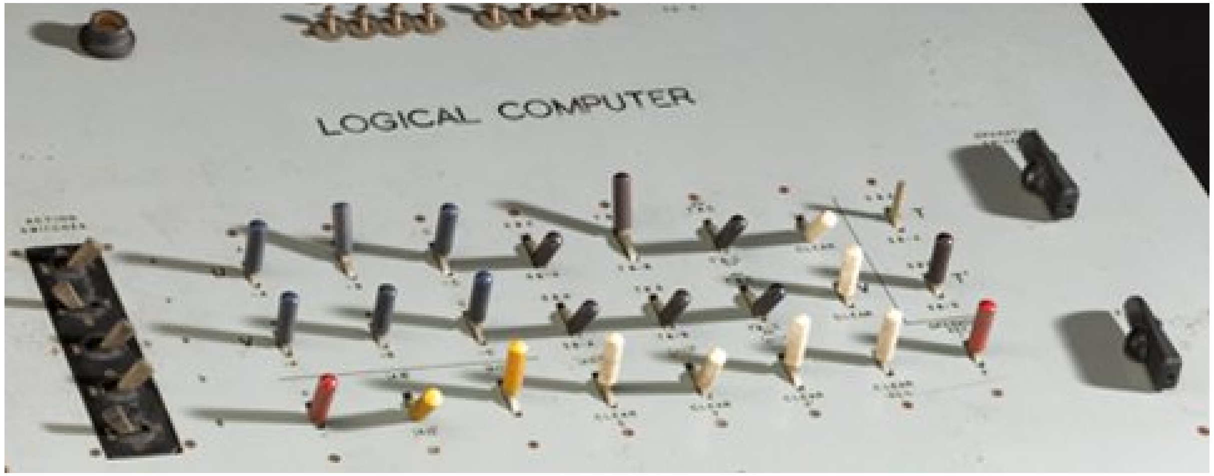
INF551

Computational Logic:

Artificial Intelligence in Mathematical Reasoning

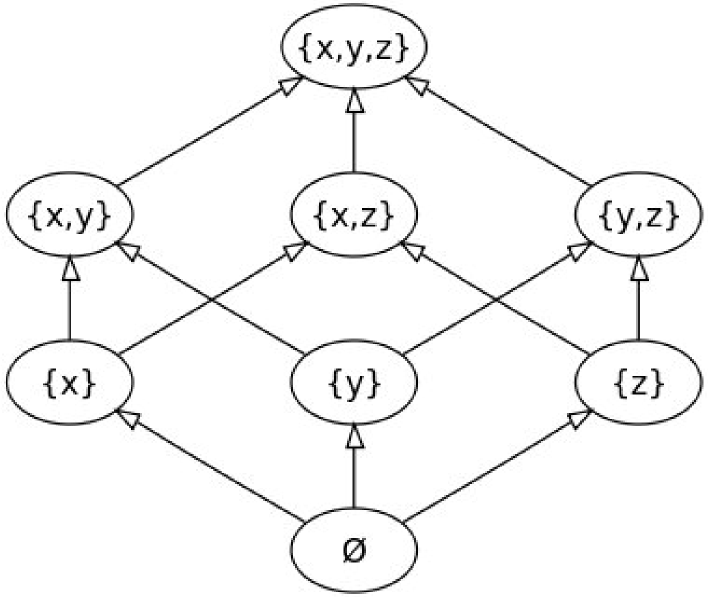


Stéphane Graham-Lengrand

Stephane.Lengrand@Polytechnique.edu

Lecture VI

The theory of sets



Where we stand today

We know computer-aided reasoning techniques for

- propositional logic
- some specific theories with or without quantifiers,
- predicate logic in general

Now:

we want a systematic way of representing any problem (of mathematical nature)

in a universal framework (language+logic+theory)

Why?

Because then,

mechanics of solving problems in that framework

$\Longrightarrow$ mechanics of solving any problem

Arithmetic?

Too weak! . . . difficult to account for different notions of infinity

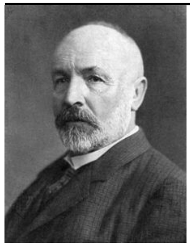
Today:

Proposal for such framework = *Set theory*

Contents

I. The mathematics chat room

The mathematics chat room

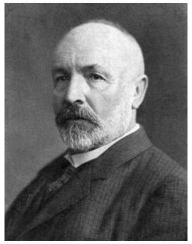


74-78: Georg enters chat.

There are different notions of infinity! Here’s the notion of bijection!

78: Leopold says

That’s all crap



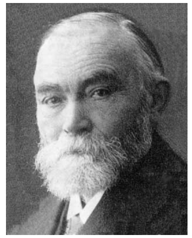
78: Georg says

I can’t prove the property that there is no cardinal between $\mathbb{Q}$ and $\mathbb{R}$.

Strange. Let’s call it the *Continuum Hypothesis*

79: Gottlob enters chat.

Hi guys! I’ve formalised logic with quantified variables. anyone interested?



82: Ferdinand says

π is transcendental

86: Leopold says

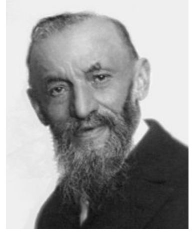
lol!

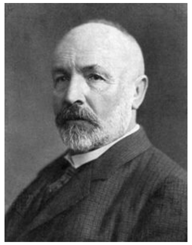
Irrational numbers do not exist, let alone transcendental numbers

The mathematics chat room

89: Giuseppe enters chat.

Here's an axiomatisation of arithmetic. Georg, you use a property that you cannot justify; let's call that the *axiom of choice*.





91: Georg says

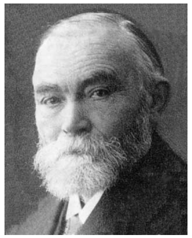
You like it, yeah?

Here are some more: axiom of *infinity* and axiom of the *power set*

91: Leopold says

This is nonsense

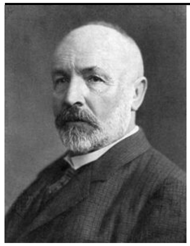
91: Leopold left the chat.



93: Gottlob says

I think Georg's ideas are cool, I'll extend my logic with them!

The mathematics chat room

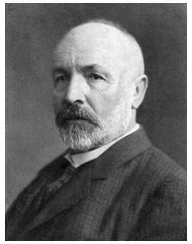


95: Georg says

Here are my latest thoughts about sets and *ordinals*.

95: David enters chat.

That’s quite a lot of ordinals. Who’s got the biggest?

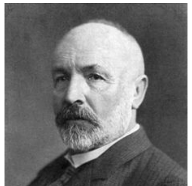


96: Georg to David (private):

Bugger, the set of all ordinals doesn’t seem to be a set; let’s keep this private

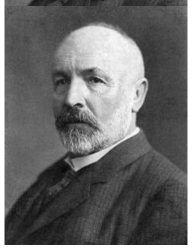
97: Cesare enters chat.

Hi Georg, the set of all ordinals doesn’t seem to be a set!



97: Georg says

Go away, you misread my paper! Damn it, I’ve been busted.



99: Georg says

Oh no! the cardinal of the set of all sets also seems problematic. . .

And I still can’t prove the continuum hypothesis.

Ok, now I’ll prove that Francis Bacon wrote Shakespeare’s plays.

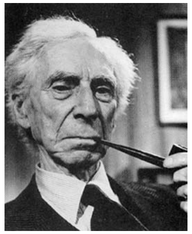
The mathematics chat room

99: David says

Now now, children, let's clear up this mess.

I have 23 problems to submit to you all.

Let's use Gottlob's logical methodology more systematically.



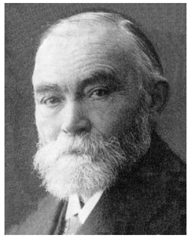
02: Bertrand enters chat.

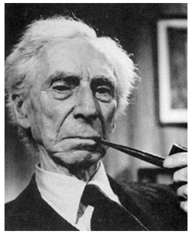
Hold on, chaps. I dare say that Gottlob's logical foundations are bugged too; and there is no such thing as the set of all sets.

03: Gottlob says

You've undermined the whole of mathematics!

I'm depressed.





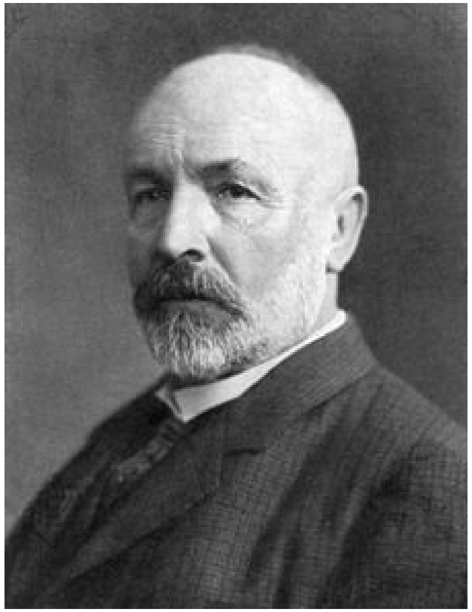
03: Bertrand says

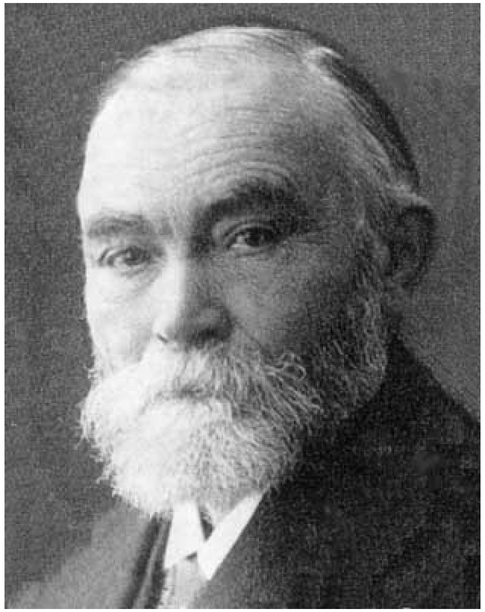
Don't worry, me and me pal Alfred will fix it with a *Theory of Types!*

08: Ernst enters chat.

Don't bother, here's an axiomatisation of set theory without the paradox.

II. Naive set theory & Russell's paradox





Naïve set theory

Syntax: Empty term signature; Predicate signature: $\in$ and $=$, arity 2

Notation: Let's fix a particular sequence of variables y_1,...,y_i,...

If A is a formula and t_1,..., t_p are p terms, then $A[t_1, \ldots, t_p]$ denotes $\left\{{}^{t_1,\ldots,t_p}\!/\!_{y_1,\ldots,y_p}\right\} A$

In Cantor's work and Frege's work, we have, for every formula A such that FV$(A) \subseteq \{y_1, x_1, \ldots, x_n\}$, an axiom

$$\forall x_1 \ldots \forall x_n \exists c \forall y \ (y \in c \Leftrightarrow A[y])$$

Informally:

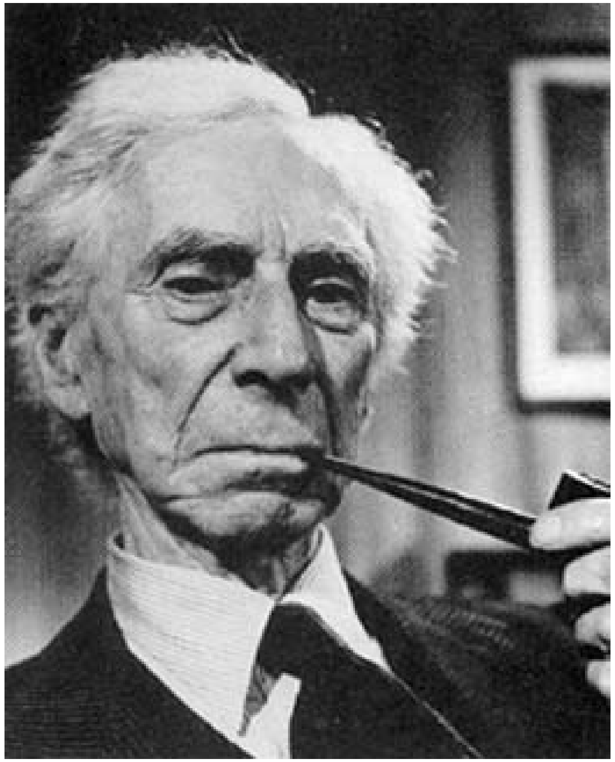
existence of the set $\{y \mid A[y]\}$, i.e. the set of all elements y satisfying $A[y]$

First instantiation: in particular we have

$$\exists r \forall y \ (y \in r \Leftrightarrow \top)$$

i.e. $\exists r \forall y \ (y \in r)$ (there is a set of all sets)

Russell's paradox (1902)



Second instantiation: in particular we have axiom R:

$$\exists r \forall y \, (y \in r \Leftrightarrow \neg y \in y)$$

What about $r \in r$? or is it $\neg r \in r$?

Clearly, $R \vdash \exists r (r \in r \Leftrightarrow \neg r \in r)$

Is this problematic?

Yes, since:

Lemma: If $\mathcal{T} \vdash (A \Leftrightarrow \neg A)$ then $\mathcal{T} \vdash \bot$

Proof: Clearly, $(A \Leftrightarrow \neg A), A \vdash \neg A$

and since we also have $(A \Leftrightarrow \neg A), A \vdash A$, we get $(A \Leftrightarrow \neg A), A \vdash \bot$

Therefore $A \Leftrightarrow \neg A \vdash \neg A$

And finally $A \Leftrightarrow \neg A \vdash \bot$

So indeed $R \vdash \bot$

III. Zermelo-Fraenkel set theory

Fixing set theory with Separation (Zermelo 1908)

Russell's paradox can be quickly fixed:

for every formula A such that FV$(A) \subseteq \{y_1, x_1, \ldots, x_n\}$,

have an axiom S_A:

$$\forall x_1 \ldots \forall x_n \forall x \exists c \forall y\ (y \in c \Leftrightarrow (y \in x \wedge A[y]))$$

Informally: existence of the set $\{y \in x \mid A[y]\}$,

i.e. the set of all elements y in x satisfying $A[y]$

Separation axiom(s) (x is split in two)

Corollary: $(S_A)_A \vdash \neg(\exists a \forall y (y \in a))$ **There is no set of all sets**

Proof: Indeed $S_{\neg y \in y} \vdash \forall a\ \exists r\ \forall y\ (y \in r \Leftrightarrow (y \in a \wedge \neg y \in y))$

so $S_{\neg y \in y}, (\exists a \forall y (y \in a)) \vdash \exists r\ \forall y\ (y \in r \Leftrightarrow (\top \wedge \neg y \in y))$

so $S_{\neg y \in y}, (\exists a \forall y (y \in a)) \vdash R$

so $S_{\neg y \in y}, (\exists a \forall y (y \in a)) \vdash \bot$.

Improving Separation with Replacement (Fraenkel 1922)

Note: the separation schema is quite restrictive

There are still instances of the bugged axiom schema that are desired but not allowed by separation.

Generalise separation schema into *replacement schema*:

for every formula A such that FV$(A) \subseteq \{y_1, y_2, x_1, \ldots, x_n\}$,

have an axiom R_A:

$$\forall x_1 \ldots \forall x_n \; [\text{functional}(A) \Rightarrow \forall x \exists c \forall y \; (y \in c \Leftrightarrow \exists z \; (z \in x \wedge A[z, y]))]$$

where functional(A) abbreviates $\forall z \forall y \forall y' \; ((A[z, y] \wedge A[z, y']) \Rightarrow y = y')$

Informally : "$c = Im(A_{|x})$"

Lemma: Generalises separation

Proof: separation axiom S_A can be proved from replacement axiom $R_{y_1 = y_2 \wedge A}$:

$$\forall x_1 \ldots \forall x_n \; [\text{functional}(y_1 = y_2 \wedge A) \\ \Rightarrow \forall x \exists c \forall y \; (y \in c \Leftrightarrow \exists z \; (z \in x \wedge z = y \wedge A[z]))]$$

(functional$(y_1 = y_2 \wedge A)$ easy to prove)

Building bigger sets (motivation)

Notice that neither the separation schema nor the replacement schema construct sets "bigger" than those already constructed

Cantor 1891:

simple proof that there is a set strictly "bigger" than that of natural numbers

Take the set ω of natural numbers

Take its power set $\mathbb{P}(\omega)$

Assume f is a surjective function from ω to $\mathbb{P}(\omega)$ (assumption H)

Let $a := \{y \in \omega \mid \neg y \in f(y)\}$. Let $x \in \omega$ such that $f(x) = a$ (f is surjective)

Question: $x \in a$?

Answer: $x \in a \Leftrightarrow (\neg x \in f(x)) \Leftrightarrow (\neg x \in a)$

Conclusion:

$$\ldots, H \vdash (A \Leftrightarrow \neg A) \text{ for some } A,$$

$$\ldots, H \vdash \bot \text{ (by previous Lemma)}$$

$$\ldots \vdash \neg H$$

What did Cantor need in ... for this?

Existence of the *set* ω, existence of a *power set* of a set, *Separation* (to define a)

Building bigger sets (axioms)

Power set axiom:

$$\forall x \exists z \forall w \, (w \in z \Leftrightarrow (\forall v \, (v \in w \Rightarrow v \in x)))$$

Informally: "$z = \mathbb{P}(x)$"

Also useful

Union axiom:

$$\forall x \exists z \forall w \, (w \in z \Leftrightarrow (\exists v \, (w \in v \wedge v \in x)))$$

Informally: "$z = \bigcup x$"

Remaining axioms

Infinity axiom:

$$\exists I\ (\forall x\ (\mathsf{Empty}[x] \Rightarrow (x \in I)) \wedge \forall x \forall y\ ((x \in I \wedge \mathsf{Succ}[x, y]) \Rightarrow (y \in I)))$$

where Empty$[x]$ is the formula $\forall y\ (\neg(y \in x))$ "$x = \emptyset$"

and Succ$[x, y]$ is the formula $\forall z\ (z \in y \Leftrightarrow (z \in x \vee z = x))$ "$y = x \cup \{x\}$"

Also useful

Extensionality axiom:

$$\forall x \forall y\ ((\forall z\ (z \in x \Leftrightarrow z \in y)) \Rightarrow x = y)$$

Removing the infinity axiom makes sense: you get the *theory of finite sets*

Removing the extensionality axiom makes sense: you get the *intentional theory of sets*

Zermelo-Fraenkel set theory ($\mathcal{ZF}^*$)

- Equality axioms
- Replacement axiom schema
- Power set axiom
- Union axiom
- Infinity
- Extensionality

IV. Doing without the bugged axiom schema

Notations and trivial constructions: intersections

- Let $a \subseteq b$ be the formula $\forall w\ (w \in a \Rightarrow w \in b)$

  For every formula A, let $\forall x \in a, A$ abbreviate $\forall x\ (x \in a \Rightarrow A)$

  and $\exists x \in a, A$ abbreviate $\exists x\ (x \in a \wedge A)$

- Let "$w \in a \cap b$" be the formula $w \in a \wedge w \in b$

  Let "$z = a \cap b$" be the formula $\forall w\ (w \in z \Leftrightarrow$ "$w \in a \cap b$")

  We have $\mathcal{ZF}^* \vdash \forall a \forall b \exists z$ "$z = a \cap b$" (separation of a: $z = \{w \in a \mid w \in a \cap b\}$)

- Let "$w \in a \backslash b$" be the formula $w \in a \wedge \neg w \in b$

  Let "$z = a \backslash b$" be the formula $\forall w\ (w \in z \Leftrightarrow$ "$w \in a \backslash b$")

  We have $\mathcal{ZF}^* \vdash \forall a \forall b \exists z$ "$z = a \backslash b$" (separation of a again)

- Let "$w \in \bigcap a$" be the formula $\forall y, y \in a \Rightarrow w \in y$

  Let "$z = \bigcap a$" be the formula $\forall w\ (w \in z \Leftrightarrow$ "$w \in \bigcap a$")

  We have $\mathcal{ZF}^* \vdash \forall a\ ((\exists y (y \in a)) \Rightarrow \exists z$ "$z = \bigcap a$") (separation of y)

Basic constructions: singleton, doubleton

- Let "$z \in \{x\}$" be the formula $z = x$ and

  let "$z = \{x\}$" be the formula $\forall w \, (w \in z \Leftrightarrow$ "$z \in \{x\}$")

  $\mathcal{ZF}^* \vdash \forall x \exists z$ "$z = \{x\}$" (separation of power set: $z = \{w \in \mathbb{P}(x) \mid w \in \{x\}\}$)

- But what about "$\{x_1, x_2\}$" ? What set can we separate to get:

  $\mathcal{ZF}^* \vdash \forall x_1 \forall x_2 \exists z \forall w \, (w \in z \Leftrightarrow (w = x_1 \vee w = x_2))$

- When separation fails, try replacement

  Let one$[x]$ be the formula $\forall y \, (y \in x \Leftrightarrow$ Empty$[y])$

  Let two$[x]$ be the formula $\forall y \, (y \in x \Leftrightarrow$ (Empty$[y] \vee$ one$[y]))$

  $\mathcal{ZF}^* \vdash \exists x$ Empty$[x]$ (pure logic+separation), call it 0

  $\mathcal{ZF}^* \vdash \exists x$ one$[x]$ (power set of 0), call it 1

  $\mathcal{ZF}^* \vdash \exists x$ two$[x]$ (power set of 1+separation), call it 2

  $\mathcal{ZF}^* \vdash \forall x \, \neg($Empty$[x] \wedge$ one$[x])$ (pure logic)

  $\mathcal{ZF}^* \vdash \forall x_1 \forall x_2 \exists z \forall w \, (w \in z \Leftrightarrow (w = x_1 \vee w = x_2))$ replacement from 2

  with $A[z, y] :=$ ((Empty$[z] \wedge y = x_1) \vee$ (one$[z] \wedge y = x_2))$ ($\mathcal{ZF}^* \vdash$ functional(A))

Basic constructions: binary unions, pairs, cartesian product

- Let "$a \cup b$" be the set $\bigcup\{a, b\}$. In other words,

  let "$w \in a \cup b$" be the formula $w \in x \vee w \in y$

  let "$z = a \cup b$" be the formula $\forall w \, (w \in z \Leftrightarrow \text{"}w \in a \cup b\text{"})$

  $\mathcal{ZF}^* \vdash \forall x \forall y \exists z \text{ "}z = a \cup b\text{"}$ (build $\{a, b\}$ then use union axiom)

- Let "(x_1, x_2)" be the set $\{\{x_1\}, \{x_1, x_2\}\}$

  In other words, let "$z = (x_1, x_2)$" be the formula

  $\forall y \, (y \in z \Leftrightarrow ((\forall w \, (w \in y \Leftrightarrow (w = x_1))) \vee (\forall w \, (w \in y \Leftrightarrow (w = x_1 \vee w = x_2)))))$

  $\mathcal{ZF}^* \vdash \forall x_1 \, \forall x_2 \, \exists z \text{ "}z = (x_1, x_2)\text{"}$ (see previous slide)

- Let "$w \in a \times b$" be the formula $\exists y_1 \, \exists y_2 \, (y_1 \in a \wedge y_2 \in b \wedge \text{"}w = (y_1, y_2)\text{"})$

  Let "$z = a \times b$" be the formula $\forall w \, (w \in z \Leftrightarrow \text{"}w \in a \times b\text{"})$

  $\mathcal{ZF}^* \vdash \forall a \, \forall b \, \exists z \text{ "}z = a \times b\text{"}$ (separation of $\mathbb{P}(\mathbb{P}(a \cup b))$)

Basic constructions: functions

A function f is represented in Set Theory as its **graph**: the set of pairs $(x, f(x))$

- Let "$y = f(x)$" be the formula

$$\exists z \in f, \text{“}z = (x, y)\text{”}$$

- Let "$f : a \longrightarrow b$" be the formula

$$\exists z\,(f \subseteq z \wedge \text{“}z = a \times b\text{”} \wedge \forall x \forall y_1 \forall y_2\,(\text{“}y_1 = f(x)\text{”} \wedge \text{“}y_2 = f(x)\text{”} \Rightarrow y_1 = y_2))$$

Let "$c = a \longrightarrow b$" be the formula $\forall f\,(f \in c \Leftrightarrow \text{“}f : a \longrightarrow b\text{”})$

$\mathcal{ZF}^* \vdash \forall a\, \forall b\, \exists c\, \text{“}c = a \longrightarrow b\text{”}$ (separation of $\mathbb{P}(a \times b)$)

- Let "$f : a \longrightarrow b$ is injective" be the formula

$$\text{“}f : a \longrightarrow b\text{”} \wedge \forall x_1 \forall x_2 \forall y\,(\text{“}y = f(x_1)\text{”} \wedge \text{“}y = f(x_2)\text{”} \Rightarrow x_1 = x_2)$$

- Let "$f : a \longrightarrow b$ is surjective" be the formula

$$\text{“}f : a \longrightarrow b\text{”} \wedge \forall y\,(y \in b \Rightarrow \exists x\, \text{“}y = f(x)\text{”})$$

- Let "$f : a \longrightarrow b$ is bijective" be the formula

$$\text{“}f : a \longrightarrow b \text{ is injective”} \wedge \text{“}f : a \longrightarrow b \text{ is surjective”}$$

Conclusion: Dropping bugged axiom is tedious and difficult

Every construct justified by separation (or replacement) of previously constructed sets

Construction of bigger and bigger sets. . .

. . . is done by explicit use of power set and union axioms

In some sense, $\mathcal{ZF}^*$ implements Kronecker's idea: the sets that one wishes to talk about must be constructed in finitely many steps from basic sets

. . . as opposed to the "virtual" sets that the bugged axiom allowed (e.g. the set of all sets) whose size is un-constrained by the size of previously constructed sets

Notice: *Infinity axiom* is not required in any of the above theorems.

Neither is *Extensionality axiom*.

Extensionality is required for unicity of the above constructions (exercise!).

Without extensionality, you can have 2 different sets containing same elements

(echo: you can have 2 different programs computing the same input-output relation)

Important remarks

Hope: set theory is consistent

Claim: All the mathematics we know can be done in set theory

(possibly with the help of 0 to 3 extra axioms -see next week)

Let's start with arithmetic!

V. Arithmetic in set theory

Peano by Von Neumann

Reminder:

Empty$[x]$ is the formula $\forall y\ (\neg(y \in x))$ "$x = \emptyset$"

Succ$[x, y]$ is the formula $\forall z\ (z \in y \Leftrightarrow (z \in x \vee z = x))$ "$y = x \cup \{x\}$"

$\mathcal{ZF}^* \vdash \exists x$ Empty$[x]$ (already done, without using extensionality)

$\mathcal{ZF}^* \vdash \forall x \exists y$ Succ$[x, y]$ (singleton+binary union, no extensionality)

$\mathcal{ZF}^* \vdash \forall x \forall y\ \neg($Succ$[x, y] \wedge$ Empty$[y])$ (kind of already done)

$\mathcal{ZF}^* \vdash \forall x \forall y \forall y'\ (($Succ$[x, y] \wedge$ Succ$[x, y']) \Rightarrow y = y')$ (using extensionality)

In set theory, natural numbers are encoded as sets:

$0 :=\ \varnothing, 1 :=\ \{0\}, 2 :=\ \{0, 1\}, 3 :=\ \{0, 1, 2\}, \ldots$

The set of natural numbers itself

Remark: all natural numbers belong to the set I of infinity axiom

The set of natural numbers ω is the intersection of all subsets of I containing 0 and closed under successor:

Let $H[a]$ be the formula

$\forall x\ (\text{Empty}[x] \Rightarrow (x \in a))) \wedge (\forall x \forall y\ ((x \in a \wedge \text{Succ}[x, y]) \Rightarrow (y \in a))$

Let $\text{Nat}[n]$ be the formula $\forall x\ (H[x] \Rightarrow n \in x)$ *Induction principle!*

We have $\mathcal{ZF}^* \vdash \exists \omega \forall n\ (n \in \omega \Leftrightarrow \text{Nat}[n])$ (axiom of infinity+separation)

Remarks:

Natural numbers defined such that induction principle works

$\mathcal{ZF}^* \vdash H[\omega]$

Notation: $\forall^\omega x, A$ (resp. $\exists^\omega x, A$) stands for $\forall x \in \omega, A$ (resp. $\exists x \in \omega, A$)

Definition by recursion

It can be proved in $\mathcal{ZF}^*$ that if $f : B \times \omega \times A \longrightarrow A$ and $h : B \longrightarrow A$

then there is a unique function $g : B \times \omega \longrightarrow A$ such that

- $\forall b \in B, g(b, 0) = h(b)$ and
- $\forall b \in B, \forall n \in \omega, g(b, Sn) = f(b, n, g(b, n))$

where Sn stands for "the set $y \in \omega$ such that Succ$[n, y]$"

Writing the above as a formula A such that $\mathcal{ZF}^* \vdash A$ can be done, but very long!

Those in INF412 should be reminded of the PC on recursive functions

Everyone can have a look at Definition 3.1 of INF551 course notes

With this we can define two formulae Plus and Mult such that:

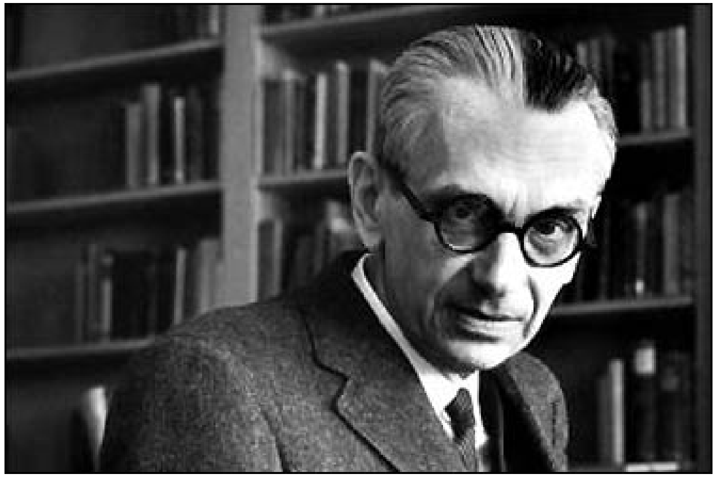
$\mathcal{ZF}^* \vdash \forall^\omega x, \forall^\omega y, \text{Empty}[x] \Rightarrow \text{Plus}[x, y, y]$

$\mathcal{ZF}^* \vdash \forall^\omega x, \forall^\omega x', \forall^\omega y, \forall^\omega z, \forall^\omega z', (\text{Succ}[x, x'] \wedge \text{Succ}[z, z'] \wedge \text{Plus}[x, y, z]) \Rightarrow \text{Plus}[x', y, z']$

$\mathcal{ZF}^* \vdash \forall^\omega x, \text{Empty}[x] \Rightarrow \text{Mult}[x, y, x]$

$\mathcal{ZF}^* \vdash \forall^\omega x, \forall^\omega x', \forall^\omega y, \forall^\omega z, \forall^\omega z', (\text{Succ}[x, x'] \wedge \text{Plus}[z, y, z'] \wedge \text{Mult}[x, y, z]) \Rightarrow \text{Mult}[x', y, z']$

VI. Church, Turing and Goedel crash the party again!



Back to Hilbert's programme. . .

Hilbert's programme was about the existence of a logic X, based on arithmetic, such that. . .

In Lecture 1, I claimed Hilbert's programme failed because of Church's, Turing's, and Goedel's theorems in Peano's arithmetic $\mathcal{PA}$.

Maybe $\mathcal{PA}$ was not the "right" X to accomplish Hilbert's programme!

What about set theory?

If it fails too, what about other theories we have not thought about yet?

Poor languages

Reminder: You have seen proofs for Church's and Goedel's theorems in $\mathcal{PA}$

...using a language with symbols 0, $=$, S,...

What if no such symbols? (as in set theory)

More generally, let us consider a language $\mathcal{L}_0$ in which we can construct formulae

- N, "to be a natural number"
- $Null$, "to be zero"
- $Succ$, "to be the successor of...",
- $Plus$, "to be the addition of ... and ...",
- $Mult$, "to be the multiplication of ... and ..."
- Eq, "to be two equal natural numbers"

In set theory, this is "simple":

$N[n]$ is just $n \in \omega$ and $Eq[n, m]$ is just $N[n] \wedge N[m] \wedge n = m$

Poor languages

Now, did we really use all the axioms of $\mathcal{PA}$ to prove Church's and Goedel's theorems?

(in infinite numbers because of the induction schema)

Def: Let $\mathcal{T}_0$ be the theory that expresses with N, $Null$, $Succ$, $Plus$, $Mult$, Eq the axioms of $\mathcal{PA}$ $(+, \times, =)$ without induction (see INF551 course notes, Def 5.2). Example:

$$\forall x \forall y \forall x' \forall y' \ ((N[x] \wedge N[y] \wedge Succ[x, x'] \wedge Succ[y, y'] \wedge Eq[x', y']) \Rightarrow Eq[x, y])$$

Remark and Idea: the axioms of $\mathcal{T}_0$ are in finite numbers...

...but $\mathcal{T}_0$ is sufficient for the constructs used in the representation theorem

(slide 29 of Lecture 3)

Def: $\mathbb{N}$-model: Any structure for language $\mathcal{L}_0$ where $\mathbb{N}$ interprets (elements satisfying) N, 0 interprets $Null$, $n \mapsto n+1$ interprets $Succ$, $+$ interprets $Plus$, $\times$ interprets $Mult$, $=$ interprets Eq

Rich theories in poor languages

General Church's theorem: Let $\mathcal{T}$ be a theory in $\mathcal{L}_0$,

that has an $\mathbb{N}$-model and where $\mathcal{T}_0$ can be proved.

Provability in $\mathcal{T}$ (i.e. $\mathcal{T} \vdash$) is undecidable

Proof:

we adapt representation of programs as formulae by replacing

- $\{^{S(t)}/_x\}A$ by $\exists x\ Succ[x, t] \wedge A$
- $\{^0/_x\}A$ by $\exists x\ Null[x] \wedge A$
- $t = u$ by $Eq[t, u]$
- ...

The representation theorem is adapted, with $\mathcal{T}$ and its $\mathbb{N}$-model in stead of $\mathcal{PA}$ and $\mathbb{N}$. To prove it we use the fact that $\mathcal{T}$ proves $\mathcal{T}_0$.

Application: Provability in $\mathcal{ZF}^*$ is undecidable.

What about inconsistent extensions? *e.g.* what if we take $\mathcal{T}_0, \perp$?

Side-question: Poor theories in poor languages

Specific Church's theorem:

Provability in the empty theory (in language $\mathcal{L}_0$) is undecidable

Proof:

Let H be the conjunction of all axioms of $\mathcal{T}_0$ (in **finite!** numbers)

Obvious (e.g. from INF412): $\mathcal{T}_0 \vdash A$ iff $\vdash H \Rightarrow A$

Examples:

- Language with 1 binary predicate symbol — undecidable
- Language with 1 predicate symbol of arity > 1 — undecidable
- Language with 1 unary predicate symbol and 1 term symbol of arity > 1 — undecidable

Some decidable theories

Provability in predicate logic (without axioms) is undecidable

But if symbols are governed by specific axioms, decidability can be recovered

Example: Presburger's arithmetic (arithmetic with $+$ but not $\times$)

Example: Euclid's geometry

Basically, decidability has no monotonicity properties:

if $\mathcal{T}_1 \subseteq \mathcal{T}_2 \subseteq \mathcal{T}_3$ and provability in $\mathcal{T}_2$ is decidable/undecidable,

nothing can be said of decidability of provability in $\mathcal{T}_1$ or $\mathcal{T}_3$.

Gödel's theorem

The implication Church $\Rightarrow$ Goedel still works!

General Goedel's theorem:

Let $\mathcal{T}$ be a theory in $\mathcal{L}_0$,

that has an $\mathbb{N}$-model,

and such that $\mathcal{T}$ is a decidable subset of the set of formulae.

There is a closed formula A such that neither $\mathcal{T} \vdash A$ nor $\mathcal{T} \vdash \neg A$

(Call such a formula a *Goedel formula*)

Proof: Proof-checking is still decidable (since belonging to $\mathcal{T}$ is decidable). Proof-search is still semi-decidable.

Run two proof-search algorithms in parallel, one on A the other on $\neg A$. If Goedel's theorem was false the parallel execution of the two programs would systematically terminate, providing algorithm to decide provability in $\mathcal{T}$, contradicting Church.

Application

Take $\mathcal{PA}$ and your favourite $\mathbb{N}$-model. Apply Goedel's theorem and get a Goedel formula A_1.

Take $\mathcal{PA}$, A_1 and extend your $\mathbb{N}$-model. Apply General Goedel's theorem and get a Goedel formula A_2.

Take $\mathcal{PA}$, A_1, A_2 and extend your $\mathbb{N}$-model. Apply General Goedel's theorem and get a Goedel formula A_3.

...

Goedel's theorem will always provide new Goedel formulae.

To be compared to the completion theorem (see in Lecture 1), that states:

A consistent theory can always be completed into another consistent theory where every closed formula A is such that either A is provable or $\neg A$ is provable.

Where is the catch???

Questions?