exists x) DEM(x, SUB(n, 17, n))$
  "Die Formel mit Gödelnummer $sub(n, 17, n)$ ist nicht demonstrierbar."
- G ist definit (keine freien Variablen); G hat Gödelnummer g
- Es gilt: $g = sub(n, 17, n)$
- Lese also G als:
  "Die Formel mit Gödelnummer g ist nicht demonstrierbar."
  "Die Formel G ist nicht demonstrierbar."

4. Satz: Das Finale

Mehr Details zu

B Zeigt: G demonstrierbar gdw. $\sim G$ demonstrierbar.
Also: Falls PM konsistent, dann ist G nicht demonstrierbar.

- Annahme G, d.h. $\sim (\exists x) DEM(x, SUB(n, 17, n))$, demonstrierbar in PM.
- Dann: Die Meta-Mathematische Aussage “Es existiert eine Demonstration von G in PM” ist wahr.
- Dann: $(\exists x) DEM(x, SUB(n, 17, n))$ demonstrierbar in PM. Widerspruch zur Annahme der Konsistenz von PM.
- Annahme: $(\exists x) DEM(x, SUB(n, 17, n))$ demonstrierbar in PM.
- Dann: G, d.h. $\sim (\exists x) DEM(x, SUB(n, 17, n))$, demonstrierbar in PM. Widerspruch zur Annahme der Konsistenz von PM.

4. Satz: Das Finale

Gödel's Vorgehen:

A Konstruiert PM Formel G für Meta-Mathematische Aussage: "Die Formel G is nicht demonstrierbar in PM"

B Zeigt: G demonstrierbar gdw. $\sim G$ demonstrierbar.
Also: Falls PM konsistent, dann ist G nicht demonstrierbar.

Hinweis: Das ist eine Vereinfachung der ursprünglichen Argumentation von Gödel; dieses stärkere Resultat wurde von Barkley und Rosser 1936 gezeigt

C Zeigt: Obwohl G nicht demonstrierbar ist in PM, so ist die durch G beschriebene arithmetische Eigenschaft dennoch wahr.

D Verknüpft B und C: PM muss unvollständig sein, weil G wahr ist, aber nicht demonstrierbar. (Erster Unvollständigkeitssatz)

E Konstruiert PM Formel A für Aussage: "PM ist konsistent"
Konstruiert PM Formel $A \supset G$ und zeigt Demonstrierbarkeit in PM.
Argumentiert: Annahme A demonstrierbar, dann auch G

Diskussion

David Hilbert
(1862-1943)

Hilbert's twenty-three problems are:

Problem	Brief explanation
1st	The continuum hypothesis (that is, there is no set whose cardinality is strictly between that of the integers and that of the real numbers)
2nd	Prove that the axioms of arithmetic are consistent.
3rd	Given any two polyhedra of equal volume, is it always possible to cut the first into finitely many polyhedral pieces which can be reassembled to yield the second?
4th	Construct all metrics where lines are geodesics.

23 Probleme (1900)

- Einflussreichster Mathematiker seiner Zeit, breites Arbeitsspektrum
- Grundlagen der Geometrie (1899)
- Hilbert's Programm – Logische Fundierung der Mathematik
  - 1900–1917: Formuliert Programm; gewinnt Mitstreiter
  - 1917–1930: Vorlesungen mit Bernays und Behmann (1917-1921), Logik 1. Stufe, Arbeit am Programm (inkl. Widerspruchsfreiheit der Arithmetik), Lehrbuch Grundzüge der theoretischen Logik (1928, mit Ackermann)
  - nach 1931: Moderne Beweistheorie