Gödel's Proof

Victoria Gitman

City University of New York

vgitman@nylogic.org
http://websupport1.citytech.cuny.edu/faculty/vgitman

January 20, 2010

Mathematical Epistemology

Mathematics, as opposed to other sciences, uses proofs instead of observations.

- a proof is a sequence of statements that follows the rules of logical inference

  (1) "If it is Christmas, then Victoria has a day off." ($A \to B$)
  (2) "It is Christmas." (A)

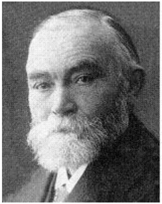
  Conclusion: "Victoria has a day off." (B) (Modus Ponens)

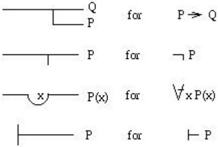
  (1) "Every organism can reproduce." ($\forall x \; A(x) \to B(x)$)
  (2) "A bacteria is an organism." (A(bacteria))

  Conclusion: "A bacteria can reproduce." (B(bacteria))

- impossible to prove all mathematical laws
- certain first laws, axioms, are accepted without proof
- the remaining laws, theorems, are proved from axioms
- How do we choose reasonable axioms? Non-contradictory axioms? Powerful axioms?
- Do the axioms suffice to prove every true statement?

Gottlob Frege (1848-1925)





Frege

- invents predicate logic: introduces symbolism, rules
- jump starts a return to *formal mathematics* of Euclid
- attempts to axiomatize the theory of sets
  (sets are the building blocks of all mathematical objects!)
- runs into trouble with his set building axiom

Frege's Set Building Axiom

"For any formal criterion, there exists a set whose members are those objects (and only those objects) that satisfy the criterion."

Frege's axioms allows us to build various sets:

- the set $\mathbb{N} = \{x : x \text{ is a natural number}\}$
- the set $\mathbb{R} = \{x : x \text{ is a real number}\}$
- the set $\mathbb{I} = \{x : x \text{ is an infinite set}\}$
- the set of all sets, $\mathbb{V} = \{x : x = x\}$

Key Observation: some sets are members of themselves, while others are not!

Examples: $\mathbb{N} \notin \mathbb{N}$, $\mathbb{R} \notin \mathbb{R}$, $\mathbb{I} \in \mathbb{I}$, $\mathbb{V} \in \mathbb{V}$

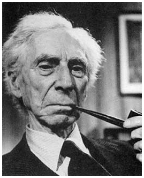
Consider the set $\mathbb{B}$ of all sets that are not members of themselves:

$$\mathbb{B} = \{x : x \notin x\}$$

Something is terribly wrong with $\mathbb{B}$!

Russell's Paradox (1901)

Bertrand Russell (1872-1970)
discovers that Frege's axioms lead to a contradiction:



$$\mathbb{B} = \{x : x \notin x\}$$

$$\mathbb{B} \in \mathbb{B} \Leftrightarrow \mathbb{B} \notin \mathbb{B}$$

Key idea: Definition of $\mathbb{B}$ exploits self-reference allowed by the Set Building Axiom!

Spoiler Alert: This idea shows up again in the proof of Gödel's theorem!

- Russell fixed Frege's system in Principia Mathematica using type theory.
- This led to the Comprehension Axiom in Zermelo-Fraenkel set theory.

Beware of self-reference:
Proof that either Tweedledum or Tweedledee exists

(1) TWEEDLEDUM DOES NOT EXIST
(2) TWEEDLEDEE DOES NOT EXIST
(3) AT LEAST ONE SENTENCE IN THIS BOX IS FALSE

hint: sentence (3) must be either TRUE or FALSE

Formal Mathematics and Meta-mathematics

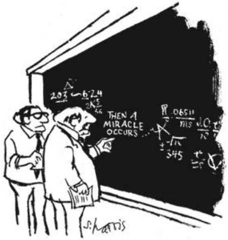
The 19th century work of Frege, Russell, Hilbert, Peano, Cantor, etc. leads to development of:

Formal Mathematics

- A formal language based on predicate logic
- Axioms explicitly stated
- Proofs are logical inferences from axioms

Meta-mathematics: debating the ground rules

- What is a formal language?
- What are logical inferences?
- Are the axioms non-contradictory?
- Are the axioms sufficient to prove all true statements?



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Hilbert's Program (1921): setting the ground rules

David Hilbert (1862-1943) aimed to provide a secure foundation for mathematics.

Two Key Questions

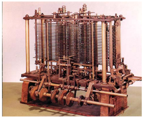
Consistency: How do we know that contradictory consequences cannot be proved from the axioms?

Completeness: How do we know that all true statements follow from the axioms?

Hilbert's Program:

Translate all mathematics into a formal language and demonstrate "by finitary means" that

- Peano Axioms (PA) for Number Theory
- Zermelo-Fraenkel (ZF) Axioms for Set Theory
- Euclidian Axioms for Geometry
- Principia Mathematica Axioms



are consistent and complete!

"finitary means"? think of running a computer program to verify it...

Primer in Formal Languages: the alphabet

1) Logical symbols:
   - Equality: =
   - Boolean connectives: $\vee$, $\wedge$, $\neg$, $\rightarrow$
   - Quantifiers: $\exists$, $\forall$
2) Functions, relations, and constants symbols: specific to subject
   - Number Theory: $+$, $\cdot$, $<$, 0, 1
   - Set Theory: $\in$
   - Group Theory: $\circ$, $^{-1}$, e
3) Variables:
   $x_1, x_2, x_3, x_4, \ldots$ infinitely many!
4) Punctuation symbols:
   (,)

For notational convenience, we will write $x, y, z, \ldots$ instead of $x_1, x_2, x_3, \ldots$

Writing Formal Mathematics: the syntax

Syntactically correct mathematical statements are called formulas

Formulas in Number Theory

- x is even: $\text{even}(x) := \exists y\ y + y = x$
- 3 is even: $\exists y\ y + y = (1 + 1) + 1$
- x divides y: $x|y := \exists z\ z \cdot x = y$
- x is prime: $\text{prime}(x) := (\forall y\ (y|x \rightarrow (y = 1 \vee y = x)) \wedge \neg x = 1)$
- $3^x = y$: suggestions? (problem: the operation is recursive)
- $x! = y$: (same problem!)
- There are infinitely many primes: $\forall x \exists y\ (y > x \wedge \text{prime}(y))$
- Every even number > 2 is a sum of two primes:
  $\forall x\ ((x > 1 + 1 \wedge \text{even}(x)) \rightarrow \exists y \exists z\ ((\text{prime}(y) \wedge \text{prime}(z)) \wedge x = y + z)))$
  (Goldbach Conjecture)

Formulas (continued...)

How do we determine whether something is a formula?

This string is a formula: (why?)

$\exists z(z > 0 \wedge x + y = z)$

This string is not a formula: (why not?)

$\forall x(y \wedge \forall z\ z > 0)$

A formula is a string of symbols built according to a finite set of simple rules.

A computer should be able to verify whether a string of symbols is a formula! (Remember Hilbert?)

What are the rules?

"Mathematics is a game played according to certain simple rules with meaningless marks on paper." ....Hilbert

Formula Witnessing Sequences

Recursive rules for building formulas:

- 'Equality' statements are formulas: $x = y$, $x + y = z \cdot z$
- 'Less than' statements are formulas: $x + 1 < z$
- Boolean combinations of formulas are formulas: if φ and ψ are formulas, then so are $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$, $(\varphi \rightarrow \psi)$.
- A formula with a quantifier-variable pair attached in front is a formula: if i is any natural number and φ is a formula and , then so are $\exists x_i\ \varphi$, $\forall x_i\ \varphi$.
- Nothing else is a formula

$\forall x((x > 0 \wedge y + x = z) \rightarrow \exists z\ y + z > 1 + 1)$

A formula witnessing sequence:

(1) $y + z > 1 + 1$,
(2) $\exists z\ y + z > 1 + 1$,
(3) $x > 0$, $y + x = z$,
(4) $(x > 0 \wedge y + x = z)$,
(5) $(x > 0 \wedge y + x = z) \rightarrow \exists z\ y + z > 1 + 1$,
(6) $\forall x((x > 0 \wedge y + x = z) \rightarrow \exists z\ y + z > 1 + 1)$

A computer program can verify whether a given string is a formula!

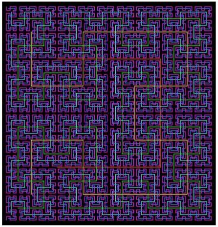
The Peano Axioms

Axiomatization of Number Theory proposed by Giuseppe Peano (1858-1932).

Peano Axioms

Addition and Multiplication

- $\forall x \forall y \forall z\ (x + y) + z = x + (y + z)$ (associativity of addition)
- $\forall x \forall y\ x + y = y + x$ (commutativity of addition)
- $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $\forall x \forall y\ x \cdot y = y \cdot x$ (commutativity of multiplication)
- $\forall x \forall y \forall z\ x \cdot (y + z) = x \cdot y + x \cdot z.$ (distributive law)
- $\forall x\ (x + 0 = x \wedge x \cdot 1 = x)$ (additive and multiplicative identity)



Peano Axioms (continued)

Order

- $\forall x \forall y \forall z\ ((x < y \wedge y < z) \rightarrow x < z)$ (the order is transitive)
- $\forall x\ \neg x < x$ (the order is anti-reflexive)
- $\forall x \forall y\ ((x < y \vee x = y) \vee y < x)$ (any two elements are comparable)
- $\forall x \forall y \forall z\ (x < y \rightarrow x + z < y + z)$ (order respects addition)
- $\forall x \forall y \forall z\ ((0 < z \wedge x < y) \rightarrow x \cdot z < x \cdot z)$ (order respects multiplication)
- $\forall x \forall y\ (x < y \leftrightarrow \exists z\ (z > 0 \wedge x + z = y))$
- $\forall x\ (x \geq 0 \wedge (x > 0 \rightarrow x \geq 1))$ (the order is discrete)

Induction Scheme

For every formula $\varphi(x)$ we have

- $(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(x+1))) \rightarrow \forall x \varphi(x)$

Hilbert: "Are the Peano Axioms consistent? Are they complete?"

Sensible Mathematician: "Duh, the Peano Axioms are consistent because the natural numbers satisfy them!"

Hilbert: "You checked all infinitely many of them?"

The Group Theory Axioms: An Easy Example

Language: $\circ$, $^{-1}$, e

Group Theory Axioms

- $\forall x \forall y \forall z \; x \circ (y \circ z) = (x \circ y) \circ z$ (associativity)
- $\forall x \; (e \circ x = x \wedge x \circ e = x)$ (e is the identity)
- $\forall x \; x \circ x^{-1} = e$ ($^{-1}$ is the inverse)

Are the Group Theory Axioms consistent? Are they complete?

$\mathbb{Z}_4$:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

S_3:

$\circ$	e	s	w	t	u	v
e	e	s	w	t	u	v
s	s	w	e	v	t	u
w	w	e	s	u	v	t
t	t	u	v	e	s	w
u	u	v	t	w	e	s
v	v	t	u	s	w	e

Presburger Arithmetic

Arithmetic without multiplication:

Presburger Axioms

Addition

- $\forall x \; \neg 0 = x + 1$
- $\forall x \forall y \; (x + 1 = y + 1 \rightarrow x = y)$
- $\forall x \; x + 0 = x$
- $\forall x \forall y \; (x + y) + 1 = x + (y + 1)$

Induction Scheme

For every formula $\varphi(x)$ we have

- $(\varphi(0) \wedge \forall x \; (\varphi(x) \rightarrow \varphi(x + 1))) \rightarrow \forall x \varphi(x)$

Mojzesz Presburger (1904-1943) showed in 1929 using finitary arguments that Presburger Arithmetic is consistent and complete!

A computer program that can decide whether any statement of Presburger Arithmetic is TRUE or FALSE!

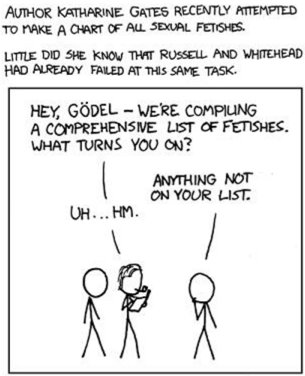
Gödel ends Hilbert's Program

Theorem (Gödel, 1931)

The Peano Axioms are not complete. In fact, any "reasonable" collection of axioms for Number Theory or Set Theory is necessarily incomplete.

Theorem (Gödel, 1931)

No proof of the consistency of the Peano Axioms can be given by "finitary means".



Richard's Paradox (1905)

Mathematics vs. Meta-mathematics: how not to mix apples and oranges!

Jules Richard (1862-1956) considered all English language expressions that unambiguously define a property of numbers.

- x is even
- x is prime
- x is a number above which Goldbach Conjecture fails.
- x is a number definable using prime many characters.

Each definition $\varphi(x)$ can be assigned a unique number code $\ulcorner\varphi(x)\urcorner$.
For example, using ASCII codes, we get:

$\ulcorner x \text{ is even}\urcorner = 120032105115101118101110$
$\ulcorner x \text{ is prime}\urcorner = 1200321051150321121141051091 01$

- $\ulcorner x \text{ is even}\urcorner$ is even
- $\ulcorner x \text{ is prime}\urcorner$ is not prime

For a definition $\varphi(x)$, it may be that $\varphi(\ulcorner\varphi(x)\urcorner)$ is true, or not!

Spoiler Alert: Russell is back!

Richard's Paradox (continued...)

Call a number n *ordinary* if:

- $n = \ulcorner \varphi(x) \urcorner$ for some formula $\varphi(x)$
- $\varphi(\ulcorner \varphi(x) \urcorner)$ is not true.

This is one of Richard's definitions!

Let m be the code of the formula "$\varphi(x) =$ x is ordinary", i.e. $m = \ulcorner \varphi(x) \urcorner$.

Here comes trouble:

m is ordinary $\Leftrightarrow$ m is not ordinary!

Richard's Paradox: the morals

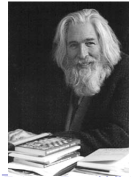
Linguistic concept of property does not distinguish between mathematical and meta-mathematical definitions:

- "x is prime" - mathematical
- "x is a number definable using prime many characters" - meta-mathematical
- "x is ordinary" - meta-mathematical

Some meta-mathematical statements incorporate infinitely many other "super complicated mathematical statements" whose truth or falseness cannot be decided uniformly!

"Everything is vague to a degree you do not realize till you have tried to make it precise."
....Russell

"Some people are always critical of vague statements. I tend rather to be critical of precise statements; they are the only ones which can correctly be labeled 'wrong'."



....Smullyan

Coding Meta-mathematics into Mathematics

Gödel observed that meta-mathematical properties can be coded as statements in the formal language of Number Theory!

Assign a unique natural number to each symbol:

$=$	$\vee$	$\wedge$	$\neg$	$\rightarrow$	$\forall$	$\exists$	$+$	$\cdot$	$<$	0	1	(	)
1	3	5	7	9	11	13	15	17	19	21	23	25	27

x_0	x_1	x_2	$x_3 \ldots$
0	2	4	6

A finite sequences of numbers can be coded by a single number: (think of your favorite coding!)

- Formulas can be coded by numbers
- Proofs can be coded by numbers

Problems:

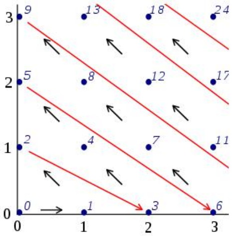
- We need a coding that can be expressed in the formal language of number theory.
- Most codings you can think of need exponentiation.
- To express exponentiation formally we need coding!

Coding in Number Theory: Pairing Function

Cantor's Pairing Function:

A simple coding of two numbers as a single number.

$$\langle x, y\rangle = \frac{(x+y)(x+y+1)}{2} + y$$



Example: the code of the pair 2 and 3.

$\langle 2, 3\rangle = \underline{\qquad}$

Formula defining the coding:

$z = \langle x, y\rangle$:

$\exists w\ (2 \cdot w = (x+y) \cdot ((x+y)+1) \wedge z = w + y)$

Coding in Number Theory: Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Suppose $a_1, \ldots, a_k$ are natural numbers, then there are natural numbers b and m such that

$$a_1 \text{ is the remainder of } \frac{b}{m+1}$$
$$a_2 \text{ is the remainder of } \frac{b}{2m+1}$$
$$\vdots$$
$$a_k \text{ is the remainder of } \frac{b}{km+1}$$

The number $\langle b, m\rangle$ codes the sequence $a_1, \ldots, a_k$!

Example: The sequence $\langle 6, 0, 9, 1\rangle$ is coded by the number 710 (why?)

- $710 = \langle 30, 7\rangle$
- No exponentiation is needed.
- There are infinitely many other numbers coding the same sequence!

Coding in Number Theory: Examples

Using this coding:

- Every finite sequence of numbers is coded by a single number.
- Every number codes some sequence of numbers.

Question: What is a 5 element sequence coded by the number 2424?

- $2424 = \langle 60, 9 \rangle$
- $(2424)_1 = 0 \quad (2424)_2 = 3 \quad (2424)_3 = 4 \quad (2424)_4 = 23 \quad (2424)_5 = 14$

Formula defining the coding:

$(s)_i = z$:

$\exists b \exists m\ (s = \langle b, m \rangle \wedge z$ is the remainder of $\frac{b}{i \cdot m + 1})$

Example: $x^y = z$:

$\exists s\ ((s)_1 = x \wedge (\forall n\ (n < y \rightarrow (s)_{n+1} = (s)_n \cdot x) \wedge (s)_y = z))$

Being a Formula is Expressible

Many meta-mathematical statements that can now be expressed in the language of Number Theory:

symbol(x):

$(\text{even}(x) \vee x < 28)$

formula(x):

$\exists s \exists n$

- $(s)_n = x$ AND
- $\forall i \; i < (n+1) \rightarrow$
  - $(s)_i$ "is the code of an equality or less than formula" OR
  - $\exists j \exists k \; (j < i \wedge k < i \wedge (s)_i$ "is the code of a boolean combination of $(s)_j$ and $(s)_k$") OR
  - $\exists j \; (j < i \wedge (s)_i$ "is the code of quantifier variable pair concatenated with $(s)_j$").

Provability from PA is Expressible

PeanoAxioms(x):

- $x = n_1 \vee x = n_2 \vee \cdots \vee x = n_{13}$ OR
- $\exists y$ (formula(y) $\wedge$ x "codes an induction axiom for the formula coded by y")

proofPA(x,s):

"s codes the proof of the formula coded by x from PA."

provablePA(x):

$\exists s$ "s codes the proof of the formula coded by x from PA."

- This is much more general than PA.
- The ability to code sequences into the mathematical objects is key.
- Provability is expressible for any expressible collection of axioms!
- "Reasonable axioms" $\Rightarrow$ expressible axioms.

Is Truth Expressible?

Big Question:
Can we write a formula true(x)
that is true exactly when x codes a true formula???

Russell's Paradox

Liar Paradox

Richard's Paradox

Truth is not Expressible (as expected!): The resolution of Richard's Paradox

Suppose there is a formula true(x).

Call a number n ordinary if:

- $n = \ulcorner\varphi(x)\urcorner$ for some formula $\varphi(x)$
- $\neg$true($\varphi(\ulcorner\varphi(x)\urcorner)$)

Then there is a formula ordinary(n):

(formula(n) $\wedge$ ($\exists y$ (formula(y)) $\wedge$ "$y = \ulcorner\varphi(n)\urcorner$" $\wedge$ $\neg$true(y)))

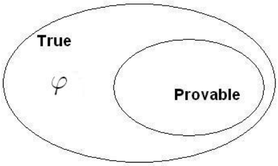
Let $m = \ulcorner$ordinary(x)$\urcorner$

Question: What is the problem?

Proof of the First Incompleteness Theorem

- Provability is expressible!
- Truth is not expressible!
- Provable is a subset of True!

Conclusion: There is a true statement that cannot be proved from PA!



Goodstein Sequences

Hereditary base n notation

Example: Write 3003 in hereditary base 3 notation.

- $3003 = 3^7 + 3^6 + 3^4 + 2 \cdot 3^1$
- $3003 = 3^7 + 3^6 + 3^4 + 3^1 + 3^1$
- $3003 = 3^{2 \cdot 3+1} + 3^{2 \cdot 3} + 3^{3+1} + 3^1 + 3^1$
- $3003 = 3^{3+3+1} + 3^{3+3} + 3^{3+1} + 3^1 + 3^1$

Goodstein Sequence $G(m)$ for a number m:

- First element: m.
- Second element: write m in hereditary base 2 notation, replace all 2's by 3's and subtract 1.
- Third element: write second element in hereditary base 3 notation, replace all 3's by 4's and subtract 1.
- etc.

Examples of Goodstein Sequences

$G(3)$: $3, 3, 3, 2, 1, 0$

value	base	expression	rep. base	expression	subtract	value
3	2	$2^1 + 1$	3	$3^1 + 1$	4-1	3
3	3	3^1	4	4^1	4-1	3
3	4	$1 + 1 + 1$	5	$1 + 1 + 1$	$3 - 1$	2
2	5	$1 + 1$	6	$1 + 1$	$2 - 1$	1
1	6	1	7	1	$1 - 1$	0

$G(4)$: $4, 26, 41, 60, 83, 109, \ldots$

value	base	expression	rep. base	expression	subtract	value
4	2	2^2	3	3^3	27-1	26
26	3	$3^{1+1} + 3^{1+1} + 3 + 3 + 1 + 1$	4	$4^{1+1} + 4^{1+1} + 4 + 4 + 1 + 1$	42-1	41
41	4	$4^{1+1} + 4^{1+1} + 4 + 4 + 1$	5	$5^{1+1} + 5^{1+1} + 5 + 5 + 1$	$61 - 1$	60
60	5	$5^{1+1} + 5^{1+1} + 5 + 5$	6	$6^{1+1} + 6^{1+1} + 6 + 6$	$84 - 1$	83
83	6	$6^{1+1} + 6^{1+1} + 6 + 1 + 1 + 1 + 1 + 1$	7	$7^{1+1} + 7^{1+1} + 7 + 1 + 1 + 1 + 1 + 1$	$110 - 1$	109

Elements of G(4) continue to increase for a while, but at base $3 \cdot 2^{402653209}$, they reach a maximum of $3 \cdot 2^{402653210} - 1$, stay there for the next $3 \cdot 2^{402653209}$ steps, then begin their first and final descent to 0!

Goodstein's Theorem: A True but Unprovable Statement

Theorem (Goodstein, 1944)

For every m, the sequence $G(m)$ is eventually 0!

Theorem (Kirby-Paris, 1982)

Goodstein's Theorem cannot be proved from PA.

So what is it a theorem of??? Zermelo-Fraenkel Set Theory.