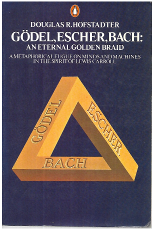
Perlen der Informatik I

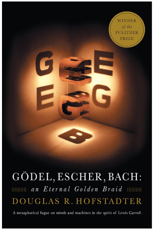
Jan Křetínský

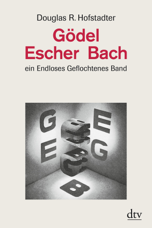
Technische Universität München
Winter 2021/2022

Overview

- language: English/German
- voluntary course
- lecture on Tuesday, in the slot 12 p.m. – 2 p.m.
- `https://www7.in.tum.de/~kretinsk/teaching/perlen.html`
- Gödel, Escher, Bach: an Eternal Golden Braid
  by Douglas R. Hofstadter







Bach

- Frederick the Great
- Leonhard Euler,. . . , J.S. Bach
- improvised 6-part fugue
- canons

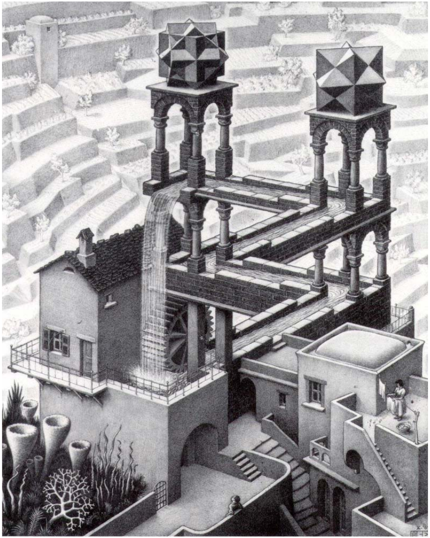
Bach

- Frederick the Great
- Leonhard Euler,. . . , J.S. Bach
- improvised 6-part fugue
- canons

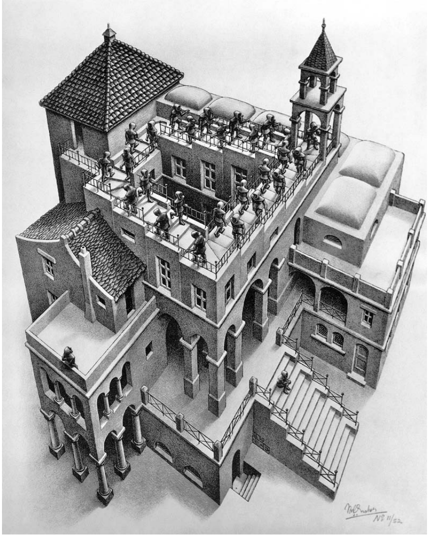
Bach

- Frederick the Great
- Leonhard Euler,. . . , J.S. Bach
- improvised 6-part fugue
- canons
  - copies differing in time, pitch, speed, direction (upside down, crab)
  - isomorphic
  - canon endlessly rising in 6 steps – “strange loop”

Escher



“Waterfall”
6-step endlessly falling loop

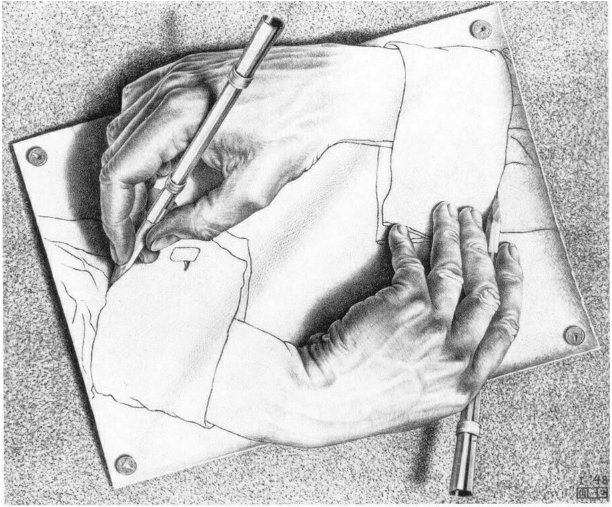


“Ascending and Descending”
illusion by Roger Penrose

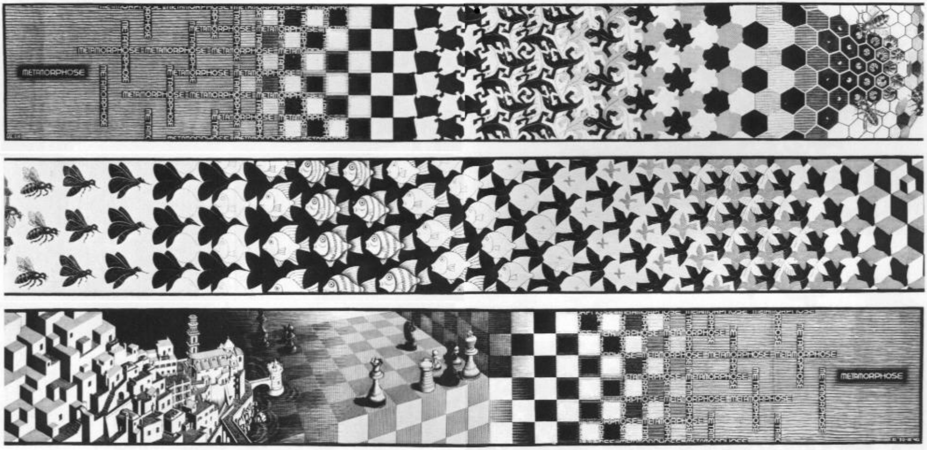
Escher

Penrose triangle
Faculty of Informatics, Brno

Escher



“Drawing hands”
his first strange loop



“Metamorphosis”
copies of one theme

Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”

Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.
- strange loop in the proof

Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.
- strange loop in the proof
- statement about numbers can talk about itself
  “This statement of number theory does not have any proof”

Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.
- strange loop in the proof
- statement about numbers can talk about itself
  “This statement of number theory does not have any proof”
- numbers $\overset{code}{\leftrightarrow}$ statements

Gödel

- Brno
- Epimenides paradox: "All Cretans are liars"
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.
- strange loop in the proof
- statement about numbers can talk about itself
  "This statement of number theory does not have any proof"
- numbers $\overset{code}{\leftrightarrow}$ statements
  215473077557

Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.

- strange loop in the proof
- statement about numbers can talk about itself
  “This statement of number theory does not have any proof”
- numbers $\overset{\textit{code}}{\leftrightarrow}$ statements
  215473077557 is in binary
  0011001000101011001100100011110100110101

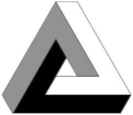
Gödel

- Brno
- Epimenides paradox: “All Cretans are liars”
- mathematical reasoning in exploring mathematical reasoning
- Incompleteness theorem:

  All consistent axiomatic formulations of number theory include undecidable propositions.
- strange loop in the proof
- statement about numbers can talk about itself
  “This statement of number theory does not have any proof”
- numbers $\overset{code}{\leftrightarrow}$ statements
  215473077557 is in binary
  0011001000101011001100100011110100110101 read as ASCII
  2+2=5
- homework:

34723379178930453204433293597543819411782291432109326918654063662

- different geometries, equally valid
- real world?
- proof?
- Russel's paradox
  - "ordinary" sets: $x \notin x$
  - "self-swallowing" sets: $x \in x$
  - R = set of all ordinary sets
- Grelling's paradox
  - self-descriptive adjectives ("pentasyllabic") vs non-self-descriptive
  - what about "non-self-descriptive"?
- self-reference
  drawing hands
  The following sentence is false. The preceding sentence is true.




Way out?

- prohibition (Principia mathematica)
- types, metalanguage
- “In this lecture, I criticize the theory of types”
  cannot discuss the type theory
- David Hilbert: consistency and completeness

Computers

- Babbage
  The course through which I arrived at it was the most entangled and perplexed which probably ever occupied the human mind.

  Ada Lovelace (daughter of Lord Byron)
  Mechanized intelligence
  "Eating its own tail" (altering own program)
- axiomatic reasoning, mechanical computation, psycholgy of intelligence
- Alan Turing ~ Gödel's counterpart in computation theory
  Halting problem is undecidable.
  Can intelligent behaviour be programmed? Rules for inventing new rules...
  Strange loops in the core of intelligence
- materialism, de la Metrie: L'homme machine

Formal system

Example (over alphabet `M,I,U`)

- initial string ("axiom"):
  - `MI`
- rules ("inference/production rules") to enlarge your collection (of "theorems")
  requirement of formality: not outside the rules
  - last letter `I` ⇒ put `U` at the end
  - `M`x ⇒ `M`xx where x can be any string
  - replace `III` by `U`
  - drop `UU`

Homework: Can you produce/derive/prove `MU` ?

- Which rule to use? That's the art.

Theorems of MIU system

Axiom: MI

Rules:

1. $x\mathtt{I} \Rightarrow x\mathtt{IU}$
2. $\mathtt{M}x \Rightarrow \mathtt{M}xx$
3. $x\mathtt{III}y \Rightarrow x\mathtt{U}y$
4. $x\mathtt{UU}y \Rightarrow xy$

Working in the system / observing the system

- human itellingece ⇒ notice properties of theorems
- machine *can* act unobservant, people cannot

Perfect test (“decision procedure”) for theorems

- tree of all theorems?
- finite time!

Another formal system

- alphabet $\{\mathtt{p}, \mathtt{q}, -\}$
- axioms (axiom schema – obvious decision procedure):

$$x\mathtt{p}{-}\mathtt{q}x{-} \qquad \text{for any } x \text{ composed from hyphens}$$

- production rules:

$$x\mathtt{p}y\mathtt{q}z \Rightarrow x\mathtt{p}y{-}\mathtt{q}z{-} \qquad \text{for any } x, y, z \text{ composed from hyphens}$$

Decision procedure

- only lengthening rules
  $\Rightarrow$ reduce to shorter ones (top-down)
  $\Rightarrow$ dovetailing longer axioms and rule application (bottom-up)
- hereditary properties of theorems

Meaning

Isomorphism

- information-preserving transformation
- creates meaning
- interpretation + correspondence between true statements and interpreted theorems
- like cracking a code
- meaningless interpretations possible
- “well-formed” strings should produce “gramatical” sentences

Meaning is passive in formal systems

- it seems the system cannot avoid taking on meaning
- is `--p--p--q------` a theorem?
- subtraction
- does not add new additions, but we learn about nature of addition
- (is reality a formal system? is universe deterministic?)

Is our formal system accurate?

- 12×12: counting vs proof
- basic properties to be believed, e.g. commutatitvity and associativity
- in reality not always: raindrop, cloud, trinity, languages in India
- ideal numbers
- counting cannot check Euclid's Theorem

Is our formal system accurate?

- 12×12: counting vs proof
- basic properties to be believed, e.g. commutatitvity and associativity
- in reality not always: raindrop, cloud, trinity, languages in India
- ideal numbers
- counting cannot check Euclid's Theorem
  - reasoning
  - non-obvious result from obvious steps
  - belief in reasoning
  - overcoming infinity ("all" N)
  - patterned structure binding statements
  - can thinking be achieved by a formal system?

Escher: Liberation

Puzzle

1 3 7 12 18 26 35 45 56 ?

Escher: Mosaic II

Can we distinguish primes from composites?

Formal systems $\sim$ typographical operations:

- read, write, copy, erase, and compare symbols
- keep generated theorems

Can we distinguish primes from composites?

Formal systems ∼ typographical operations:

- read, write, copy, erase, and compare symbols
- keep generated theorems

Multiplication:

- axiom $x\texttt{t-q}x$ for every hyphen-string x
- rule $x\texttt{t}y\texttt{q}z \Rightarrow x\texttt{t}y\texttt{-q}zx$ for hyphen-strings x, y, z

Composites:

- rule $x\texttt{-t}y\texttt{-q}z \Rightarrow \texttt{C}z$ for hyphen-strings x, y, z

Can we distinguish primes from composites?

Formal systems ∼ typographical operations:

- read, write, copy, erase, and compare symbols
- keep generated theorems

Multiplication:

- axiom $x\texttt{t-q}x$ for every hyphen-string x
- rule $x\texttt{t}y\texttt{q}z \Rightarrow x\texttt{t}y\texttt{-q}zx$ for hyphen-strings x, y, z

Composites:

- rule $x\texttt{-t}y\texttt{-q}z \Rightarrow \texttt{C}z$ for hyphen-strings x, y, z

Primes:

- rule: $\texttt{C}x$ is not a theorem $\Rightarrow \texttt{P}x$ for every hyphen-string x

Can we distinguish primes from composites?

Formal systems ∼ typographical operations:

- read, write, copy, erase, and compare symbols
- keep generated theorems

Multiplication:

- axiom $x\texttt{t-q}x$ for every hyphen-string x
- rule $x\texttt{t}y\texttt{q}z \Rightarrow x\texttt{t}y\texttt{-q}zx$ for hyphen-strings x, y, z

Composites:

- rule $x\texttt{-t}y\texttt{-q}z \Rightarrow \texttt{C}z$ for hyphen-strings x, y, z

Primes:

- rule: $\texttt{C}x$ is not a theorem $\Rightarrow \texttt{P}x$ for every hyphen-string x
- reasoning what cannot be generated is outside of system, requirement of formality

Negative definitions: figure and ground

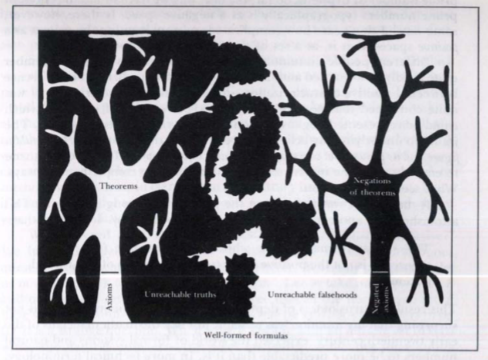
Negative definitions: figure and ground

Negative definitions: figure and ground

Sets

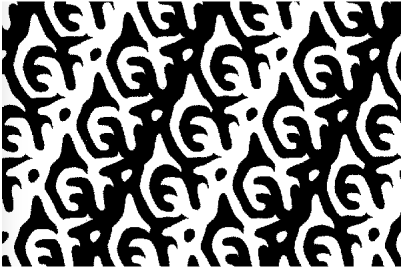
- recursive: decision procedure
- recursively enumerable (r.e.): can be generated
- non-r.e.

Negative definitions: figure and ground



Characterize false statements

- negative space of theorems
- altered copy of theorems



Impossible!

Impossibility

- some negative spaces cannot be positive
- = there are non-recursive r.e. sets
- $\Rightarrow$ there are formal sytems with no decision procedure

Primes are recursive

Primes are recursive

- axiom $x y \mathtt{DND} x$ for hyphen-strings x, y
- rules
  $x\mathtt{DND}y \Rightarrow x\mathtt{DND}xy$
  $\mathtt{--DND}z \Rightarrow z\mathtt{DF--}$
  $z\mathtt{DF}x$ and $x\mathtt{-DND}z \Rightarrow z\mathtt{DF}x\mathtt{-}$
  $z\mathtt{-DF}z \Rightarrow \mathtt{P}z\mathtt{-}$

Primes are recursive

- axiom $x y \texttt{DND} x$ for hyphen-strings x, y
- rules

  $x\texttt{DND}y \Rightarrow x\texttt{DND}xy$

  $\texttt{--DND}z \Rightarrow z\texttt{DF--}$

  $z\texttt{DF}x$ and $x\texttt{-DND}z \Rightarrow z\texttt{DF}x\texttt{-}$

  $z\texttt{-DF}z \Rightarrow \texttt{P}z\texttt{-}$
- axiom $\texttt{P--}$

Impossibility

- if a set is generatable in increasing order then so is its complement
- lengthening interleaved with shortening causes Gödel's Theorem, Turing's Halting Problem etc.

Diagonalisation: Cantor

$$
\begin{array}{rcl}
s_1 & = & {\color{red}0}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \ldots \\
s_2 & = & 1\ {\color{red}1}\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots \\
s_3 & = & 0\ 1\ {\color{red}0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ \ldots \\
s_4 & = & 1\ 0\ 1\ {\color{red}0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots \\
s_5 & = & 1\ 1\ 0\ 1\ {\color{red}0}\ 1\ 1\ 0\ 1\ 0\ 1\ \ldots \\
s_6 & = & 0\ 0\ 1\ 1\ 0\ {\color{red}1}\ 1\ 0\ 1\ 1\ 0\ \ldots \\
s_7 & = & 1\ 0\ 0\ 0\ 1\ 0\ {\color{red}0}\ 0\ 1\ 0\ 0\ \ldots \\
s_8 & = & 0\ 0\ 1\ 1\ 0\ 0\ 1\ {\color{red}1}\ 0\ 0\ 1\ \ldots \\
s_9 & = & 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ {\color{red}1}\ 1\ 0\ \ldots \\
s_{10} & = & 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ {\color{red}0}\ 1\ \ldots \\
s_{11} & = & 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ {\color{red}0}\ \ldots \\
\vdots & & \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \ddots
\end{array}
$$

$$
s = {\color{blue}1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1}\ \ldots
$$

Diagonalisation: Cantor

$$
\begin{array}{lcccccccccccc}
s_1 & = & \color{red}{0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \ \ldots \\
s_2 & = & 1 & \color{red}{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \ \ldots \\
s_3 & = & 0 & 1 & \color{red}{0} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \ \ldots \\
s_4 & = & 1 & 0 & 1 & \color{red}{0} & 1 & 0 & 1 & 0 & 1 & 0 & 1 \ \ldots \\
s_5 & = & 1 & 1 & 0 & 1 & \color{red}{0} & 1 & 1 & 0 & 1 & 0 & 1 \ \ldots \\
s_6 & = & 0 & 0 & 1 & 1 & 0 & \color{red}{1} & 1 & 0 & 1 & 1 & 0 \ \ldots \\
s_7 & = & 1 & 0 & 0 & 0 & 1 & 0 & \color{red}{0} & 0 & 1 & 0 & 0 \ \ldots \\
s_8 & = & 0 & 0 & 1 & 1 & 0 & 0 & 1 & \color{red}{1} & 0 & 0 & 1 \ \ldots \\
s_9 & = & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & \color{red}{1} & 1 & 0 \ \ldots \\
s_{10} & = & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & \color{red}{0} & 1 \ \ldots \\
s_{11} & = & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & \color{red}{0} \ \ldots \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ \ddots
\end{array}
$$

$$
s = \color{blue}{1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1}\ \ldots
$$

$f : S \to \mathcal{P}(S)$

Diagonalisation: Russell

$R = \{x \mid x \notin x\}$

Then $R \in R \iff R \notin R$

Diagonalisation: Turing

f(i,j)		i					
		1	2	3	4	5	6
j	1	1	0	0	1	0	1
	2	0	0	0	1	0	0
	3	0	1	0	1	0	1
	4	1	0	0	1	0	0
	5	0	0	0	1	1	1
	6	1	1	0	0	1	0
	f(i,i)	1	0	0	1	1	0
	g(i)	U	0	0	U	U	0

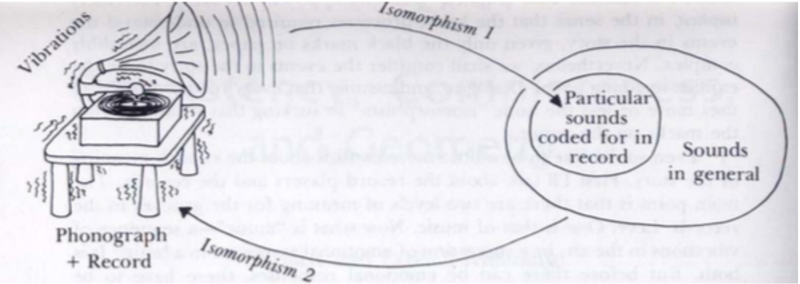
program e: `if f(i,i) == 0 then return 0 else loop forever`

- $f(e,e) = 0 \implies g(e) = 0 \implies$ program e halts on input e $\implies f(e,e) = 1$
- $f(e,e) \neq 0 \implies g(e)$ undef. $\implies$ program e doesn't halt on input e $\implies f(e,e) = 0$

Diagonalisation: Gödel (vague idea)

", when preceded by itself in quotes, is unprovable.", when preceded by itself in quotes, is unprovable.

For any player, there is a record which it cannot play because it will cause its indirect destruction.



Bach – self-reference in the Art of the Fugue

Story isomorphism

Phonograph <= =>axiomatic system for number theory

low-fidelity phonograph <= =>"weak" axiomatic system

high-fidelity phonograph <= =>"strong" axiomatic system

"Perfect" phonograph" <= => complete system for number theory'

Blueprint" of phonograph <= => axioms and rules of formal system

record <= => string of the formal system

playable record<= => theorem of the axiomatic system

unplayable record <= =>nontheorem of the axiomatic system

sound <= =>true statement of number theory

reproducible sound <= => 'interpreted theorem of the system

unreproducible sound <= => true statement which isn't a theorem:

song title <= =>implicit meaning of Gödel’s string:

"I Cannot Be Played on Record Player X"	"I Cannot Be Derived in Formal System X"

Consistency

Example: pq-system

- Axiom schema II: $x\mathtt{p}\text{-}\mathtt{q}x$ for every hyphen-string x
- inconsistent with external world

Consistency

Example: pq-system

- Axiom schema II: $x\mathtt{p}\text{-}\mathtt{q}x$ for every hyphen-string x
- inconsistent with external world
- reinterpret: $\geq$
- consistency depends on interpretation
- consistency = Every theorem, when interpreted, becomes a true statement.

Consistency

Example: non-Euclid geometry

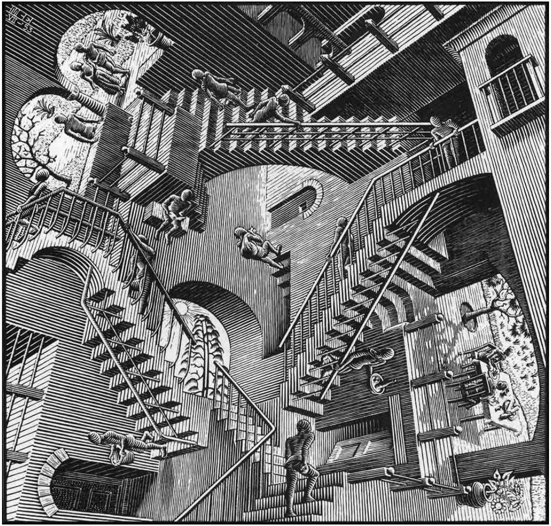
- Elements
- rigor
- axiomatic system
- fifth postulate not a consequence
- Saccheri, Lambert, Bolyai, Lobachevskiy
- elliptical/spherical (no parallel) and hyperbolical ($\geq$ 2 parallels) geometry (4 geometrical postlates remain, “absolute geometry” included)
- real points and lines vs. explicit definitions vs. implicit propositions

Consistency

- internal consistency: theorems mutually compatible
  holds in some “imaginable” world
- logical, mathematical, physical, biological etc. consistency
- Is number theory/geometry the same in all conceivable worlds?
  - Peano arithmetic $\sim$ absolute (core) geometry
  - number theories are the same for practical purposes
  - Gauss attmepted to measure angles between three mountains
    general relativity
    more geometries in mathematics and even physics

Consistency

Relativity



Completeness

Consistency: minimal condition for passive meaning

Completeness: maximal confirmation of passive meanings

“ Every true statement which can be expressed in the notation of the system is a theorem”

- Example: 2+3+4=9 in pq
- Example: pq with Axiom schema II
  (1) add rules or (2) tighten the interpretation

Gödel's 1st incompleteness theorem

Theorem

There are true arithmetical formulae unprovable in PA (or other consistent formal systems).

Gödel's proof (sketch)

- it is possible to construct a PA formula ρ such that

$$PA \quad \vdash \quad \rho \iff \neg\texttt{Provable}([\rho])$$

  i.e. "ρ says "I'm not provable"" is provable in PA
- by consistency of PA this is true in arithmetics
- if $\neg\rho$ then $\texttt{Provable}([\rho])$, a contradiction
  if ρ then $\neg\texttt{Provable}([\rho])$ hence $PA \nvdash \rho$ □

Gödel's 1st incompleteness theorem

Recall:

- $\texttt{Accept} := \{i \mid M_i \text{ accepts } i\}$
- $\texttt{Accept}$ is r.e., but not recursive
- $\overline{\texttt{Accept}}$ is not r.e.

Alternative proof: $\texttt{Provable} \subsetneq \texttt{Valid}$

- $\texttt{Provable}$ is r.e. (for PA and similar)
- $\texttt{Provable} \subseteq \texttt{Valid}$ by consistency
- we prove $\texttt{Valid}$ is not r.e., hence $\subsetneq$
  - construct a program transforming $n \in \mathbb{N}$ into a formula φ:

    $$\varphi \in \texttt{Valid} \quad \text{iff} \quad n \in \overline{\texttt{Accept}}$$

    it computes the formula "M_n does not accept n"
  - computation is a sequence of configurations (numbers)
  - one can encode that a configuration c follows a given configuration d
  - every finite sequence can be encoded by a formula β:
    For every $n_1, \ldots, n_k$ there are $a, b \in \mathbb{N}$ such that

    $$\beta(a, b, i, x) \text{ iff } x = n_i$$

Let $\beta(a, b, i, x)$ be true iff $x = a \bmod (1 + b(1 + i))$

- expressible in simple arithmetics:

  $$a \geq 0 \wedge b \geq 0 \wedge \exists k \big(k \geq 0 \wedge k * c \leq a \wedge (k+1) * c > a \wedge x = a - (k * c)\big)$$

  where c is a shortcut for $(1 + b * (1 + i))$
- for every a, b the predicate β induces a unique sequence, where the ith element is $a \bmod (1 + b(1 + i))$
- every finite sequence can be encoded by β for some a, b:

Theorem

For every $n_1, \ldots, n_k$ there are $a, b \in \mathbb{N}$ such that

$$\beta(a, b, i, x) \textit{ iff } x = n_i$$

Gödel's 1st incompleteness theorem

$\beta(a, b, i, x)$ iff $x = a \bmod (1 + b(1 + i))$

Theorem

For every $n_1, \ldots, n_k$ there are $a, b \in \mathbb{N}$ such that

$$\beta(a, b, i, x) \textit{ iff } x = n_i$$

Proof.

- $b := (\max\{k, n_1, \ldots, n_k\})!$
- $p_i := 1 + b(1 + i)$ is $\geq n_i$ and are co-prime (gcd of each pair is 1)
- $c_i := \prod_{j \neq i} p_j$
- $\exists! \quad 0 \leq d_i \leq p_i : c_i \cdot d_i \bmod p_i = 1$
- $a := \sum_{i=1}^{k} c_i \cdot d_i \cdot n_i$
- hence $n_i = a \bmod p_i$

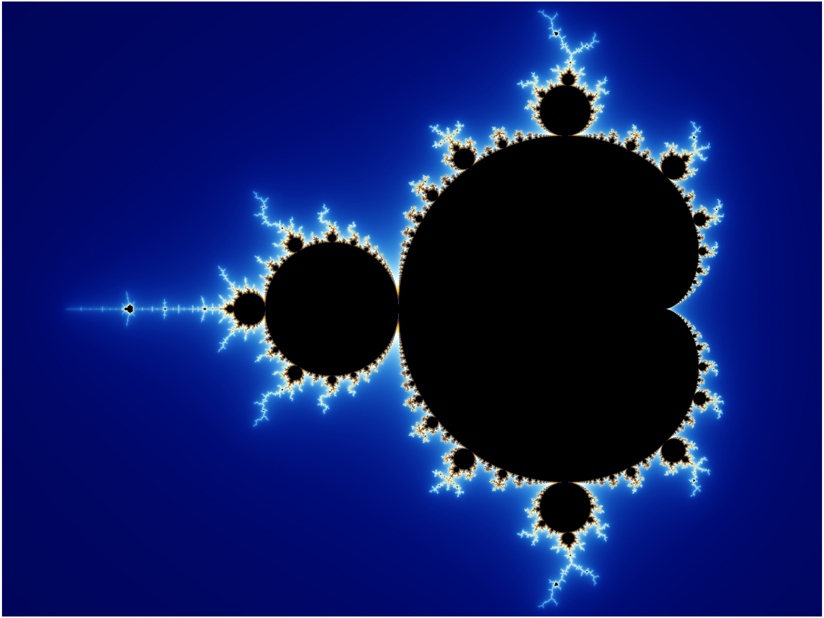
□

Recursion

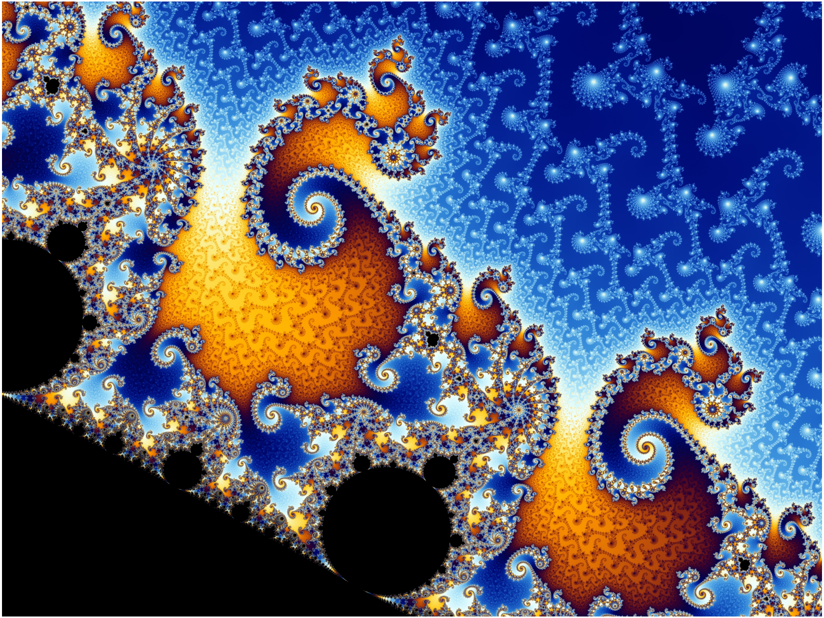
Examples

- recursive defintions
  - in terms of *simpler* versions of itself
  - some part avoids self-reference (vs. circular definitions)
- pushdown systems
- music: tonic and pseudo-tonic
- language: verb at the end
- indirect recursion in Epimenides
- Fib(n)=Fib(n-1)+Fib(n-2)
- computer programs
- fractals
- Cantor set

Mandelbrot set

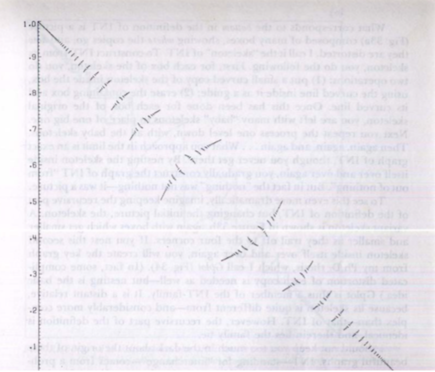


Mandelbrot set



Further examples

energies of electrons in a crystal in a magnetic field



Cantor set

Sidenote: Location of meaning

- is meaning of a message an inherent property of the message?
- meaning is part of an object to the extent that it acts upon intelligence in a predictable way
- levels of informtion
  - frame message: “this bears information”
  - outer message: “this is in Japanese”
  - inner message: “this says ...”
- if all juke-boxes would play the same song on “A-5”, it wouldn’t be just a trigger but a meaning of “A-5”
- mass is intrinsic, weight is not; or yes, but at the cost of geocentricity
-

  .

  .

Propositional calculus: Definition

- purely typographic
- alphabet: $< > \quad P\ Q\ R\ ' \ \wedge\ \vee\ \supset \sim\ [\ ]$
- well-formed strings:
  - atoms: P, Q, R + adding primes
  - formation rules: if x and y are wel-formed then so are $\sim x, < x \wedge y >, < x \vee y >, < x \supset y >$
- rules
  - joining: x and $y \Rightarrow < x \wedge y >$
  - separation:$< x \wedge y > \Rightarrow x$ and y
  - double-tilde: $\sim\sim$ can be deleted or inserted
  - contrapositive: $< x \supset y >$ and $<\sim y \supset\sim x >$ interchangable
  - De Morgan: $\sim< x \vee y >$ and $<\sim x \wedge \sim y >$ interchangable
  - Switcheroo: $< x \vee y >$ and $<\sim x \supset y >$ interchangable
  - no axioms

Propositional calculus: Definition

- purely typographic
- alphabet: $< >$ $P\ Q\ R\ '$ $\wedge$ $\vee$ $\supset \sim$ $[\ ]$
- well-formed strings:
  - atoms: P, Q, R + adding primes
  - formation rules: if x and y are wel-formed then so are $\sim x, < x \wedge y >, < x \vee y >, < x \supset y >$
- rules
  - joining: x and $y \Rightarrow < x \wedge y >$
  - separation:$< x \wedge y > \Rightarrow x$ and y
  - double-tilde: $\sim\sim$ can be deleted or inserted
  - contrapositive: $< x \supset y >$ and $<\sim y \supset\sim x >$ interchangable
  - De Morgan: $\sim< x \vee y >$ and $<\sim x \wedge \sim y >$ interchangable
  - Switcheroo: $< x \vee y >$ and $<\sim x \supset y >$ interchangable
  - no axioms
  - fantasy rule (Deduction Theorem): y derived from $x \Rightarrow< x \supset y >$
  - carry-over theorems into fantasy
  - detachment (Modus Ponens): x and $< x \supset y >\Rightarrow y$

Propositional calculus: Properties

- decision procedure:

Propositional calculus: Properties

- decision procedure: truth tables

- simplicity, precision
- other versions (axiom schemata + detachment)

  extensions (valid propositional inferences,
  incompleteness/inconsistency only due to embedding system)

Propositional calculus: Properties

- decision procedure: truth tables
- simplicity, precision
- other versions (axiom schemata + detachment)

  extensions (valid propositional inferences, incompleteness/inconsistency only due to embedding system)

Informal

- proof: normal thought
- simplicity: sounds right
- complexity: human language

Formal

- derivation: artificial, explicit
- simplicity: trivial
- astronomical size

Propositional calculus: Contradictions

- $< <P \wedge \sim P> \supset Q >$
- infection vs. mental break-down
- $1 - 1 + 1 - 1 + 1 \cdots$
- relevant implication

Typographical number theory: Syntax

- natural-numbers theory N $\rightarrow$ TNT
  1. 2 is not a square.
  2. 5 is a prime.
  3. There are infinitely many primes.

Typographical number theory: Syntax

- natural-numbers theory N $\rightarrow$ TNT
  1. 2 is not a square.
  2. 5 is a prime.
  3. There are infinitely many primes.
- primitives: for all numbers, there exists a number, equals, greater than, times, plus, 0, 1, 2, ...
- variables: a, b, a'
  terms: $(a \cdot b), (a + b), 0, S0, SS0$
  atoms: $S0 + S0 = SS0$
  quantifiers: $\exists b : (b + S0) = SS0$, similarly $\forall$

Typographical number theory: Syntax

- natural-numbers theory N → TNT
    1. 2 is not a square.
    2. 5 is a prime.
    3. There are infinitely many primes.
- primitives: for all numbers, there exists a number, equals, greater than, times, plus, 0, 1, 2, ...
- variables: a, b, a'
  terms: $(a \cdot b), (a + b), 0, S0, SS0$
  atoms: $S0 + S0 = SS0$
  quantifiers: $\exists b : (b + S0) = SS0$, similarly $\forall$

Puzzle: encode the following

- b is a power of 2
- b is a power of 10

Propositional calculus: Examples

- $\sim\forall c : \exists b : (SS0 \cdot b) = c$
- $\forall c : \sim\exists b : (SS0 \cdot b) = c$
- $\forall c : \exists b : \sim(SS0 \cdot b) = c$
- $\sim\exists b : \forall c : (SS0 \cdot b) = c$
- $\exists b : \sim\forall c : (SS0 \cdot b) = c$
- $\exists b : \forall c : \sim(SS0 \cdot b) = c$

Propositional calculus: Derivations

Axioms:

1. $\forall a : {\sim}Sa = 0$
2. $\forall a : (a + 0) = a$
3. $\forall a : \forall b : (a + Sb) = S(a + b)$
4. $\forall a : (a \cdot 0) = 0$
5. $\forall a : \forall b : (a \cdot Sb) = ((a \cdot b) + a)$

Propositional calculus: Derivations

Axioms:

1. $\forall a : \sim Sa = 0$
2. $\forall a : (a + 0) = a$
3. $\forall a : \forall b : (a + Sb) = S(a + b)$
4. $\forall a : (a \cdot 0) = 0$
5. $\forall a : \forall b : (a \cdot Sb) = ((a \cdot b) + a)$

Rules:

1. specification: $\forall u : x \Rightarrow x[u'/u]$ for any term u'
2. generalization: $x \Rightarrow \forall u : x$ for a free variable u
3. interchange: $\forall u :\sim$ and $\sim \exists u :$ are interchangeable
4. existence: $x[u'/u] \Rightarrow \exists u : x$
5. symmetry: $r = s \Rightarrow s = r$
6. transitivity: $r = s$ and $s = t \Rightarrow r = t$
7. successorship: $r = t \Leftrightarrow Sr = St$

Propositional calculus: Derivations

Axioms:

1. $\forall a : \sim Sa = 0$
2. $\forall a : (a + 0) = a$
3. $\forall a : \forall b : (a + Sb) = S(a + b)$
4. $\forall a : (a \cdot 0) = 0$
5. $\forall a : \forall b : (a \cdot Sb) = ((a \cdot b) + a)$

Rules:

1. specification: $\forall u : x \Rightarrow x[u'/u]$ for any term u'
2. generalization: $x \Rightarrow \forall u : x$ for a free variable u
3. interchange: $\forall u :\sim$ and $\sim \exists u :$ are interchangeable
4. existence: $x[u'/u] \Rightarrow \exists u : x$
5. symmetry: $r = s \Rightarrow s = r$
6. transitivity: $r = s$ and $s = t \Rightarrow r = t$
7. successorship: $r = t \Leftrightarrow Sr = St$

Example: $S0 + S0 = SS0$

Typographical number theory: Induction

- can derive
  - $(0 + 0) = 0$
  - $(0 + S0) = S0$
  - $(0 + SS0) = SS0$
  - $\vdots$
- can derive $\forall a : (0 + a) = a$?

Typographical number theory: Induction

- can derive
  - $(0 + 0) = 0$
  - $(0 + S0) = S0$
  - $(0 + SS0) = SS0$
  - $\vdots$
- can derive $\forall a : (0 + a) = a$?
- nor its negation
  undecidable in TNT (like Euclid's 5th postulate in absolute geometry)
- rule of induction: u variable, $X\{u\}$ well-formed formula with u free,
  $X\{0/u\}, \; \forall u :< X\{u\} \supset X\{Su/u\} > \;\Rightarrow\; \forall u : X\{u\}$

Typographical number theory: Consistency

- we believe in each rule
- are natural numbers a coherent construct??

Typographical number theory: Consistency

- we believe in each rule
- are natural numbers a coherent construct??
  Peano's axioms:
  1. zero is a number
  2. every number has a successor (which is a number)
  3. zero is not a successor of any number
  4. different numbers have different successors
  5. if zero has X and every number relays X to its successor, then all numbers have X

Typographical number theory: Consistency

- we believe in each rule
- are natural numbers a coherent construct??
  Peano's axioms:
  1. zero is a number
  2. every number has a successor (which is a number)
  3. zero is not a successor of any number
  4. different numbers have different successors
  5. if zero has X and every number relays X to its successor, then all numbers have X
- want to convince of consistency of TNT using a weaker system

Typographical number theory: Consistency

- we believe in each rule
- are natural numbers a coherent construct??
  Peano's axioms:
  1. zero is a number
  2. every number has a successor (which is a number)
  3. zero is not a successor of any number
  4. different numbers have different successors
  5. if zero has X and every number relays X to its successor, then all numbers have X
- want to convince of consistency of TNT using a weaker system
- Gödel's 2nd Theorem: Any system that is strong enough to prove TNT's consistency is at least as strong as TNT itself.

Recall: MIU system

- alphabet M,I,U
- initial string ("axiom"):
  - MI
- rules
  1. $x\mathtt{I} \Rightarrow x\mathtt{IU}$
  2. $\mathtt{M}x \Rightarrow \mathtt{M}xx$
  3. $x\mathtt{III}y \Rightarrow x\mathtt{U}y$
  4. $x\mathtt{UU}y \Rightarrow xy$
- Can you produce MU ?

Recall: MIU system

- alphabet M,I,U
- initial string ("axiom"):
  - MI
- rules
  1. xI $\Rightarrow$ xIU
  2. Mx $\Rightarrow$ Mxx
  3. xIIIy $\Rightarrow$ xUy
  4. xUUy $\Rightarrow$ xy
- Can you produce MU ?
- No:
  - I-count starts at 1 (not multiple of 3)
  - I-count is a multiple of 3 only it was before applying the most recent rule

Gödel numbering

- All problems about any formal system can be encoded into number theory!
- define arithmetization on symbols (Gödel number):
  - $\mathtt{M} \leftrightarrow 3$
  - $\mathtt{I} \leftrightarrow 1$
  - $\mathtt{U} \leftrightarrow 0$
- extend it to all strings
  1. $\mathtt{MI} \leftrightarrow 31$
  2. $\mathtt{MIU} \leftrightarrow 310$

Example: Rule 1

1. $x\mathtt{I} \Rightarrow x\mathtt{IU}$
2. $x1 \Rightarrow x10$
3. $x \Rightarrow 10 \cdot x$ for any $x \bmod 10 = 1$

Typographical rules on numerals are actually arithmetical rules on numbers.

- Is $\mathtt{MU}$ a theorem of the MIU-system?
- Is 30 a MIU-number?

Gödel numbering

- All problems about any formal system can be encoded into number theory!
- define arithmetization on symbols (Gödel number):
  - $\mathtt{M} \leftrightarrow 3$
  - $\mathtt{I} \leftrightarrow 1$
  - $\mathtt{U} \leftrightarrow 0$
- extend it to all strings
  1. $\mathtt{MI} \leftrightarrow 31$
  2. $\mathtt{MIU} \leftrightarrow 310$

Example: Rule 1

1. $x\mathtt{I} \Rightarrow x\mathtt{IU}$
2. $x1 \Rightarrow x10$
3. $x \Rightarrow 10 \cdot x$ for any $x \bmod 10 = 1$

Typographical rules on numerals are actually arithmetical rules on numbers.

- Is MU a theorem of the MIU-system?
- Is 30 a MIU-number?

1. “MU is a theorem” into number theory
2. number theory into TNT

Self-swallowing TNT

1 Gödel-number TNT:

- $S0 = 0$ is a theorem of TNT $\longrightarrow$ $123,666,111,666$ is a TNT-number

Self-swallowing TNT

1 Gödel-number TNT:

- $S0 = 0$ is a theorem of TNT $\longrightarrow$ $123,666,111,666$ is a TNT-number
- thus for any formalization of number theory, its metalanguage is embedded in it

Self-swallowing TNT

1. Gödel-number TNT:
   - $S0 = 0$ is a theorem of TNT $\longrightarrow$ $123,666,111,666$ is a TNT-number
   - thus for any formalization of number theory, its metalanguage is embedded in it
2. self-reference:
   - find a string G that says "G is not a theorem"
   - theorem $\implies$ truth $\implies$ not a theorem $\implies$ truth, but unprovable

Self-swallowing TNT

1 Gödel-number TNT:

- $S0 = 0$ is a theorem of TNT $\longrightarrow$ $123,666,111,666$ is a TNT-number
- thus for any formalization of number theory, its metalanguage is embedded in it

2 self-reference:

- find a string G that says "G is not a theorem"
- theorem $\implies$ truth $\implies$ not a theorem $\implies$ truth, but unprovable

Summary :
There is a string of TNT expressing a statement about numbers (interpretable as "I am not a theorem of TNT").
By reasoning outside of the system, we can show it is true.
But still it is not a theorem of TNT (TNT says neither true nor false).

Gödel's Proof I/IV

Proof pairs:

- (MI MII MIIII MUI, MUI)
  (31 311 31111 301, 301)
- recognizing is primitive recursive, hence there is a formula MIU-PP(a, a') expressing "a is a proof of a'"
- $\exists a$:TNT-PP(a, $\underbrace{SS \cdots S}_{666\,111\,666\times} 0/a'$)

Gödel's Proof I/IV

Proof pairs:

- (MI MII MIIII MUI, MUI)
  (31 311 31111 301, 301)
- recognizing is primitive recursive, hence there is a formula MIU-PP(a, a') expressing "a is a proof of a'"
- $\exists a$:TNT-PP$(a, \underbrace{SS \cdots S}_{666\,111\,666\times} 0/a')$

Substitution:

- SUB(a, a', a'') for replacing all free variables in a by a' yields a''
- $a = a$ with $2/a$ yields $2 = 2$
  SUB$(\underbrace{S \cdots S}_{262\,111\,262\times} 0/a, SS0/a', \underbrace{S \cdots S}_{123\,123\,666\,111\,123\,123\,666\times} 0/a)$

Gödel's Proof II/IV

Arithmoquining

- Quine ___ is one.: "is one" is one.
- Arithmoquine $a = S0$: $\underbrace{S \cdots S}_{262\,111\,123\,666\times} 0 = S0$

Gödel's Proof II/IV

Arithmoquining

- Quine ___ is one.: "is one" is one.
- Arithmoquine $a = S0$: $\underbrace{S \cdots S}_{262\,111\,123\,666\times} 0 = S0$
- AQ(a'', a') abbreviation for SUB(a'', a'', a')
  (use the same number in two different ways:
  diagonalization+coding)
- Arithmoquinification of $a = S0$: $\underbrace{123 \cdots 123}_{262\,111\,123\,666\times}$ 666 111 123 666
- now, quine a quine-mentioning sentence

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(a'', a')$ has number u

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \land AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \land AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \land AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \land AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?

Gödel's Proof III/IV

- G's uncle $\neg \exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg \exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(\underbrace{S \cdots S}_{u \times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?
  - There is no number a forming a proof pair with arithmoquinification of u

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?
  - There is no number a forming a proof pair with arithmoquinification of u
  - The formula whose number is arithmoquinification of u is not a theorem.

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?
  - There is no number a forming a proof pair with arithmoquinification of u
  - The formula whose number is arithmoquinification of u is not a theorem.
  - G is not a theorem.

Gödel's Proof III/IV

- G's uncle $\neg\exists a\exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a\exists a' : \mathit{TNT\text{-}PP}(a, a') \wedge AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?
  - There is no number a forming a proof pair with arithmoquinification of u
  - The formula whose number is arithmoquinification of u is not a theorem.
  - G is not a theorem.
  - I am not a theorem of TNT.

Gödel's Proof III/IV

- G's uncle $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(a'', a')$ has number u
- Arithmoquine(uncle): $\neg\exists a \exists a' : TNT\text{-}PP(a, a') \wedge AQ(\underbrace{S \cdots S}_{u\times} 0, a')$

  is Gödel's formula G
- its Gödel's number is Arithmoquinification(u)
- What does G mean?
  - There is no number a forming a proof pair with arithmoquinification of u
  - The formula whose number is arithmoquinification of u is not a theorem.
  - G is not a theorem.
  - I am not a theorem of TNT.
- TNT sentence with low-level interpretation has high-level interpretation (a sentence of meta-TNT)

Gödel's Proof IV/IV

Falsehood	<==>	nontheoremhood
quotation of a phrase	<==>	
preceding a predicate by a subject	<==>	definite term) into an open formula
preceding a predicate by a quoted phrase	<==>	substituting the Gödel number of a string into an open formula
preceding a predicate by itself, in quotes ("quining")	<==>	substituting the Gödel number of an open formula into the formula itself ("arithmoquining")
yields falsehood when quined (a predicate without a subject)	<==>	"uncle" of **G**" the(an open formula of **TNT**
"yields falsehood when quined" (the above predicate. quoted)	<==>	the number a (the Gödel number of the above open formula)
"yields falsehood when quined" yields falsehood when quined (complete sentence formed by quining the above predicate)	<==>	G itself (sentence of TNT formed by□substituting a into the uncle,□i.e., arithmoquining the uncle)

Summary

- There is a string of TNT expressing a statement about numbers (interpretable as “I am not a theorem of TNT”).
- By reasoning outside of the system, we can show it is true.
- But still it is not a theorem of TNT (TNT says neither true nor false).

Summary

- There is a string of TNT expressing a statement about numbers (interpretable as “I am not a theorem of TNT”).
- By reasoning outside of the system, we can show it is true.
- But still it is not a theorem of TNT (TNT says neither true nor false).

Monk: Does a dog have Buddha-nature, or not?
Jōshū: MU

Has a dog Buddha-nature?
This is the most serious question of all.
If you say yes or no,
You lose your own Buddha-nature.

(Mumon on Jōshū’s MU)

Consequences

- Gödels's Second Theorem
  - $\neg\exists a$:TNT-PP(a, $\underbrace{S \cdots S}_{223\,666\,111\,666\times} 0/a'$)
  - can be proven only if TNT inconsistent

Consequences

- Gödels's Second Theorem
  - $\neg\exists a$:TNT-PP(a, $\underbrace{S\cdots S}_{223\,666\,111\,666\times}$ $0/a'$)
  - can be proven only if TNT inconsistent
- incomplete, then add G as axiom or its negation?

$$\exists a : (a + a) = S0$$
$$\exists a : Sa = 0$$
$$\exists a : (a \cdot a) = SS0$$
$$\exists a : S(a \cdot a) = 0$$

- the proof of G is "infinitely" large (how large is i?)
- supernatural numbers
  - Heisenberg's uncertainty principle for sum and product
  - also fractions, reals, dx, dy: non-standard analysis
  - are they real? is $\sqrt{-1}$?

Last words

Free will, consciousness

- computer vs. human?
- self-design, choosing one's wants?
- Do words and thoughts follow formal rules?

Free will, consciousness

- computer vs. human?
- self-design, choosing one's wants?

- Do words and thoughts follow formal rules?
- rules on the lowest level, e.g. neurons
- software rules change, hardware cannot

Strange loops, tangled hierarchies: Examples

- self-modifying game
- Escher's hands
- symbols in brain (on neuronal substrate)
- ? washing hands, dialogue
- language, Klein bottle
- we feel self-programmed, but we are just shielded from neurons
- Watergate
- fact A, evidence B, meta-evidence C that B is evidence of A,...
  built-in hardware for what is evidence

Klein bottle

Dualism

Subject vs Object

- old science
- prelude to modern phase: quantum mechanics, metamathematics, science methodology, AI

Use vs Mention

- symbols vs just be (Zen)
- John Cage: Imaginary Landscape No.4
- René Magritte: Common Sense, The Two Mysteries

Magritte: The Two Mysteries

Self

- limitative theorems (Gödel, Church, Turing, Tarski,. . .)
- imagine your own non-existence
- cannot be done fully, TNT does not contain its full meta-theory

- “self” necessary for free will
- strange loops necessary
- not non-determinism, but choice-maker: identification with a high-level description of the process when program is running
- Gödel, Escher, Bach