Incompleteness Phenomena in Mathematics: From Kurt Gödel to Harvey Friedman

Lasse Grinderslev Andersen

August 28th, 2016

Overview of this talk

- Genesis of modern rigorous mathematics
  - Logic & formal systems
  - Basic set theory
- Mathematical Incompleteness
- Reverse Mathematics (**optional**)
- Extremely strong case of (concrete) incompleteness

A few basic objects:

- Natural numbers: $\mathbb{N} = \{0, 1, 2, 3..\}$
- Integers: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3..\}$
- Rationals: $\mathbb{Q} = \{\frac{n}{m} | n \in \mathbb{Z}, m \in \mathbb{N}\}$
- Reals: $\mathbb{R} = \mathbb{Q} \cup \{\text{The Rest}\}$

Genesis of modern rigorous mathematics

The entire concept of function was put into question:

> "By about 1800 the mathematicians began to be concerned about the looseness in the concepts and proofs of the vast branches of analysis. The very concept of a function was not clear; the use of series without regard to convergence and divergence had produced paradoxes and disagreements"
>
> — M. Kline

The work of Cantor

Generalized the notion of infinity in several ways:

a **Transfinite orderings (ordinals)**

$$1, 2, 3, \ldots, n, \ldots, \omega, \omega + 1, \omega + 2, \omega + 3, \ldots, \omega + n, \ldots, 2 \cdot \omega, 3 \cdot \omega, \ldots, n \cdot \omega,$$

$$\ldots, \omega^2, \omega^3, \ldots, \omega^n, \ldots, \omega^3, \ldots, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots$$

$$\left.\omega^{\omega^{\omega^{\omega^{\omega}}}} \right\}\omega \; = \varepsilon_0, \varepsilon_0 + 1, \varepsilon_0 + 2, \varepsilon_0 + 3, \ldots, \varepsilon_0 + n, \ldots, \varepsilon_0^{\varepsilon_0}, \varepsilon_0^{\varepsilon_0^{\varepsilon_0}}, \ldots$$

The work of Cantor

Generalized the notion of infinity in several ways:

a **Transfinite orderings (ordinals)**

$$1, 2, 3, \ldots, n, \ldots, \omega, \omega+1, \omega+2, \omega+3, \ldots, \omega+n, \ldots, 2\cdot\omega, 3\cdot\omega, \ldots, n\cdot\omega,$$

$$\ldots, \omega^2, \omega^3, \ldots, \omega^n, \ldots, \omega^3, \ldots, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots$$

$$\left.\omega^{\omega^{\omega^{\omega^\omega}}}\right\}\omega = \varepsilon_0, \varepsilon_0+1, \varepsilon_0+2, \varepsilon_0+3, \ldots, \varepsilon_0+n, \ldots, \varepsilon_0^{\varepsilon_0}, \varepsilon_0^{\varepsilon_0^{\varepsilon_0}}, \ldots$$

More generally, two kinds exist

$$\text{Successor: } S(\alpha) = \alpha \cup \{\alpha\} \text{ and limit: } \lambda = \bigcup_{\alpha<\lambda} \alpha \Rightarrow On$$

The work of Cantor

Generalized the notion of infinity in several ways:

a **Transfinite orderings (ordinals)**

$$1, 2, 3, \ldots, n, \ldots, \omega, \omega+1, \omega+2, \omega+3, \ldots, \omega+n, \ldots, 2\cdot\omega, 3\cdot\omega, \ldots, n\cdot\omega,$$

$$\ldots, \omega^2, \omega^3, \ldots, \omega^n, \ldots, \omega^3, \ldots, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots$$

$$\left.\omega^{\omega^{\omega^{\omega^\omega}}}\right\}\omega = \varepsilon_0, \varepsilon_0+1, \varepsilon_0+2, \varepsilon_0+3, \ldots, \varepsilon_0+n, \ldots, \varepsilon_0^{\varepsilon_0}, \varepsilon_0^{\varepsilon_0^{\varepsilon_0}}, \ldots$$

More generally, two kinds exist

$$\text{Successor: } S(\alpha) = \alpha \cup \{\alpha\} \text{ and limit: } \lambda = \bigcup_{\alpha<\lambda} \alpha \Rightarrow On$$

The hierachy goes on and on and...

$$\ldots\ldots\ldots, \omega_1, \ldots \text{ where } \omega_1 = \bigcup \alpha \ , \ |\alpha| = \aleph_0$$

The work of Cantor

Generalized the notion of infinity in two ways:

b **Different degrees of infinity (cardinals)**

Countably infinite sets

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega = \aleph_0$$

Cantors Diagonal argument:

$$|\mathbb{N}| < |\mathbb{R}|$$

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$$

$$|\mathcal{P}(X)| = 2^{|X|} > |X|$$

Cantors continuum hypothesis

$$|\mathbb{R}| = \aleph_1 \text{ or } \aleph_{\alpha+1} = 2^{\aleph_\alpha}$$

The work of Cantor

Generalized the notion of infinity in two ways:

b **Different degrees of infinity (cardinals)**

$$
\begin{aligned}
s_1 &= \mathbf{0}\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \ldots\\
s_2 &= 1\ \mathbf{1}\ 1\ 1\ 1\ 1\ 1\ 1 \ldots\\
s_3 &= 0\ 1\ \mathbf{0}\ 1\ 0\ 1\ 0\ 0 \ldots\\
s_4 &= 1\ 0\ 1\ \mathbf{0}\ 1\ 0\ 1\ 1 \ldots\\
s_5 &= 1\ 1\ 0\ 1\ \mathbf{0}\ 1\ 1\ 1 \ldots\\
s_6 &= 0\ 0\ 1\ 1\ 0\ \mathbf{1}\ 1\ 0 \ldots\\
s_7 &= 1\ 0\ 0\ 0\ 1\ 0\ \mathbf{0}\ 0 \ldots\\
s_8 &= 1\ 0\ 0\ 0\ 1\ 0\ 1\ \mathbf{1} \ldots\\
&\vdots\\
s_{\text{troll}} &= \mathbf{1\ 0\ 1\ 1\ 1\ 0\ 1\ 0} \ldots
\end{aligned}
$$

Countably infinite sets

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega = \aleph_0$$

Cantors Diagonal argument:

$$|\mathbb{N}| < |\mathbb{R}|$$

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$$

$$|\mathcal{P}(X)| = 2^{|X|} > |X|$$

Cantors continuum hypothesis

$$|\mathbb{R}| = \aleph_1 \text{ or } \aleph_{\alpha+1} = 2^{\aleph_\alpha}$$

The work of Cantor

Generalized the notion of infinity in two ways:

b **Different degrees of infinity (cardinals)**

Input : **1 2 3 4 5 6 7 8**

P_1 : **0** 0 0 0 0 0 0 0 . . .

P_2 : 1 **1** 1 1 1 1 1 1 . . .

P_3 : 0 1 **0** 1 0 1 0 0 . . .

P_4 : 1 0 1 **0** 1 0 1 1 . . .

P_5 : 1 1 0 1 **0** 1 1 1 . . .

P_6 : 0 0 1 1 0 **1** 1 0 . . .

P_7 : 1 0 0 0 1 0 **0** 0 . . .

P_8 : 1 0 0 0 1 0 1 **1** . . .

$\vdots$

$P_{\text{troll}} = 1\ U\ 1\ 1\ 1\ U\ 1\ U \ldots$

Countably infinite sets

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega = \aleph_0$$

Cantors Diagonal argument:

$$|\mathbb{N}| < |\mathbb{R}|$$

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$$

$$|\mathcal{P}(X)| = 2^{|X|} > |X|$$

Cantors continuum hypothesis

$$|\mathbb{R}| = \aleph_1 \text{ or } \aleph_{\alpha+1} = 2^{\aleph_\alpha}$$

The work of Cantor

Generalized the notion of infinity in two ways:

b **Different degrees of infinity (cardinals)**

Countably infinite sets

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega = \aleph_0$$

Cantors Diagonal argument:

$$|\mathbb{N}| < |\mathbb{R}|$$

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$$

$$|\mathcal{P}(X)| = 2^{|X|} > |X|$$

Cantors continuum hypothesis

$$|\mathbb{R}| = \aleph_1 \text{ or } \aleph_{\alpha+1} = 2^{\aleph_\alpha}$$

Reception of Cantors work

The reception of Cantors discoveries were mixed...

> “I don’t know what predominates in Cantor’s theory - philosophy or theology, but I am sure that there is no mathematics there.”
>
> — Leopold Kronecker

Others were more positive:

> “No one shall expel us from the paradise that Cantor has created for us.”
>
> — David Hilbert

Hilbert program and the formalization of mathematics

Hilbert 'wanted to battle Kronecker on is own playing field':

- Formalize (infinitary) mathematics, making it a 'game of symbols'
- A game of symbols can be described and investigated by mathematics!
- Prove consistency of mathematics by finitary methods

A formal system example: 'MU'

The alphabet of the MU-system is {M, U, I} with rules of inference and axiom:

Rule I Any string ending with I, you may add U at the end.

Rule II Given string Mx beginning with M, x can be duplicated: Mxx

Rule III If III occur in a string, it may be replaced by U

Axiom MI

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

MI, MII, MIIII, MUI, MUIU □

Metatheorem

MU is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the `MU`-system is $\{\mathtt{M}, \mathtt{U}, \mathtt{I}\}$ with rules of inference and axiom:

Rule I Any string ending with `I`, you may add `U` at the end.

Rule II Given string `Mx` beginning with `M`, `x` can be duplicated: `Mxx`

Rule III If `III` occur in a string, it may be replaced by `U`

Axiom `MI`

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

`MI,MII,MIIII,MUI,MUIU` □

Metatheorem

`MU` is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the MU-system is $\{M, U, I\}$ with rules of inference and axiom:

Rule I Any string ending with I, you may add U at the end.

Rule II Given string Mx beginning with M, x can be duplicated: Mxx

Rule III If III occur in a string, it may be replaced by U

Axiom MI

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

MI,MII,MIIII,MUI,MUIU $\square$

Metatheorem

MU is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the `MU`-system is $\{\texttt{M}, \texttt{U}, \texttt{I}\}$ with rules of inference and axiom:

- **Rule I** Any string ending with `I`, you may add `U` at the end.
- **Rule II** Given string `Mx` beginning with `M`, `x` can be duplicated: `Mxx`
- **Rule III** If `III` occur in a string, it may be replaced by `U`
- **Axiom** `MI`

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

`MI,MII,MIIII,MUI,MUIU` □

Metatheorem

`MU` is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the `MU`-system is $\{\mathtt{M}, \mathtt{U}, \mathtt{I}\}$ with rules of inference and axiom:

Rule I Any string ending with `I`, you may add `U` at the end.

Rule II Given string `Mx` beginning with `M`, `x` can be duplicated: `Mxx`

Rule III If `III` occur in a string, it may be replaced by `U`

Axiom `MI`

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

`MI,MII,MIIII,MUI,MUIU` $\square$

Metatheorem

`MU` is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the MU-system is $\{M, U, I\}$ with rules of inference and axiom:

- **Rule I** Any string ending with I, you may add U at the end.
- **Rule II** Given string Mx beginning with M, x can be duplicated: Mxx
- **Rule III** If III occur in a string, it may be replaced by U
- **Axiom** MI

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

MI, MII, MIIII, MUI, MUIU $\square$

Metatheorem

MU is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the MU-system is $\{\mathtt{M}, \mathtt{U}, \mathtt{I}\}$ with rules of inference and axiom:

- **Rule I** Any string ending with I, you may add U at the end.
- **Rule II** Given string Mx beginning with M, x can be duplicated: Mxx
- **Rule III** If III occur in a string, it may be replaced by U
- **Axiom** MI

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

MI, MII, MIIII, MUI, MUIU $\square$

Metatheorem

MU is unprovable in MUI arithmetic.

A formal system example: 'MU'

The alphabet of the `MU`-system is $\{\mathtt{M}, \mathtt{U}, \mathtt{I}\}$ with rules of inference and axiom:

Rule I Any string ending with `I`, you may add `U` at the end.

Rule II Given string `Mx` beginning with `M`, `x` can be duplicated: `Mxx`

Rule III If `III` occur in a string, it may be replaced by `U`

Axiom `MI`

Theorem

MUIU (Notation: 'MU'-system $\vdash$ MUIU)

Proof.

`MI,MII,MIIII,MUI,MUIU` $\square$

Metatheorem

`MU` is unprovable in MUI arithmetic.

First Order Logic

The basis of most formal system (or language): $\mathcal{L}_{FOL}$
Logical symbols:

- **Equality** $=$
- **Connectives** '*or*': $\vee$, '*and*': $\wedge$, '*not*': $\neg$, '*if-then*': $\rightarrow$, '*if-and-only-if*': $\leftrightarrow$
- **Quantifiers** 'for-all': $\forall$, 'there exists': $\exists$
- **Variables** $x, y, z, ...$

Non-logical symbols:

- **Relations** $R_1, R_2, R_3, \ldots$
- **Functions** $f_1, f_2, f_3, \ldots$

Example:
For relation '$<$' (*larger than*) we have

$$\forall x \forall y \forall z \, (x < y \wedge y < z \rightarrow x < z) \tag{1}$$

Peano Arithmetic

Standard axioms of arithmetic in language $\mathcal{L}_{PA}$ with signature $0, S, +, *, <$

- P1 For every $n \neq 0$ there exists a unique k s.t. $n = S(k)$.
- P2 0 is not the successor of any n
- P3 For all n we have $n + 0 = n$
- P4 For all n, k we have $n + S(k) = S(n + k)$
- P5 For all n we have $n * 0 = 0$
- P6 For all n, k we have $n * S(k) = n * k + n$
- P7 For each formula $\phi(n)$ if $\phi(0)$ and $\phi(n) \rightarrow \phi(n + 1)$ then $\forall n \phi(n)$
- P8 Axioms for the relation $<$...

- The structure $\mathbb{N} = (\mathbb{N}, 0', S', +', *', <')$ is a model for *PA*: $\mathbb{N} \models PA$.
- There exists uncountably many *non-standard* models of *PA*
- There exits models of *PA* with arbitrary uncountable cardinality

Peano Arithmetic

Standard axioms of arithmetic in language $\mathcal{L}_{PA}$ with signature $0, S, +, *, <$

P1 $\forall n \exists ! k (n \neq 0 \wedge n = S(k))$

P2 $\neg \forall n (0 = S(n))$

P3 $\forall n (n + 0 = n)$

P4 $\forall n, k (n + S(k) = S(n + k))$

P5 $\forall n (n * 0 = 0)$

P6 $\forall n, k (n * S(k) = n * k + n)$

P7 $(\phi(0) \wedge (\phi(n) \rightarrow \phi(n+1)) \rightarrow \forall n \phi(n))$

P8 Axioms for the relation $<$...

- The structure $\mathbb{N} = (\mathbb{N}, 0', S', +', *', <')$ is a model for *PA*: $\mathbb{N} \models PA$.
- There exists uncountably many *non-standard* models of *PA*
- There exits models of *PA* with arbitrary uncountable cardinality

Peano Arithmetic

Standard axioms of arithmetic in language $\mathcal{L}_{PA}$ with signature $0, S, +, *, <$

P1 $\forall n \exists ! k(n \neq 0 \wedge n = S(k))$

P2 $\neg \forall n(0 = S(n))$

P3 $\forall n(n + 0 = n)$

P4 $\forall n, k(n + S(k) = S(n + k))$

P5 $\forall n(n * 0 = 0)$

P6 $\forall n, k(n * S(k) = n * k + n)$

P7 $(\phi(0) \wedge (\phi(n) \rightarrow \phi(n+1)) \rightarrow \forall n \phi(n))$

P8 Axioms for the relation $<$...

- The structure $\mathbb{N} = (\mathbb{N}, 0', S', +', *', <')$ is a model for *PA*: $\mathbb{N} \models PA$.
- There exists uncountably many *non-standard* models of *PA*
- There exits models of *PA* with arbitrary uncountable cardinality

Zermelo-Fraenkel set theory

Zermelo-Fraenkel set theory with axiom of choice (ZFC) formulated in $\mathcal{L}_{ZFC}$ with signature $\in$:

Pairing/Union If we have x, y we also have $\{x, y\}$ and $x \cup y$.

Empty set There exist an empty set $\emptyset$.

Infinity There exist a set x s.t. $\emptyset \in x$ and $\forall y \in x(y \cup \{x\})$.

Extensionabilty Two sets with the same elements are equal.

Foundation No set is an element of itself and no infinite descending chains $...x_3 \in x_2 \in x_1 \in x_0$ exist.

Powerset For all sets x exists a corresponding set $\mathcal{P}(x)$ of subsets of x.

Seperation For all sets a and formulas $\phi(x)$ there exists a set $y = \{z \in a | \phi(z)\}$.

Replacement If F is a function and x is a set, then $F''(x)$ is a set $(F''(x) = \{y | \forall z \in x(y = F(z))\}$.

choice For any set of sets x there exists a function that takes an element a of x as input and outputs a $z \in a$

Standard model of ZFC

Models of ZFC are structures $V = (V, \in)$.
Construction of a universe of sets by transfinite recursion along *On*

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \end{aligned}$$

A couple of remarks:

- $V_{2\omega} \models Z$, i.e. all axioms except replacement and choice
- There exist a countable model of ZFC!
- If κ is an *inaccessible* cardinal, $V_\kappa \models ZFC$.

Standard model of ZFC

Models of ZFC are structures $V = (V, \in)$.
Construction of a universe of sets by transfinite recursion along *On*

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \end{aligned}$$

A couple of remarks:

- $V_{2\omega} \models Z$, i.e. all axioms except replacement and choice
- There exist a countable model of ZFC!
- If κ is an *inaccessible* cardinal, $V_\kappa \models ZFC$.

Inaccessible cardinals

Definition

A cardinal κ is inaccessible if

1. $\kappa > \aleph_0$
2. For any cardinal $\lambda < \kappa$ we have $2^\lambda < \kappa$
3. For any union λ of $< \kappa$ ordinals, each which is $< \kappa$ we have $\lambda < \kappa$ (Assuming choice)

i.e. even larger than $\beth_\omega$ in the hierachy given by

$$\begin{aligned} \beth_0 &= \aleph_0 \\ \beth_{\alpha+1} &= 2^{\beth_\alpha} \\ \beth_\lambda &= \bigcup_{\alpha<\lambda} \beth_\alpha \text{ (where } \lambda \text{ a limit ordnial)} \end{aligned}$$

many inaccessible cardinals have been discovered, one larger than the other.

Inaccessible cardinals

Definition

A cardinal κ is inaccessible if

1. $\kappa > \aleph_0$
2. For any cardinal $\lambda < \kappa$ we have $2^\lambda < \kappa$
3. For any union λ of $< \kappa$ ordinals, each which is $< \kappa$ we have $\lambda < \kappa$ (Assuming choice)

i.e. even larger than $\beth_\omega$ in the hierachy given by

$$\begin{aligned} \beth_0 &= \aleph_0 \\ \beth_{\alpha+1} &= 2^{\beth_\alpha} \\ \beth_\lambda &= \bigcup_{\alpha<\lambda} \beth_\alpha \text{ (where } \lambda \text{ a limit ordnial)} \end{aligned}$$

many inaccessible cardinals have been discovered, one larger than the other.

Discovery of the incompleteness phenomena

Gödels first incompleteness theorem (for *PA*)

There exist a sentence σ where $\mathbb{N} \models \sigma$ but $PA \nvdash \sigma$(if PA is consistent)

Gödels first incompleteness theorem (for *ZFC*)

There exists sentences σ where $V \models \sigma$ but $ZFC \nvdash \sigma$ (if ZFC is consistent)

Gödels first incompleteness theorem

For any r.e. theory T strong enough to prove 'basic properties' of natural numbers, there exists sentences σ where $M \models \sigma$ but $T \nvdash \sigma$
(if T is consistent)

Discovery of the incompleteness phenomena

Gödels first incompleteness theorem (for *PA*)

There exist a sentence σ where $\mathbb{N} \models \sigma$ but $PA \nvdash \sigma$(if PA is consistent)

Gödels first incompleteness theorem (for *ZFC*)

There exists sentences σ where $V \models \sigma$ but $ZFC \nvdash \sigma$ (if ZFC is consistent)

Gödels first incompleteness theorem

For any r.e. theory T strong enough to prove 'basic properties' of natural numbers, there exists sentences σ where $M \models \sigma$ but $T \nvdash \sigma$
(if T is consistent)

Discovery of the incompleteness phenomena

Gödels first incompleteness theorem (for *PA*)

There exist a sentence σ where $\mathbb{N} \models \sigma$ but $PA \nvdash \sigma$(if PA is consistent)

Gödels first incompleteness theorem (for *ZFC*)

There exists sentences σ where $V \models \sigma$ but $ZFC \nvdash \sigma$ (if ZFC is consistent)

Gödels first incompleteness theorem

For any r.e. theory T strong enough to prove 'basic properties' of natural numbers, there exists sentences σ where $M \models \sigma$ but $T \nvdash \sigma$
(if T is consistent)

Discovery of the incompleteness phenomena

Gödels first incompleteness theorem (for *PA*)

There exist a sentence σ where $\mathbb{N} \models \sigma$ but $PA \nvdash \sigma$(if PA is consistent)

Gödels first incompleteness theorem (for *ZFC*)

There exists sentences σ where $V \models \sigma$ but $ZFC \nvdash \sigma$ (if ZFC is consistent)

Gödels first incompleteness theorem

For any r.e. theory T strong enough to prove 'basic properties' of natural numbers, there exists sentences σ where $M \models \sigma$ but $T \nvdash \sigma$
(if T is consistent)

Proof outline:

- Reduce the mechanical workings of the formal system into arithmetic on $\mathbb{N}$.
- i.e. assign unique numbers to formulas and sequences of formulas etc.
- Construct troll sentence σ expressing 'σ cannot be proved in T'.

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that GCH and axiom of choice is independent of ZFC
- 'There exists a ordinal κ that is inaccesable' is independent of ZFC
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that GCH and axiom of choice is independent of ZFC
- 'There exists a ordinal κ that is inaccesable' is independent of ZFC
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of PA $\leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that GCH and axiom of choice is independent of ZFC
- 'There exists a ordinal κ that is inaccesable' is independent of ZFC
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that GCH and axiom of choice is independent of ZFC
- 'There exists a ordinal κ that is inaccesable' is independent of ZFC
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that *GCH* and axiom of choice is independent of *ZFC*
- 'There exists a ordinal κ that is inaccesable' is independent of *ZFC*
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that *GCH* and axiom of choice is independent of *ZFC*
- 'There exists a ordinal κ that is inaccesable' is independent of *ZFC*
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

A couple of incompleteness examples

- The Gödel sentence σ of his first incompleteness theorem
- In every (consistent) system T we have $Con(T)$ incomplete in T (Gödels 2. incompleteness theorem, destroyed Hilberts program)
- In every (consistent) system T there exists diophantine equations incomplete in T
- Gentzen proved that $PRA + \epsilon_0 \vdash Con(PA)$ thus $PRA + \epsilon_0$ independent of PA
- Gödel and P. Cohen proved that GCH and axiom of choice is independent of ZFC
- 'There exists a ordinal κ that is inaccesable' is independent of ZFC
- Paris and Harrington proved that (a strong) finite ramsey theorem is independent of $PA \leftarrow$ (using non-standard models) **first non-foundational result**

Harvey Friedman: Reverse mathematics

Friedman was one of the founders of 'Reverse Mathematics' in the 1970s. The basic idea was:

- Forward Mathematics (= usual math): Theorems are deduced from axioms.
- Reverse Mathematics: Deduce the axioms from the theorem.
- A formal system proved equivalent to a theorem cannot be proved in a weaker subsystem: Independence!
- Classically a hierarchy of subsystems of second order arithmetic Z_2 have been used (second order = two variables: $n \in \mathbb{N}$ and $X \in \mathcal{P}(\mathbb{N})$)

Subsystems of reverse mathematics

Definition (Arithmetical Hierarchy)

1. ϕ/ψ is a Σ^0_0/Π^0_0-formula iff every quantifier is bounded
2. For $k \in \omega$, ϕ is a Σ^0_k-formula (resp. Π^0_k-formula) if it is of the form

   $$\exists n_1 \forall n_2 \exists n_3 \cdots n_k \ \psi \ \ (\text{respectively} \ \ \forall n_1 \exists n_2 \forall n_3 \cdots n_k \ \phi)$$

   where ϕ/ψ is as above.
   If η, σ is Σ^0_k, Π^0_k and

   $$\eta \leftrightarrow \sigma$$

   they are Δ^0_k formulas.

Thus formula-complexity increases with k and this is the arithmetical hierarchy.

Subsystems of reverse mathematics

All subsystems are embedded in Z_2:

Definition

(i) The axioms from PA excluding induction

(ii) The induction axiom:

$$\forall X \, (0 \in X \wedge \forall x \, (n \in X \rightarrow n + 1 \in X)) \rightarrow \forall n \, (n \in X)$$

(iii) The comprehension axiom:

$$\exists X \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ is a Z_2-formula in which X does not occur free.

!!: Problematic standard semantics: $X \in \mathcal{P}(\mathbb{N})$
This strong statement can be gradually weakened giving the base systems

Subsystems of reverse mathematics: RCA_0

The standard base theory for reverse mathematics

Definition (RCA_0)

(i) The basic (PA) axioms ((i) from before)

(ii) Σ^0_1-induction:

$$(\phi(0) \wedge \forall n\,(\phi(n) \to \phi(n+1))) \to \forall n\,\phi(n)$$

where $\phi(n)$ is Σ^0_1.

(ii) The scheme of Δ^0_1-comprehension, that is:

$$\forall n\,(\phi(n) \leftrightarrow \psi(n)) \to \exists X \forall n\,(n \in X \leftrightarrow \phi(n))$$

where $\phi(n)$ is a Σ^0_1-formula, $\psi(n)$ is a Π^0_1-formula $\psi(n)$.

RCA_0 proves in itself various results, e.g.

- Picard-Lindelöf theorem
- The intermediate value theorem on continuous real functions
- The existence of an algebraic closure for a countable field (but not its uniqueness)

Subsystems of reverse mathematics: RCA_0

The standard base theory for reverse mathematics

Definition (RCA_0)

(i) The basic (PA) axioms ((i) from before)

(ii) Σ^0_1-induction:

$$(\phi(0) \wedge \forall n\,(\phi(n) \to \phi(n+1))) \to \forall n\,\phi(n)$$

where $\phi(n)$ is Σ^0_1.

(ii) The scheme of Δ^0_1-comprehension, that is:

$$\forall n\,(\phi(n) \leftrightarrow \psi(n)) \to \exists X \forall n\,(n \in X \leftrightarrow \phi(n))$$

where $\phi(n)$ is a Σ^0_1-formula, $\psi(n)$ is a Π^0_1-formula $\psi(n)$.

RCA_0 proves in itself various results, e.g.

- Picard-Lindelöf theorem
- The intermediate value theorem on continuous real functions
- The existence of an algebraic closure for a countable field (but not its uniqueness)

Subsystems of reverse mathematics: WKL_0

Definition (WKL_0)

(i) The axioms of RCA_0.

(ii) Weak König's Lemma: Every infinite binary subtree has an infinite path.

Examples of theorems that WKL_0 is provably equivalent to (over RCA_0)

- Gödel's completeness theorem
- Every countable commutative ring has a prime ideal
- A continuous real function on the closed unit interval is Riemann integrable
- Peano's theorem on the existence of ODEs

Subsystems of reverse mathematics: WKL_0

Definition (WKL_0)

(i) The axioms of RCA_0.

(ii) Weak König's Lemma: Every infinite binary subtree has an infinite path.

Examples of theorems that WKL_0 is provably equivalent to (over RCA_0)

- Gödel's completeness theorem
- Every countable commutative ring has a prime ideal
- A continuous real function on the closed unit interval is Riemann integrable
- Peano's theorem on the existence of ODEs

Subsystems of reverse mathematics: ACA_0

Definition (ACA_0)

(i) RCA_0 + full second order induction

(ii) The arithmetical comprehension scheme, that is:

$$\exists X \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ in an arithmetical formula.

Examples of theorems that ACA_0 is provably equivalent to (over RCA_0)

- Königs lemma
- Bolzano-Weierstrass theorem
- Every countable commutative ring has a maximal ideal.

Subsystems of reverse mathematics: ACA_0

Definition (ACA_0)

(i) RCA_0 + full second order induction

(ii) The arithmetical comprehension scheme, that is:

$$\exists X \forall n \, (n \in X \leftrightarrow \varphi(n))$$

where $\varphi(n)$ in an arithmetical formula.

Examples of theorems that ACA_0 is provably equivalent to (over RCA_0)

- Königs lemma
- Bolzano-Weierstrass theorem
- Every countable commutative ring has a maximal ideal.

Subsystems of reverse mathematics: ATR_0

Definition (ATR_0)

(i) ACA_0

(iii) Transfinite recursion of $\theta(n, X)$ along any countable well-ordering

where $\theta(n, X)$ is an arithmetical formula with (at least) one free number and set variable n, X.

Examples of theorems that ATR_0 is provably equivalent to (over RCA_0)

- Any two countable well orderings are comparable.
- Ulm's theorem for countable reduced Abelian groups.
- Various classical results from descriptive set theory

Subsystems of reverse mathematics: ATR_0

Definition (ATR_0)

(i) ACA_0

(iii) Transfinite recursion of $\theta(n, X)$ along any countable well-ordering

where $\theta(n, X)$ is an arithmetical formula with (at least) one free number and set variable n, X.

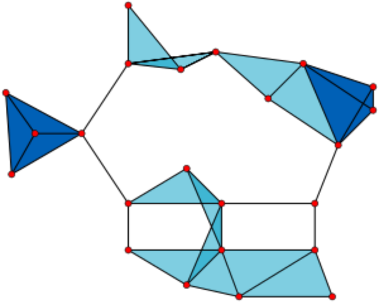
Examples of theorems that ATR_0 is provably equivalent to (over RCA_0)

- Any two countable well orderings are comparable.
- Ulm's theorem for countable reduced Abelian groups.
- Various classical results from descriptive set theory

Friedmans extremely strong concrete statements

Theorem (Invariant Maximal Clique Theorem)

Every order invariant graph $G = (V, E)$ on $\mathbb{Q}[0, n]^k$ has an upper Z^+ order invariant maximal clique.



Friedmans extremely strong concrete statements

Theorem (Invariant Maximal Clique Theorem)

Every order invariant graph $G = (V, E)$ on $\mathbb{Q}[0, n]^k$ has an upper Z^+ order invariant maximal clique.

Definition (Order invariant graph)

G as above is an order invariant graph iff for all order equivalent $x, y \in \mathbb{Q}[0, n]^{2k}$ we have $x \in E \to y \in E$ $(\subseteq \mathbb{Q}[0, n]^{2k})$

Definition (Order equivalence)

$x, y \in \mathbb{Q}[0, n]^{2k}$ are order euqivalent if for all $1 \leq i, j \leq 2k$, $x_i < x_j \leftrightarrow y_i < y_j$

Friedmans extremely strong concrete statements

Theorem (Invariant Maximal Clique Theorem)

Every order invariant graph $G = (V, E)$ on $\mathbb{Q}[0, n]^k$ has an upper Z^+ order invariant maximal clique.

Definition (Upper Z^+ Order invariant graph)

G as above is an order invariant graph iff for all upper Z^+ order equivalent $x, y \in \mathbb{Q}[0, n]^{2k}$ we have $x \in E \rightarrow y \in E$

Definition (Upper Z^+ Order equivalence)

$x, y \in \mathbb{Q}[0, n]^{2k}$ are upper Z^+ order euqivalent iff they are order equivalent and for all i, if $x_i \neq y_i$ then $x_j \geq x_i$, $x_j \geq y_i$, $y_j \geq x_i$ and $y_j \geq y_i$ lies in Z^+

Friedmans extremely strong concrete statements

Theorem (Invariant Maximal Clique Theorem)

Every order invariant graph $G = (V, E)$ on $\mathbb{Q}[0, n]^k$ has an upper Z^+ order invariant maximal clique.

Theorem

Con(SRP) + ACA' $\vdash$ IMCT and IMCT + ACA' $\vdash$ Con(SRP)

here $SRP = ZFC+$ 'there exists extremely large cardinals' and $ACA_0 < ACA' < ATR_0$.

Thank you for your attention

Thanks and dedication to Mette E. Larsen for slides, suggestions and neverending formalist trolling! :-)