Examples of theories - Soundness - Independence
0. Summary of previous episodes
Syntax of predicate logic

The notion of proof

The notion of model
Logic on Mars

What should we think, if the Martians had a deduction rule

\[
\Gamma \vdash A
\]

\[
\Gamma \vdash A \land B
\]

instead of

\[
\Gamma \vdash A \quad \Gamma \vdash B
\]

\[
\Gamma \vdash A \land B
\]
Logic on Mars

What should we think, if the Martians had a deduction rule

\[
\Gamma \vdash A \\
\Gamma \vdash A \land B
\]

instead of

\[
\Gamma \vdash A \quad \Gamma \vdash B \\
\Gamma \vdash A \land B
\]

? 

That, in Martian, the disjunction, and not the conjunction, is written $\land$
What is the answer to the question: “What is the meaning of symbol “∧”?”?

It is the deduction rule

\[
\Gamma \vdash A \quad \Gamma \vdash B \\
\hline
\Gamma \vdash A \land B
\]

(and the other deduction rules)
How do we know that we can deduce $A \land B$ from $A$ and $B$?

The rule

$$
\Gamma \vdash A \quad \Gamma \vdash B
\hline
\Gamma \vdash A \land B
$$

is part of the definition of the meaning of $\land$.
I. The notion of theory
Why theories?

A language: 0: constant, =: binary predicate symbol
A proposition 0 = 0
Natural deduction rules
No way to prove

0 = 0

We do not know what the symbol = means
May be it means “different”
A two-stage rocket

The logic (deduction rules) defines the meaning of the symbols \( \top, \bot, \neg, \land, \lor, \Rightarrow, \forall, \exists \)

The theory (axioms...) defines the meaning of the symbols 0, \( =, \leq, \in \), point, line...
How can we use an axiom in a proof?

Either

an extra rule

\[ \Gamma \vdash A \quad A \in \mathcal{T} \]

Or

a proof of \( \Gamma \vdash B \) in \( \mathcal{T} \): proof of \( \Gamma, \mathcal{T} \vdash B \)

\textbf{Axiom} rule of \( \text{la natural deduction} \)

Infinite theories: each proof uses a finite number of axioms

\( \Gamma, \mathcal{T}’ \vdash A \), for \( \mathcal{T}’ \) finite subset of \( \mathcal{T} \)
An exercise

Prove the proposition $0 = 0$ in the theory $\forall x \ (x = x)$
II. Examples of theories
A wide diversity of theories

- Express a **part** of mathematics: geometry, arithmetic...
- Express mathematics **"as a whole"**: set theory, type theory...
- Express a **specific knowledge** (expert systems): theory of tomato fungal diseases...
- Theories for which we are not so interested to build proofs, but whose **models** are interesting: group theory...
The theory of equality

Two axioms

Reflexivity (identity)

\[ \forall x \ (x = x) \]

Substitutivity (Leibniz)

Two objects are equal if every property that holds for one, also holds for the other

\[ \forall x \forall y \ (x = y \Rightarrow (x/z)A \Rightarrow (y/z)A) \]

Example

\[ \forall x \forall y \ (x = y \Rightarrow (5 \leq x \land x \leq 28) \Rightarrow (5 \leq y \land y \leq 28)) \]
In fact

A finite number of instances are enough

For each function symbol $f$ and for each index $i$
\[
\forall w_1 \ldots \forall w_{i-1} \forall w_{i+1} \ldots \forall w_n \forall x \forall y (x = y \Rightarrow f(w_1, \ldots, w_{i-1}, x, w_{i+1}, \ldots, w_n) = f(w_1, \ldots, w_{i-1}, y, w_{i+1}, \ldots, w_n))
\]

For each predicate symbol $P$ and for each index $i$
\[
\forall w_1 \ldots \forall w_{i-1} \forall w_{i+1} \ldots \forall w_n \forall x \forall y (x = y \Rightarrow P(w_1, \ldots, w_{i-1}, x, w_{i+1}, \ldots, w_n) \Rightarrow P(w_1, \ldots, w_{i-1}, y, w_{i+1}, \ldots, w_n))
\]
An exercise to start with: how can we express that there are an infinite number of objects?
An exercise to start with: how can we express that there are an infinite number of objects?

\[
\begin{align*}
f, \ a \\
\forall x \ \forall y \ (f(x) = f(y) \Rightarrow x = y) \\
\forall x \ \neg (a = f(x))
\end{align*}
\]
One way (among others) to build natural numbers: 
0 = a, 1 = f(a), 2 = f(f(a)), 3 = f(f(f(a))), ...
Better call a: 0 and f: S

∀x ∀y (S(x) = S(y) ⇒ x = y)
∀x ¬(0 = S(x))

Peano third and fourth axioms

Exercise: prove that 2 and 7 are different
Restrict the universe to natural numbers

The set of natural numbers contains 0 and is closed by $S$
Is it the only one?
Restrict the universe to natural numbers

The set of natural numbers contains 0 and is closed by $S$. Is it the only one?

No, but it is the smallest (intersection). Every property that is verified by 0 and that is closed by $S$ holds for every natural number

$$
\bar{\forall} ((0/z)A \Rightarrow \forall x ((x/z)A \Rightarrow (S(x)/z)A) \Rightarrow \forall y (y/z)A)
$$

Peano fifth axiom (scheme)
Almost done: addition and multiplication

\[
\forall y \ (0 + y = y)
\]

\[
\forall x \ \forall y \ (S(x) + y = S(x + y))
\]

\[
\forall y \ (0 \times y = 0)
\]

\[
\forall x \ \forall y \ (S(x) \times y = (x \times y) + y)
\]
An exercise: prove $\forall x \ (x + 0 = x)$?

$0 + 0 = 0$

If $x + 0 = x$ then $S(x) + 0 = S(x + 0) = S(x)$

What’s next?
An exercise: prove $\forall x \ (x + 0 = x)$?

$0 + 0 = 0$

If $x + 0 = x$ then $S(x) + 0 = S(x + 0) = S(x)$

What’s next?

The property $z + 0 = z$ holds for 0 and is closed by $S$

It holds for all numbers

$0 + 0 = 0 \Rightarrow \forall x \ (x + 0 = x \Rightarrow S(x) + 0 = S(x)) \Rightarrow \forall y \ y + 0 = y$

Fifth axiom: induction axiom
A fair question

Why + and × and not ↑

Because ↑ (and all the computable functions) are definable

But not ×, if only +
Another fair question

Why third, fourth, and fifth?

Another formulation of arithmetic with a predicate symbol $N$ characterizing the natural numbers

$$N(0)$$

$$\forall x \ (N(x) \Rightarrow N(S(x)))$$
Naive set theory

For each $A$ an axiom

$$\forall \exists E \forall y \ (y \in E \iff A)$$

Comprehension axiom scheme
Russell’s paradox (1902)

But

\[ \exists R \forall y \ (y \in R \iff \neg y \in y) \]

\[ R \in R \iff \neg R \in R \]

If \( R \in R \), then \( \neg R \in R \), hence \( \bot \)

Thus \( \neg R \in R \), therefore \( R \in R \), hence \( \bot \)
Zermelo’s set theory

Four particular cases of the comprehension scheme

Pairing:
\[ \forall x \forall y \exists z \forall w \ (w \in z \iff (w = x \lor w = y)) \]

Union:
\[ \forall x \exists z \forall w \ (w \in z \iff (\exists v \ (w \in v \land v \in x))) \]

Power set:
\[ \forall x \exists z \forall w \ (w \in z \iff (\forall v \ (v \in w \Rightarrow v \in x))) \]

Subset (separation, restricted comprehension):
\[ \forall A \exists x \forall z \forall w \ (w \in z \iff (w \in x \land A)) \]
No Russell’s paradox

\[ \exists R \forall y \ (y \in R \iff \neg y \in y) \]
The axiom of extensionality

\[ \forall E \forall F \ ((\forall x \ (x \in E \iff x \in F)) \Rightarrow E = F) \]
No set of all sets

Otherwise the separation axiom scheme becomes the comprehension scheme

\[ \forall \forall x \exists z \forall w \ (w \in z \iff (w \in x \land A)) \]

More direct: for each set \( E \) a set \( R_E \) such that

\[ \forall w \ (w \in R_E \iff (w \in E \land \neg w \in w)) \]

\[ R_E \in R_E \iff (R_E \in E \land \neg R_E \in R_E) \]

If \( R_E \in R_E \), then \( \neg R_E \in R_E \), hence \( \bot \)

Thus \( \neg R_E \in R_E \)

If \( R_E \in E \), then \( R_E \in R_E \), hence \( \bot \)

Therefore \( \neg R_E \in E \)
Natural numbers in set theory

Three possible definitions: Cantor - Peano - Von Neumann

Cantor:
3 is the set of all three element sets (equinumerosity, cardinals):
but no such set

An axiom expressing the existence of an infinite set $B$
Finite cardinals in $B$
3 is the set of all set of three elements of $B$
Natural numbers elements of the power set of the power set of $B$
Peano:
An axiom expressing the existence of an infinite set $B$
$S$ injective but not surjective from $B$ to $B$, $0$ an element that is not
in the image of $S$

Von Neumann:
$n$ set of natural numbers $< n$
$0 = \emptyset, 1 = \{\emptyset\}, 2 = \{\emptyset, \{\emptyset\}\}, ...$
Still an axiom expressing the existence of the set $\mathbb{N}$

Always an axiom expressing the existence of an infinite set (to be
continued)
Functions

Functions as graphs: sets of ordered pairs
Group theory

∀x∀y∀z ((x + y) + z) = (x + (y + z))
∀x (x + 0 = x)
∀x (0 + x = x)
∀x (I(x) + x = 0)
∀x (x + I(x) = 0)

Not very interesting as a deductive theory: \( I(e) = e, \)
\∀x I(I(x)) = x...

But its models are interesting \textit{per se}
III. The soundness theorem
How can we prove that a proposition is not provable?
The soundness theorem

If a sequent is provable, then it is valid in all models
The soundness theorem

A mere induction on proof structure

\[
\begin{array}{c}
\pi_1 \\
\Gamma \vdash A \\
\gamma_2 \\
\Gamma \vdash B \\
\hline
\Gamma \vdash A \land B
\end{array}
\]

Induction hypothesis: \( \Gamma \vdash A \) and \( \Gamma \vdash B \) valid in all models
\( \Gamma = \{G_1, \ldots, G_n\} \) and \( G = G_1 \land \ldots \land G_n \)
\( G \Rightarrow A \) and \( G \Rightarrow B \) valid in all models hence \( G \Rightarrow (A \land B) \) valid in all models
Same for the other rules
Soit

- $\mathcal{T}$ be a theory
- $\mathcal{M}$ be a model in which all the axioms of $\mathcal{T}$ are valid
- $A$ a proposition

If $A$ is provable in $\mathcal{T}$, then $A$ is valid in $\mathcal{M}$

There exists a finite subset $\Gamma$ of $\mathcal{T}$ such that $\Gamma \vdash A$ provable
$\Gamma \vdash A$ valid in $\mathcal{M}$ hence $A$ valid in $\mathcal{M}$
Contrapositive

Let

- $\mathcal{T}$ be a theory
- $\mathcal{M}$ be a model in which all the axioms of $\mathcal{T}$ are valid
- $A$ a proposition

If $A$ is not valid in $\mathcal{M}$ then $A$ is not provable in $\mathcal{T}$
The three forms of the soundness theorem

1. If $A$ provable in $\mathcal{T}$ then, $A$ valid in all models of $\mathcal{T}$

2. If there exists a model of $\mathcal{T}$ that is not a model of $A$, then $A$ is not provable in $\mathcal{T}$

3. If $\mathcal{T}$ has a model then $\mathcal{T}$ is consistent
A method to prove that $A$ is not provable in $\mathcal{T}$

Find a model $\mathcal{M}$ in which

all the axioms of $\mathcal{T}$ are valid

$A$ is not valid
An example

A theory $\mathcal{T}$ containing one axiom: $P(c) \lor Q(c)$

Prove that $P(c)$ is not provable in $\mathcal{T}$
Prove that $Q(c)$ is not provable in $\mathcal{T}$
Another example

A binary function symbol $+$, binary predicate symbol $=$

$(\mathbb{N}, \text{addition on } \mathbb{N}, \text{equality on } \mathbb{N})$ Is $\forall x \forall y \exists z \ (x + z = y)$ valid? Same question for $\mathbb{Z}$ equipped with addition and equality on $\mathbb{Z}$? Is the proposition $\forall x \forall y \exists z \ (x + z = y)$ provable?

Is the proposition $\forall x \forall y \ (x + y = y + x)$ valid in these models? In all models?
The axiom of parallels

[Diagram of a point and a line]

(after 22 centuries) not provable from the other axioms of geometry
The axiom of parallels

(after 22 centuries) not provable from the other axioms of geometry
The axiom of parallels

(after 22 centuries) not provable from the other axioms of geometry
The axiom of parallels

(after 22 centuries) not provable from the other axioms of geometry
The axiom of infinity

- $V_0 = \emptyset$
- $V_{i+1} = \mathcal{P}(V_i)$
- $V_\omega = \bigcup_i V_i.$

All the elements of $V_\omega$ are finite

- $M = V_\omega$

- $\hat{\equiv}$ function from $M \times M$ to $\{0, 1\}$ such that $\hat{\equiv}(a, b) = 1$ if $a$ is equal to $b$ and $\hat{\equiv}(a, b) = 0$ otherwise
- $\hat{\in}$ function from $M \times M$ to $\{0, 1\}$ such that $\hat{\in}(a, b) = 1$ is $a$ is an element of $b$ nd $\hat{\in}(a, b) = 0$ otherwise

Model of the axioms of pairing, union axiom, power set, subset, and extensionality

But not of the axiom of infinity
In TD: Examples of theories

Next time: the completeness theorem