Lecture 1

17 January 2008
08:58

Books

«Notes on logic and set theory»

— P.T. Johnstone

«Logic and structure»

— D. van Dalen.

«Logic induction and sets»

— T. Forster

Chapter 1. well-orderings and ordinals

1.1. Motivation

For the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$

we have proof by induction,

if $\begin{cases} P(0) \\ \forall n.\ P(n) \Rightarrow P(n+1) \end{cases}$ then $\forall n\ P(n)$.

definition and recursion,

$$0! = 1, \quad (n+1)! = (n+1)\, n!$$

idea, if we have dealt with an initial

idea, if we have dealt with an initial segment of $\mathbb{N}$, then there is a next element.

if we know to go on we can go on for ever.

how general is this?

1.2. Totally ordered sets

definition:

A totally ordered set $(X, <)$ is a set X with a binary relation $<$ s.t.

$$x<y \text{ and } y<z \Rightarrow x<z \quad \forall x,y,z$$

$$x \not< x \quad \forall x$$

either $x<y$ or $x=y$ or $y<x$ $\forall x,y$ $\square$

N.B. only one possibility holds in trichotomy.

$S^1 = \{(x,y) : x^2+y^2=1\}$ with $(x_1, y_1) < (x_2, y_2)$ iff $y_1 < y_2$ is not totally ordered, $\because (-1,0)$

and $(1,0)$ do not satisfy trichotomy.

<u>example:</u>

the lexicographic ordering.

let Σ be a set [alphabet] and write

$\Sigma^* = List(\Sigma)$ for the set of finite sequences

$\underline{a} = (a_1, \ldots, a_n)$ of members of Σ.

it's good taste to include the empty word.

now suppose we have a total order $<$ on Σ.

define $<$ on Σ^* as follows,

$\underline{a} = (a_1, \ldots, a_n) < \underline{b} = (b_1, \ldots, b_m)$ iff $\exists\, i$ s.t.

$a_j = b_j$ for $j < i$ and either $\nexists\, a_i$ while $\exists\, b_i$,

or $a_i < b_i$

this is the order at which words appear in

a dictionary.

we check trichotomy.

suppose $\underline{a} \neq \underline{b}$.

let i be the first place where they differ.

either one is defined at i and the other isn't, in which case second < first, or a_i, b_i both exist and $a_i < b_i \Rightarrow \underline{a} < \underline{b}$, $b_i < a_i \Rightarrow \underline{b} < \underline{a}$ $\square$.

write $x \leq y$ for $x < y$ or $x = y$.

we can define totally ordered sets in terms of $\leq$.

$x \leq y$ and $y \leq z \Rightarrow x \leq z \quad \forall x, y, z$

$x \leq y$ and $y \leq x \Rightarrow x = y \quad \forall x, y$

$x \leq y$ or $y \leq x \quad \forall x, y$.

1.3. Well-orderings

definition:

A well-ordered set $(A, <)$ is a totally set satisfying if $\emptyset \neq X \subseteq A$ then X has a $<$-least element $\square$

examples:

$\{1-\frac{1}{n} : n \geq 1\} \cup \{1\}$ is order-isomorphic to $\mathbb{N}$, with an extra point on top.

$\{1-\frac{1}{n} : n \geq 1\} \cup \{2-\frac{1}{n} : n \geq 1\}$.

suppose $X \neq \emptyset$ in the set above.

either X intersects $\{1-\frac{1}{n} : n \geq 1\}$ and we can take a minimum element, or X only intersects $\{2-\frac{1}{n} : n \geq 1\}$ and we can take a minimum element.

what about $\{m-\frac{1}{n} : n, m \geq 1\}$? $\square$

is $\mathbb{N}^*$ with the lexicographic ordering well-ordered?

Lecture 2

19 January 2008
09:04

proposition:

A total ordering is a well-ordering if and only if it satisfies principles of $<$-induction.

proof:

induction principle says

if $\forall a \, (\forall b < a, \, b \in P \Rightarrow a \in P)$ then $a \in P$.

suppose $(A, <)$ is well-ordered.

take $P \subseteq A$ satisfying the induction condition.

suppose $P \neq A$, then $A - P \neq \emptyset$ and we take $a \in A - P$ $<$-minimal.

then $\forall b < a$, $b \in P$ $\because$ inf $A \in P$ vacuously.

so by induction condition, $a \in P$ ※.

conversely suppose $(A, <)$ satisfies induction.

take $X \subseteq A$ with no $<$-minimal element.

then $A - X$ satisfies the induction condition,

$\because$ if $\forall b < a$, $b \notin X$ then $a \notin X$ else it is

$<$-minimal

so by induction $A - X = A$ and $X = \emptyset$

so if $X \neq \emptyset$ then X has a minimal element $\square$.

if $(X, \leqslant)$ is a total order, an initial

segment is $S \subseteq X$ s.t. $x \leqslant y \in S \Rightarrow x \in S$.

an initial segment S is proper if $S \neq A$.

$A_{<a} := \{x \mid x < a\}$ is an initial segment.

in a well-ordering, all proper initial

segments are of the form $A_{<a}$ for

some a.

indeed, suppose S is a proper initial

segment.

$A - S \neq \emptyset$ and we take $a \in A - S$ $<$-minimal.

$\forall b < a$, $b \in S$ by minimality.

so $A_{<a} \in S$

if $x \in S$ then $x \not> a$ else $a \in S$ $\therefore$ S is initial.

$\therefore$ $S = A_{<a}$.

so for each proper initial segment B of $(A, <)$ well-order, $\exists$ $s(B) \in A$ with $B = A_{<s(B)}$. ⊕

conversely if $(A, <)$ satisfies ⊕ then A is well-ordered.

1.4 Order isomorphisms

let $(A, <)$ and $(B, <)$ be well-orderings.

definition:

An order isomorphism from A to B is a map $: A \mapsto B$ which is bijective and s.t. $a < a' \Rightarrow f(a) < f(a')$ $\forall a, a' \in A$ $\square$

note $a < a' \iff f(a) < f(a')$ by trichotomy, so

the inverse is also an order isomorphism.

if f is such, then

$$B_{<f(a)} = f(A_{<a}).$$

we are interested in partial order isomorphisms.

that is order isomorphisms $A' \to B'$ between

initial segments of A and B.

suppose f is an order isomorphism.

note that $f(a) = s(B_{<f(a)}) = s(f(A_{<a}))$

lemma:

If $f, g : A' \to B'$ are order isomorphisms then $f = g$.

proof:

by induction, suppose $f = g$ on $A_{<a}$,

then $f(a) = s f(A_{<a}) = s g(A_{<a}) = g(a)$ $\square$.

N.B. induction says suppose (P holds on $A_{<a}$ $\Rightarrow$

P holds at a) then P holds on A.

suppose $f_1 : A_1 \mapsto B_1$

$f_2 : A_2 \mapsto B_2$

are order isomorphisms between initial segments of A and B.

then $f_1|_{A_1 \cap A_2} = f_2|_{A_1 \cap A_2}$

let $(f_i : A_i \mapsto B_i)_{i \in I}$ be the family of all order isomorphisms between initial segments of A and B

then we have an order isomorphism

$$\bigcup A_i = A' \xrightarrow[f' := \bigcup f_i]{} \bigcup B_i = B'$$

with $f'(a) = b$ iff $\exists f_i(a) = b$

suppose both A' and B' are proper.

then we can extend f' to an order isomorphism $A' \cup \{s(A')\} \mapsto B' \cup \{s(B')\}$ taking $s(A')$ to $s(B')$ ※.

Theorem:

Let $(A, <)$ and $(B, <)$ be well-orderings. Then A is uniquely order isomorphic to an initial segment of B, or the other way round.

proof:

either $A' = A$ or $B' = B$ [AS ABOVE].

$$a < a' \Leftrightarrow f(a) < f(a')$$

and so the inverse is an order isomorphism $\square$.

Lecture 3

22 January 2008
09:04

1.5 Ordinals as order types

want to regard a well-ordering $(A, <)$ as having a "shape" independently of what are the elements of A, i.e. we want to consider of up to order isomorphism.

formally we say $(A, <)$ and $(A', <')$ have the same order type and so represent the same ordinal iff they are order isomorphic.

[Frege], an ordinal is an equivalence class of well-orderings under order isomorphism.

notation, write $\alpha, \beta, \ldots$ for ordinals and [Cantor] $\breve{A} = \alpha$ for A is a representative of α.

there are in fact canonical representatives for α.

we have an ordering on ordinals, $\alpha \underset{<}{\leq} \beta$

some

just when for all !! $\bar{A} = \alpha$, $\bar{B} = \beta$, A

initial

is a proper initial segment of B.

recall, order isomorphisms between initial segments of well-orderings are unique.

$\therefore$ if $\bar{A} \leq \bar{B}$ and $\bar{B} \leq \bar{A}$ then $\bar{A} = \bar{B}$.

indeed, if either $\bar{A} < \bar{B}$ or $\bar{B} < \bar{A}$ then we'd have $\bar{A} < \bar{A}$ and in a well-ordered set cannot be order isomorphic to a proper initial segment of itself, the unique order isomorphism is the identity.

either $\bar{A} \leq \bar{B}$ or $\bar{B} \geq \bar{A}$.

so it follows that On, the collection of ordinals is totally ordered by $<$.

the proper initial segments of a well-order A are of the form $A_{<a}$ for some unique $a \in A$.

so the proper initial segments are order isomorphic to A under the ___?___ relation $\subset$.

$\therefore$ for any ordinal α, $\{\beta : \beta < \alpha\}$ is "order isomorphic to α", has order type α.

suppose $\emptyset \neq X \subseteq On$.

take $\alpha \in X$.

either α is $<$-minimal in X, or

$$\{\beta < \alpha : \beta \in X\} \neq \emptyset$$

and so we can find a $<$-minimal element β, this is a $<$-minimal element of X.

thus On is well-ordered by $<$.

Burali-Forti paradox:

Let Ω be the order type of On.

Then On is order isomorphic to $\{\alpha : \alpha < \Omega\} = On_{<\Omega}$ and On is order isomorphic to an initial segment of themselves $\times\!\!\times$.

Cantor's paradox:

Let V be the collection of all sets, then $\mathcal{P}(V) = V$ $\times\!\!\times$.

1.6 Ordinal arithmetic

1.) the least ordinal 0 is the order type of the $\emptyset$ well-ordering.

2.) suppose $\alpha = \bar{A}$, take $\infty \notin A$ and order $A \cup \{\infty\}$ by extending the order on A by $a < \infty$ $\forall a \in A$.

this is a well-ordering of order type $\alpha + 1$.

observe if $\bar{A} = \alpha$ and A has a maximal element a_0 say then $\beta = \overline{A_{<a_0}}$ is s.t.

$\alpha = \beta + 1$.

ordinals of this kind are successor ordinals.

the others are

- 0

? - the limit ordinals that is the non-0 ordinals with the property that $\beta < \alpha$ then there is γ s.t. $\beta < \gamma < \alpha$.

3.) let $\alpha = \bar{A}$, $\beta = \bar{B}$.

take $A + B$ disjoint union, e.g. $\{0\} \times A \cup \{1\} \times B$.

extend the order on A, B.

by setting $a < b$ $\forall a \in A$, $b \in B$, we have a well-ordering.

4.) let $\alpha = \bar{A}$, $\beta = \bar{B}$.

take the product $A \times B$ and order it antilexicographically by

$(a, b) < (a', b')$

$\iff b < b'$ or $(b = b'$ and $a < a')$.

if $X \neq \emptyset \subseteq A \times B$, we first choose b_0 least

s.t. $\exists a$ s.t. $(a, b_0) \in X$.

$X_{b_0} = \{a : (a, b_0) \in X\} \neq \emptyset \subseteq A$ and we take

a_0 least in it, check (a_0, b_0) least in X.

5.) suprema of sets of ordinals to be explained.

some ordinals

$$
\begin{aligned}
& 1 \\
& 2 \\
& \vdots \\
& \omega \\
& \omega + 1 \qquad \text{N.B. } 1 + \omega = \omega. \\
& \vdots \\
\omega \cdot 2 = \ & \omega + \omega \qquad \text{N.B. } 2 \cdot \omega = \omega \\
& \omega \cdot 3 \\
& \vdots \\
\omega^2 = \ & \omega \cdot \omega = \omega \cdot (1 + \omega) = \omega + \omega^2 \\
& \vdots \\
& \omega^\omega = \omega^{1+\omega} = \omega \cdot \omega^\omega \\
& \vdots \\
\omega^{\varepsilon_0} = \ & \varepsilon_0
\end{aligned}
$$

Lecture 4

22 January 2008
11:36

if $\beta \geq \alpha$, set $\alpha - \beta = 0$

if $\beta \leq \alpha$, take $\bar{A} = \alpha$ and B an initial segment with $\bar{B} = \beta$.

then $A - B \subseteq A$ is well-ordered and its order type is $\alpha - \beta$.

let X be a set of ordinals.

assume we have representatives A_β for $\beta \in X$ with the property that if $\beta \leq \gamma$ in X then A_β is an initial segment of A_γ.

then $\bigcup_{\beta \in X} A_\beta = A$ is well-ordered by union of the order relations.

clearly, e.g. $a < b < c \in A$ then $c \in A_\beta$

then $a < b < c \in A_\beta$ so $a < c \in A_\beta$ etc..

if $\emptyset \neq X \subseteq A$ then some $X \cap A_\beta \neq \emptyset$ and a $<$-minimal element in A_β is a $<$-

minimal element of A $\therefore A_\beta$ is an initial segment of A.

does the assumption matter?

no.

① if we take any $\bar{A}_\beta = \beta$ then we can quotient the $\cup A_\beta$ by identifying elements which correspond under the unique order isomorphisms between initial segments.

② for each $\beta \in X$ we could take $\{\rho : \rho < \beta\} = On_{<\beta}$ which is of order type β, and then the assumption is satisfied.

note, $\alpha + \sup_{i \in I} \beta_i = \sup_{i \in I} \alpha + \beta_i$, $I \neq \emptyset$

$$\alpha \sup_{i \in I} \beta_i = \sup_{i \in I} \alpha \beta_i$$

Hartogs's lemma:

Let X be a set. Then $\exists$ a least ordinal $\gamma = \gamma(X)$ s.t. γ does not inject into X, i.e. if $\bar{C} = \gamma$

then C does not inject into X.

<u>proof:</u>

consider the set

$W = \{R \subseteq X \times X : R$ is a well-ordering of

some subset of $X\}$.

have $W \longrightarrow On$; $R \longrightarrow \rho = \bar{R}$ the

ordinal represented.

the image Z is a set of ordinals.

$\because W$ is closed under initial segments, Z ???

is an initial segment of the ordinals.

so Z is well-ordered.

the order type γ of Z is s.t. $Z = On_{<\gamma}$,

??? $\gamma \notin Z$ and is least with this property $\square$.

recall $\omega = \bar{\mathbb{N}}$, we might set $\omega_0 = \omega$.

what is $\gamma(\mathbb{N})$?

it is the least uncountable ordinal.

set $\omega_1 = \gamma(\omega_0)$.

then we have $\gamma(\omega_1) = \omega_2$ so on.

1.7 Recursion theorem

Theorem:

suppose $(A, <)$ is a well-ordered set and X a set and

$$g : \mathrm{Ftl}(A, X) \mapsto X.$$

Then $\exists$ a unique function $f : A \mapsto X$ s.t. $f(a) = g(f|_{A_{<a}})$.

example of use:

suppose $(A, <)$ and $(B, <)$ are well-orderings.

set $X = B \cup \{\infty\}$, where $\infty \notin B$.

then by the theorem $\exists$ a function

$f : A \mapsto B \cup \{\infty\}$ s.t. $f(a) = s\{f(a') : a' < a\}$

as long as $\{f(a'): a' < a\}$ is an initial segment of B, and ∞ otherwise.

either ∞ is not in the image of f,

then f is an order isomorphism from A to an initial segment of B.

or, ∞ is in the image of f.

take a_0 least s.t. $f(a_0) = \infty$.

then $f|_{A_{<a_0}}$ is an order isomorphism from $A_{<a_0}$ to an initial segment of B, which is not proper $\because f(a_0) = \infty$, and the inverse is an order isomorphism from B to a proper initial segment of A $\square$.

<u>proof of theorem:</u>

let an attempt be a map ϕ where

$\phi: A' \mapsto X$, A' an initial segment of A,

$\phi(a) = g(\phi|_{A_{<a}})$ $\forall a \in A'$.

by induction we see that if $\phi_1 : A_1 \mapsto X$

and $\phi_2 : A_2 \mapsto X$ are attempts then $\phi_1 = \phi_2$

on $A_1 \cap A_2 = A_1$ or A_2 in this case.

induction step

$$\phi_1(a) = g(\phi_1|_{A_{<a}}) = g(\phi_2|_{A_{<a}}) = \phi_2(a).$$

so we take $f = \bigcup \phi$, i.e. $f(a) = x$ iff $\exists$

attempt ϕ s.t. $\phi(a) = x$.

then $f(a) = g(f|_{A_{<a}})$ for any $a \in \operatorname{dom} f = \bigcup \operatorname{dom} \phi$.

$\operatorname{dom} f = A'$ is itself an initial and f is an

attempt.

[not finished].

Lecture 5

26 January 2008
09:06

for now we want also to take a recursion theorem where we replace $(A, <)$ by $(On, <)$.

write $Fel(On, V) = \{\phi : \phi$ is defined on some subset of On, and $\phi(\alpha)$ is a set where defined$\}$.

set of all sets.

given $G : Fel(On, V) \to V$, $\exists$ a unique $F : On \to V$ with the property that $F(\alpha) = G(F|_{On_{<\alpha}})$.

<u>examples:</u>

① for fixed α, we define $\alpha + \beta$ by recursion on $\beta \in On$ as follows.

$$\alpha + 0 = \alpha$$

$$\alpha + (\beta + 1) = (\alpha + \beta) + 1$$

$$\alpha + \lambda = \sup_{\beta < \lambda} \alpha + \beta, \quad \lambda \text{ limit}$$

what is G ?

it could be a function defined labouriously

as follows.

G looks at ϕ, if ϕ is everywhere

undefined, $G(\phi) = \alpha$.

if ϕ is defined on an initial segment

of ordinals with greatest element β_0

and $\phi(\beta_0)$ is itself an ordinal,

$G(\phi) = \phi(\beta_0) + 1$.

if ϕ is .... $\neq \emptyset$ with no greatest

element and $\mathrm{rge}(\phi) \subseteq On$ then

$G(\phi) = \sup(\mathrm{rge}(\phi))$.

else G is whatever, 0 say.

or, $G(\phi) = \alpha \vee \sup\{\phi(\beta)+1 : \beta$ ordinal in

domain of ϕ and $\phi(\beta)$ an ordinal$\}$.

② for fixed α, define $\alpha \times \beta$ by recursion on $\beta \in On$ as follows.

$$\alpha \cdot 0 = 0$$

$$\alpha(\beta+1) = \alpha \cdot \beta + \alpha$$

$$\alpha \cdot \lambda = \sup_{\beta<\lambda} \alpha \cdot \beta, \quad \lambda \text{ limit.}$$

③ for fixed α, define α^β by recursion

on $\beta \in On$ as follows.

$$\alpha^0 = 1$$

$$\alpha^{\beta+1} = (\alpha^\beta) \cdot \alpha$$

$$\alpha^\lambda = \sup_{\beta<\lambda} \alpha^\beta, \quad \lambda \text{ limit.}$$

note we can show easily by induction

on β that if α and β are countable

then so is α^β.

Chapter 2, Axiom of choice

2.1 Statement and some observations

Axiom of choice:

Let X be a set of non-empty sets.

Then there is a function

$$c : X \mapsto \bigcup X = \bigcup\{x : x \in X\}$$

with the property that $c(x) \in x \ \forall x \in X$. $\square$.

let $\{x_i : i \in I\}$ be an indexed family of non-empty sets.

then $\exists\ c : I \mapsto \bigcup\{x_i : i \in I\}$ s.t. $c(i) \in x_i$ $\forall\ i \in I$.

suppose $Z \xrightarrow{p} I$ is a surjective map.

then $\exists$ map $I \xrightarrow{s} Z$ s.t. $p \circ s : I \mapsto I$ is the identity.

in case I is finite, there is no problem.

if $I = \{1, \dots, n\}$, we take $c_i \in x_i$, $1 \leq i \leq n$ and define $c(i) = c_i \ \forall\ 1 \leq i \leq n$.

on the other hand, it is no help at all if the x_i are finite.

even then it depends on the nature of the sets.

[Russel], we can pick members from an infinite collection of pairs of shoes, but can we take ... ... of pairs of socks?

2.2 Zorn's lemma

definition:

A partially ordered set $(X, <)$ or $(X, \leq)$ is one s.t. $x \leq y, y \leq z \Rightarrow x \leq z$ and $x \leq y, y \leq x \Rightarrow x = y$. A subset C of a poset is a chain just when it is a totally ordered set. $\square$

an upper bound for $Y \subseteq X$, X a poset, is an element $y_0 \in X$ with $y_0 \geq y$ $\forall y \in Y$.

a maximal element in a poset $(X, \leq)$ is an element x_0 s.t. $\forall x \in X$, $x \geq x_0 \Rightarrow x = x_0$.

Zorn's lemma:

Let $(X, \leq)$ be a poset in which every chain has an upper bound. Then X has a maximal element.

Lecture 6

29 January 2008
09:09

~~proof:~~

suppose that X has no maximal elements.

take a chain C, it has an upper bound

$\bar{u}_c$ and by supposition it is not maximal

and so we can take $u_c > \bar{u}_c$.

thus every chain has a strict upper bound

i.e. $\exists\, u_c > x \;\; \forall x \in C$.

by AC there is a function

u: chains in $X \longrightarrow X$

with $u(C)$ a strict upper bound $\forall\, C$.

by Hartog $\exists$ an ordinal $\gamma(X)$ least

s.t. $\gamma(X)$ does not embed in X.

define $f : On_{<\gamma(X)} \hookrightarrow X$ by recursion as

follows.

$$f(\alpha) = \begin{cases} u(f(On_{<\alpha})), & f(On_{<\alpha}) \text{ is a chain} \end{cases}$$

$\quad \left\{ u(\emptyset), \qquad \text{otherwise.} \right.$

claim $\forall \alpha < \gamma(X)$, $f(On_{<\alpha})$ is a chain.

prove by induction on α.

suppose $\forall \beta < \alpha$, $f(On_{<\beta})$ is a chain

in case $\alpha = 0$ or a limit ordinal,

$$On_{<\alpha} = \bigcup_{\beta<\alpha} On_{<\beta}$$

and so $f(On_{<\alpha}) = \bigcup_{\beta<\alpha} f(On_{<\beta})$, a nested

union of chains, so is a chain.

in case $\alpha = \beta + 1$ then $On_{<\alpha} = On_{<\beta} \cup \{\beta\}$ and

so $f(On_{<\alpha}) = f(On_{<\beta}) \cup f(\beta)$, which is

a chain ~~together~~ with a proper upper

bound and so a chain.

$\therefore f(On_{<\alpha})$ is a chain $\forall \alpha < \gamma(X)$.

thus the first condition on definition of

f always applies.

so if $\beta < \alpha < \gamma(X)$, $\overset{???}{\neq}$, $\nearrow$???

$$f(\alpha) = u(f(On_{<\alpha})) > f(\beta).$$

thus $f : On_{<\gamma(x)} \mapsto X$ is injective $\times$ $\square$.

we have really used a modified principle of induction.

suppose $P \subseteq On_{<\gamma}$ satisfies the modified induction condition,

$$\left(\begin{array}{l} P(0), \\ \forall \beta,\ P(\beta) \Rightarrow P(\beta+1), \\ \forall \beta<\lambda,\ P(\beta) \Rightarrow P(\lambda),\ \lambda \text{ limit} \end{array}\right)$$

$$\Rightarrow \forall \alpha < \gamma,\ P(\alpha).$$

this follows easily from our official principle of $<$-induction, $\because$ the official induction condition follows easily from the modified condition.

<u>2.3 Uses of ZL</u>

we usually only use a simpler form.

definition:

Suppose X is a poset, $Y \subseteq X$. A supremum for Y is an element y_0 in X s.t. $y_0 > y\ \forall y \in Y$ and if $z \geq y\ \forall y \in Y$ then $z \geq y_0$.

$(X, \leq)$ is complete just when all subsets have suprema.

$(X, \leq)$ is chain-complete if all chains have suprema $\square$.

if $(X, \leq)$ is chain-complete then $(X, \leq)$ has a maximal element.

application, any vector space has a basis.

let L be the partially ordered set of linearly independent subsets of V ordered by inclusion.

claim L is chain-complete.

suppose $\{L_i : i \in I\}$ is a chain in $\mathcal{L}$.

then $\bigcup_{i \in I} L_i$ is linearly independent.

take $\underline{e}_1, \ldots, \underline{e}_n \in \bigcup_i L_i$ with $\sum \lambda_i \underline{e}_i = 0$.

each $\underline{e}_k$ is in some L_{i_k} say and

$L_{i_1}, \ldots, L_{i_n}$ is a finite # of elements of

a chain and so ~~there~~ is a maximal

element $L = L_{i_k}$ for some k.

then $\underline{e}_1, \ldots, \underline{e}_n \in L$ linearly independent

so $\lambda_i = 0$ as required.

thus by ZL $\mathcal{L}$ has a maximal element L_0.

if L_0 not a then we take $\underline{v} \in V \setminus \langle L_0 \rangle$

and then $L_0 \cup \{\underline{v}\}$ is linearly independent $\times$

by maximality of L_0

application 2, any ring R with $0 \neq 1$

has a maximal element.

consider the collection of proper ideals

$I \triangleleft R$.

it is chain complete.

$\emptyset$-chain has $\{0\} \triangleleft R$ as supremum.

$(I_k : k \in K)$ non-empty chain has $\bigcup_{k \in K} I_k$

as supremum.

thus by ZL we have a maximal element

of the poset, so a maximal ideal.

application 3, suppose R ring, $I \triangleleft R$ an

ideal and $a \in R$ s.t. $a^n \notin I$ for any n.

then there is a prime ideal P of R with $a^n \notin P$

for any n.

take the poset of ideals J with $I \leq J$ and

$a^n \notin J$ $\forall n$.

this poset is chain complete as before, so by

ZL $\exists$ a maximal element.

$a^0 = 1 \notin P$.

suppose $b, c \notin P$, then

$$\langle P, b \rangle \ni a^r$$

$$\langle P, c \rangle \ni a^s$$

so $a^r = p_0 + \lambda b$, $a^s = p_1 + \mu c$,

$$a^{r+s} = [p_0 p_1 + \dots + \dots] + \lambda\mu bc.$$

so $\langle P, bc \rangle > P$, so $bc \notin P$.

Lecture 7

31 January 2008
09:06

2.4 Well-ordering principle

Theorem:

Any set can be well-ordered.

proof:

take a set X and consider the set W of well-orderings of subsets of X ordered by initial segments.

consider a chain $\{A_i : i \in I\}$ in W.

this is a set of well orderings s.t. for any two, one is an initial segment of the other.

so the union $\bigcup_{i \in I} A_i$ is a well ordering.

hence W is chain-complete and so by ZL,

W has a maximal element $(X', <')$ say.

if $X' \neq X$ take $x_0 \in X \setminus X'$, and order

$X' \cup \{x_0\}$ by $x' < x_0$ $\forall x' \in X'$, this is a well-ordering with $(X', <')$ as an initial segment, ※ $\square$.

the well-ordering principle is just this statement.

<u>proposition:</u>

Well-ordering principle implies AC.

<u>proof:</u>

suppose $(X_i : i \in I)$ is a family of non-$\emptyset$ sets.

take $\bigcup_{i \in I} X_i$ and a well-ordering of it.

define $c: I \to \bigcup_{i \in I} X_i$ by

$c(i) = <$-least element in $X_i \subseteq \bigcup_j X_j$ $\square$.

remark

$$\begin{tikzcd} & AC \arrow[dr, Rightarrow] & \\ WO \arrow[ur, Rightarrow] & & ZL \arrow[ll, Rightarrow] \end{tikzcd}$$

what does a well-ordering of $\mathbb{R}$ look like?

<u>2.5 ZL via the Bourbaki-Witt theorem</u>

Theorem:

Let $(X, \leq)$ be a chain complete poset.

Let $h: X \mapsto X$ be an increasing function.

Then h has a fixed point.

proof:

consider $C = \bigcap \{A \subseteq X : A$ is closed under

$\cup$s of chains in X and

closed under h, i.e. $h(A) \subseteq A\}$.

this has an induction principle.

it suffices to prove it is a chain as then

take $c = \sup C$, then $c \in C$ so $c \leq h(c) \in C$,

$h(c) \leq \sup C$, so $h(c) = c$.

inspiration 1, prove

$\forall x, \forall y, \quad x \leq y$ or $h(y) \leq x$ $\quad (\dagger)$.

by induction on x.

easy to see that x s.t. $(\dagger)$ closed under $\cup$s is it closed under h?

inspiration 2, for each such x, prove

$y \leq x$ or $h(x) \leq y$ by induction on y.

take these y, closed under $\bigcup$s of chains

as before.

is it closed under h?

$$\begin{array}{ccc} y \leq x & \text{or} & h(x) \leq y \\ \Downarrow & & \Downarrow \\ x \leq y \text{ or } f(y) \leq x & & f(x) \leq f(y) \\ \Downarrow & & \\ x = y \Rightarrow f(x) \leq f(y). & & \end{array}$$

$\therefore C$ is a chain $\square$.

Lecture 8

7

02 February 2008
09:05

Chapter 3. Cardinals and their arithmetic

3.1 Cardinals via equinumerosity

informal account, we want to consider the size of a set, independently of its elements, i.e. up to bijective equivalence.

given sets X and Y, we say X and Y are equinumerous, written $X \approx Y$, if $\exists$ a bijection $X \to Y$.

then a cardinal is just an equivalence class of sets.

operation on, properties of, propositions about cardinals are those about representative sets invariant under $\approx$.

big difference between this and the ordinal case, order-isomorphisms between ordinals are unique, bijections are seldom so.

if $\exists$ an injection $X \rightarrowtail Y$, we write $X \lesssim Y$.

evidently invariant under $\approx$, so $|X| \leq |Y|$.

$\because$ a composite $X \rightarrowtail Y \rightarrowtail Z$ of injections is injective, we have $|X| \leq |Y|$, $|Y| \leq |Z|$,

$\Rightarrow |X| \leq |Z|$.

is $\leq$ a partial ordering?

Schröder - Bernstein theorem:

Suppose $f: A \rightarrowtail B$ and $g: B \rightarrowtail A$ are injections, then $\exists$ a bijection $A \rightarrowtail B$.

proof:

write $A_{2n} = (gf)^n A \quad A_{2n+1} = (gf)^n g B$

$B_{2n} = (fg)^n B \quad B_{2n+1} = (fg)^n f A$.

$f: A_{2n} \rightarrowtail B_{2n+1}$

$A_{2n+1} \rightarrowtail B_{2n+2}$

so $f: A_{2n} - A_{2n+1} \xrightarrow{\sim} B_{2n+1} - B_{2n+2}$

similarly $B_{2n} - B_{2n+1} \xrightarrow{\sim} A_{2n+1} - A_{2n+2}$

also $f^{-1}(\bigcap_{k\geq 0} B_k) = f^{-1}(\bigcap_{k\geq 1} B_k) = \bigcap_{k\geq 1} f^{-1} B_k = \bigcap_{k\geq 0} A_k$

so $f: \bigcap_{k\geq 0} A_k \xrightarrow{\sim} \bigcap_{k\geq 0} B_k$. ?

we have

$$A = (A_0 - A_1) \cup (A_1 - A_2) \cup \cdots \cup \bigcap_k A_k$$

$$B = (B_0 - B_1) \cup (B_1 - B_2) \cup \cdots \cup \bigcap_k B_k$$

inverse of $g: (A_{2n+1} - A_{2n+2}) \xrightarrow{\sim} (B_{2n} - B_{2n+1})$

$$f: (A_{2n} - A_{2n+1}) \xrightarrow{\sim} (B_{2n+1} - B_{2n+2})$$

$$\bigcap A_k \xrightarrow{\sim} \bigcap B_k \qquad \square.$$

3.2 Tarski fixed point theorem

recall a poset is complete when all subsets

$Y \subseteq X$ have suprema.

write $\bigvee Y = \sup Y$ for the supremum.

<u>example:</u>

for any set A consider the power set $\mathcal{P}(A)$.

$\mathcal{P}(A) = \{x : x \subseteq A\}$ under $\subseteq$.

this is a complete lattice with

$$\bigvee\{x_i : i \in I\} = \bigcup\{x_i : i \in I\},$$

if $X \subseteq \mathcal{P}(A)$ closed under $\bigcup$s then

$(X, \subseteq)$ is also a complete poset.

in particular in (A, τ_A) is a topological

space, then $(\tau_A, \subseteq)$ is complete $\square$.

<u>definition:</u>

$f : (X, \leq) \mapsto (Y, \leq)$ between posets is

order-preserving if $f(x) \leq f(y)$ when $x \leq y$ $\square$.

<u>Theorem:</u>

Let $(X, \leq)$ be complete and $f : X \mapsto X$

order preserving. Then f has a fixed

point.

<u>proof:</u>

let $a = \sup\{x : x \leq f(x)\}$.

then for $x \le f(x)$ we have $x \le a$ so

$f(x) \le f(a)$ and $x \le f(x) \le f(a)$.

so $a \le f(a)$. $\Leftarrow$ A IS LEAST UPPER BOUND

so $f(a) \le f(f(a))$, so $f(a) \in \{x : x \le f(x)\}$.

$\therefore f(a) \le a$ $\square$.

application:

let $f : A \rightarrowtail B$ and $g : B \rightarrowtail A$ be injections.

define $F : \mathcal{P}(A) \to \mathcal{P}(A)$ by

$$F(x) = A - g(B - f(x))$$

if $x \le y$ then $f(x) \le f(y)$

$$B - f(x) \ge B - f(y)$$

$$g(B - f(x)) \ge g(B - f(y))$$

$$F(x) = A - g(B - f(x)) \subseteq A - g(B - f(y)) = F(y).$$

so there is a fixed point $\bar{A} \subseteq A$ with

$$\bar{A} = F(\bar{A}) = A - g(B - f(\bar{A}))$$

then $f : \bar{A} \xrightarrow{\sim} f(\bar{A}) = \bar{B} \subseteq B$.

$$g : (B - \bar{B}) \mapsto \underset{\underset{\displaystyle A - \bar{A}}{\parallel}}{g(B - \bar{B})} \subseteq A.$$

so the inverse of $g : A - \bar{A} \xrightarrow{\sim} B - \bar{B}$ $\square$.

Lecture 9

05 February 2008
09:11

3.3 Cardinal arithmetic

addition defined by disjoint union.

multiplication $\underline{m} \cdot \underline{n} = |M \times N|$.

exponentiation $\underline{n}^{\underline{m}} = |N^M| = |\{f : M \to N\}|$.

all obvious elementary rules of arithmetics apply.

examples:

① finite cardinals, cardinals of finite sets and finite ordinals.

$$0 = |\emptyset|$$

$$1 = |\{1\}|$$

$$2 = |\{0, 1\}| \quad \text{etc.}$$

② the cardinal of $\mathbb{N}$ is any of

$$\omega = \omega_0 = \aleph_0 = |\mathbb{N}|$$

this is the denumerable or countably infinite ordinal.

③ $\omega_1 = \aleph_1$ is the cardinal of the first uncountable ordinal.

④ $2^{\omega} = 2^{\aleph_0}$ defined by exponentiation is the cardinal of the continuum.

why?

$2^{\mathbb{N}} \approx \mathbb{R}$.

$\exists$ an injection $2^{\mathbb{N}} \rightarrowtail \mathbb{R}$.

either $(a_0, a_1, \ldots) \mapsto \sum_{n=0}^{\infty} a_n \left(\frac{2}{3}\right)^{n+1}$ onto the Cantor set,

or $2^{\mathbb{N}} \rightarrowtail \mathbb{N}^{\mathbb{N}} \rightarrowtail \mathbb{R}$

$$(x_0, x_1, \ldots) \mapsto x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cdots}}$$

$\exists$ an injection $\mathbb{R} \rightarrowtail 2^{\mathbb{N}}$.

take the composite of injections

$$\mathbb{R} \rightarrowtail (0, \infty) \rightarrowtail (0, 1)$$

$$x \mapsto e^x = y \mapsto \frac{y}{1+y}$$

then inject $(0,1)$ into $2^{\mathbb{N}}$ by taking each real $\in (0,1)$ to its expansion in binary choosing the non-terminating one where there is a choice $\square$.

for clarity write $\underline{n} \leq^* \underline{m}$ to mean that when $|N| = \underline{n}$, $|M| = \underline{m}$ then either $N = \emptyset$ or $\exists$ a surjection $M \twoheadrightarrow N$.

so $\underline{n} \leq \underline{m} \Rightarrow \underline{n} \leq^* \underline{m}$.

indeed, take $f : N \rightarrowtail M$ injective, either $N = \emptyset$ or take $a \in N$ and define $g : M \twoheadrightarrow N$ by

$$g(y) = \begin{cases} x & \text{if it exists s.t. } f(x) = y \\ a & \text{otherwise.} \end{cases}$$

with AC, $\underline{n} \leq^* \underline{m} \Rightarrow \underline{n} \leq \underline{m}$.

Theorem:

We never have $2^{\underline{n}} \leq^* \underline{n}$, and in particular, never $2^{\underline{n}} \leq \underline{n}$.

proof:

note $2^X \approx \mathcal{P}(X)$ by characteristic functions,

and is never $\emptyset$.

so suppose $g : X \mapsto \mathcal{P}(X)$.

consider $\{x : x \in X,\ x \notin g(x)\}$.

if this is equal to $g(a)$ say, then $a \in g(a)$

iff $a \notin g(a)$ ※ $\square$.

we now abuse notation for cardinals and

ordinals.

here and below we mean cardinals always.

▷ $\omega + \omega = \omega$.

$\exists$ a bijection $\mathbb{N} + \mathbb{N} \mapsto \mathbb{N}$.

▷ $\omega \cdot \omega = \omega$.

$\exists$ a bijection $\mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$

$$(m,n) \mapsto \tfrac{1}{2}(m+n)(m+n+1) + n.$$

▷ $2^\omega \cdot 2^\omega = 2^{\omega+\omega} = 2^\omega$.

▷ cardinality of real sequences?

$$(2^\omega)^\omega = 2^{\omega\cdot\omega} = 2^\omega.$$

cardinality of the set $\mathbb{R}^\mathbb{R}$ of all

$f: \mathbb{R} \mapsto \mathbb{R}$?

$$(2^\omega)^{2^\omega} = 2^{\omega\cdot 2^\omega}.$$

note $+, \cdot$ behave well w.r.t. $\leq$.

$$1\cdot 2^\omega \leq \omega\cdot 2^\omega \leq 2^\omega\cdot 2^\omega = 2^\omega.$$

so $\omega\cdot 2^\omega = 2^\omega$ and $|\mathbb{R}^\mathbb{R}| = 2^{2^\omega}$, bigger

than 2^ω by Cantor.

Lecture 10

05 February 2008
10:33

3.4 Hierarchy of alephs

we consider the cardinality of well-orderable sets [with AC that's all sets].

if X is well-orderable, $\exists$ minimal α s.t. X has well-ordering of type α.

ordinals κ of this kind have the property that $\forall \beta < \kappa$, $|On_{<\beta}| \neq |On_{<\kappa}|$

$$\forall \beta < \kappa, \quad |\beta| \neq |\kappa|$$

clearly if $\beta < \kappa$ then $|\beta| \leq |\kappa|$, so $|\beta| < |\kappa|$.

call ordinals of this kind initial ordinals.

if κ, μ are initial ordinals we have

$$\kappa \leq \mu \text{ as ordinals}$$

$$|\kappa| \leq |\mu| \text{ as cardinals.}$$

clearly if $\kappa \leq \mu$ as ordinals then $|\kappa| \leq |\mu|$.

conversely suppose $|\kappa| \leq |\mu|$.

if $\mu < \kappa$, then $\because \kappa$ is initial, we have

$|\mu| < |\kappa|$ ※, so $\kappa \leq \mu$

what are these initial orderings?

$0, 1, 2, 3, \ldots$

$\aleph_0 = \omega_0 = \omega$, the least infinite ordinal.

$\aleph_1 = \omega_1$, least uncountable ordinal.

$\aleph_2 = \omega_2$, etc.

for any cardinal $\underline{m} = |M|$, define $\underline{m}^+$ to be $|\gamma(M)|$.

from the definition, clear that $\gamma(M)$ is always initial.

define a function $On \to On$

$$\alpha \mapsto \omega_\alpha = \aleph_\alpha$$

by recursion as follows,

$\omega_0 = \omega$, $\omega_{\beta+1} = \omega_\beta^+$,

$\omega_\lambda = \sup_{\beta<\lambda} \omega_\beta$, λ limit.

▷ $\beta \leq \gamma \Rightarrow \omega_\beta \leq \omega_\gamma$ by induction on $\gamma \geq \beta$.

▷ $\forall \alpha$, ω_α is initial, proof by induction.

▷ $\alpha \leq \omega_\alpha$ by induction.

$\therefore$ the hierarchy ω_α of alephs enumerate

the infinite initial ordinals.

N.B. the ordering of cardinals under AC

is $\omega + On = On$.

3.5 Cardinal arithmetic with choice.

Theorem:

Suppose κ is an infinite well-ordered

cardinal. Then $\kappa \cdot \kappa = \kappa$.

proof:

induction on $\kappa \geq \omega$.

we've done $\omega \cdot \omega = \omega$.

for induction it suffices to assume that

$\mu \cdot \mu = \mu$ $\forall$ infinite $\mu \leq \kappa$ and deduce

. .

that $\kappa \cdot \kappa = \kappa$.

define an ordering $\prec$ on

$$\kappa \times \kappa = \{(\alpha, \beta) : \alpha, \beta < \kappa\}$$

by $(\alpha, \beta) \prec (\gamma, \delta)$

$\iff$ either $\max(\alpha, \beta) < \max(\gamma, \delta)$

or $\max(\alpha, \beta) = \max(\gamma, \delta)$ and $\alpha < \gamma$

or $\max(\alpha, \beta) = \max(\gamma, \delta)$ and $\alpha = \gamma$

and $\beta < \delta$.

$\prec$ is a total ordering.

it's a well-ordering $\because$ if $\emptyset \neq X \subseteq \kappa \times \kappa$

then take ρ least ordinal s.t. $\rho = \max(\alpha, \beta)$

for some $(\alpha, \beta) \in X$.

X_ρ corresponding subset of X.

take α_0 least s.t. $\exists \beta$ with $(\alpha_0, \beta) \in X_\rho$.

X_{ρ, α_0} corresponding subset of X, take β_0

least s.t. $(\alpha_0, \beta_0) \in X_{\rho, \alpha_0}$.

$(\kappa\times\kappa, \prec)$ is the union of the $(\rho\times\rho, \prec)$ as initial segments.

any initial segment of $\kappa\times\kappa$ is included in some $\rho\times\rho$.

$|\rho| = \mu$ is a cardinal $<\kappa$ and so $|\rho\times\rho| = \mu$ by induction hypothesis.

thus all proper initial segments of $(\kappa\times\kappa, \prec)$ have cardinality $<\kappa$ and so have order type $<\kappa$.

$\therefore$ order type of $(\kappa\times\kappa, \prec)$ is $\leq \kappa$.

$\therefore \kappa\cdot\kappa \leq \kappa \Rightarrow \kappa\cdot\kappa = \kappa$ $\square$.

with AC some cardinal arithmetics are ~~trivial~~.

if ρ, κ are infinite cardinals, then

$$\mu + \kappa = \mu\cdot\kappa = \max(\mu, \kappa).$$

assume $\mu \leq \kappa$.

then $\kappa \leq \mu + \kappa \leq \kappa + \kappa = 2\cdot\kappa \leq \mu\cdot\kappa \leq \kappa\cdot\kappa = \kappa$.

addition and multiplication boring.

Lecture 12

12 February 2008
09:05

propositional calculus is based on the free BA on a countable set $\{p_0, p_1, \ldots\}$, $B(\mathbb{N}) = B(\omega)$.

study it via homomorphisms

$$v : B(\omega) \to 2.$$

by freeness such v is determined by the function $v : \{p_0, p_1, \ldots\} \to 2 = \{\top, \bot\}$.

conversely, $v : \{p_0, p_1, \ldots\} \to \{\top, \bot\}$ is a valuation - it says for each p_i whether p_i is true $\top$ or false $\bot$.

a homomorphism $B \to 2$ is determined by either $v^{-1}(\top)$ which is prime filter, or $v^{-1}(\bot)$ which is prime ideal.

a filter $\Phi \subseteq B$ is s.t.

$$\top \in \Phi,$$

$$a, b \in \Phi \Rightarrow a \cap b \in \Phi$$

$$a \geq b \in \Phi \Rightarrow a \in \Phi.$$

Φ is prime if $0 \notin \Phi$ and if $a \vee b \in \Phi$ then $a \in \Phi$ or $b \in \Phi$.

the completeness theorem for propositional calculus amounts to the following.

suppose $\Gamma \subseteq B(\omega)$ and $A \in B(\omega)$.

then $A \in fil(\Gamma)$ iff whenever $v : B(\omega) \to 2$ is s.t. $v(c) = \top \ \forall c \in \Gamma$ then $v(A) = \top$

proof:

if $\Gamma \subseteq v^{-1}(\top)$, a filter, then $fil(\Gamma) \subseteq v^{-1}(\top)$.

by ZL take a maximal filter $\Phi \supseteq \Gamma$ and with $A \notin \Phi$.

this is prime & corresponds to $v : B(\omega) \to 2$ with $v(A) = \perp$ and $v(c) = \top \ \forall c \in \Gamma$ $\square$.

4.3 Propositional calculus, semantic entailment

start with a countable set $\{p_0, p_1, \ldots\}$

of atomic propositions.

form a set of all propositions by construction as follows.

- $\perp \in \text{Prop}$

- if $A, B \in \text{Prop}$ then $A \to B \in \text{Prop}$.

given a valuation $v : \{p_0, p_1, \dots\} \mapsto \{T, \perp\}$, extend it to $v : \text{Prop} \to \{T, \perp\}$ as follows.

$$v(\perp) = \perp$$

$$v(A \to B) = \begin{cases} \perp & \text{if } v(A) = T \text{ and } v(B) = \perp. \\ T & \text{otherwise.} \end{cases}$$

definition:

$\Gamma \subseteq \text{Prop}$, $A \in \text{Prop}$. Write $\Gamma \vDash A$, Γ semantically entails A, when $\forall v$, if $v(c) = T \ \forall c \in \Gamma$ then $v(A) = T$. An A s.t. $\vDash A$ is a tautology. $\square$.

traditional picture, $\to$ is determined by traditional picture, $\to$ is determined by its truth table

$A \backslash B$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\top$	$\top$

from BA primitives we could define

$a \to b = \neg a \vee b.$

conversely, given $\to$ and $\bot$, we can define

$$\neg a = a \to \bot$$

$$a \vee b = \neg a \to b$$

$$a \wedge b = \neg(\neg a \vee \neg b)$$

$$= \neg(a \to \neg b)$$

4.4 Syntactic entailment

we aim to define a relation $\Gamma \vdash A$ meaning "there is a proof of A from Γ".

secret. $\Gamma \vdash A$ will hold just when A is secret. $\Gamma \vdash A$ will hold just when A is in fil(A).

we defined this by giving

① axioms $A \to (B \to A)$.

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

$$\neg\neg A \to A$$

② natural stipulation, if $c \in \Gamma$ then $\Gamma \vdash c$.

③ rule of inference [Modus Ponens, MP].

$$\frac{A \to B \quad A}{B}$$

if $\Gamma \vdash A \to B$ and $\Gamma \vdash A$ then $\Gamma \vdash B$.

so unravelling this,

$\Gamma \vdash A$ iff there is a finite sequence $A_0, \dots, A_n = A$ with the property that $\forall\ i$, either A_i is an atom, or in Γ, or $\exists\ j, k < i$ with $A_j = A_k \to A_i$.

lemma:

$$\vdash A \to A$$

<u>proof:</u>

by axiom ②,

$$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)).$$

by axiom ①,

$$A \to ((A \to A) \to A)$$

by MP, $(A \to (A \to A)) \to (A \to A)$

by axiom ①, $A \to (A \to A)$

by MP, $A \to A$ $\square$.

observe that if $\Gamma \vdash A \to B$ then

$\Gamma, A \vdash A \to B$ and $\Gamma, A \vdash A$ so by

MP, $\Gamma, A \vdash B$.

<u>Deduction theorem:</u>

If $\Gamma, A \vdash B$ then $\Gamma \vdash A \to B$.

<u>proof:</u>

by induction on the proof of $\Gamma, A \vdash B$.

by induction on the proof of $\Gamma, A \vdash B$.

in case B is an axiom or in Γ, then we have $\Gamma \vdash B$, $\Gamma \vdash B \to (A \to B)$, so by MP $\Gamma \vdash A \to B$.

in case B is A, apply the lemma $\Gamma \vdash A \to A$.

suppose inductively we had $\Gamma, A \vdash D \to B$ and $\Gamma, A \vdash D$ and we deduce $\Gamma, A \vdash B$.

but by Ax2 $\Gamma \vdash (A \to (D \to B))$

$$\to ((A \to D) \to (A \to B))$$

and by two uses of MP we get

$$\Gamma \vdash A \to B \quad \square .$$

Lecture 13

12 February 2008
09:34

evident property, if $\Gamma, A \vdash B$ and $\Gamma \vdash A$

then $\Gamma \vdash B$.

special case, $A \vdash B$, $B \vdash C$ then $A \vdash C$.

<u>lemma:</u>

$\bot \vdash A$ for any A.

<u>proof:</u>

$\vdash \bot \to (A \to \bot)$ i.e. $\vdash \bot \to \neg A$ is an

instance of axiom 1.

putting $\neg A$ for A we have $\vdash \bot \to \neg\neg A$

$\forall A$, so $\bot \vdash \neg\neg A$ $\forall A$.

but axiom 3 is $\neg\neg A \to A$.

so $\neg\neg A \vdash A$ $\forall A$.

thus $\bot \vdash A$ $\forall A$ $\square$.

<u>4.5 Soundness</u>

the rule MP is sound in the sense that

if $v(A \to B) = T$ and $v(A) = T$ then

$v(B) = T$.

the axioms are sound in that $v(\text{axiom}) = T$

$\forall v$.

▷ $v(\neg\neg A \to A) = T$ $\because$ $v(\neg\neg A) = v(A)$ and

look at diagonal of truth table.

▷ for $v(A \to (B \to A)) = \perp$ we need $v(A) = T$

and $v(B \to A) = \perp$ and so we need

further $v(B) = T$, $v(A) = \perp$ ※.

▷ $v((A \to (B \to C)) \to ((A \to B) \to (A \to C))) = \perp$

we need $v(A \to (B \to C)) = T$ and

$$v((A \to B) \to (A \to C)) = \perp$$

so also $v(A \to B) = T$ but $v(A \to C) = \perp$

so also $\underbrace{v(A) = T}$ and $v(C) = \perp$.

gives $v(B \to C) = T$ and $v(B) = T$, so

$v(C) = T$ ※.

Soundness theorem:

If $\Gamma \vdash A$ then $\Gamma \vDash A$.

proof:

take a valuation v s.t. $v(C) = T$ $\forall C \in \Gamma$.

show by induction on length of proofs

that if $\Gamma \vdash A$ then $v(A) = T$.

case A axiom is above observation.

case $A \in \Gamma$ is OK by hypothesis.

case A has followed from early B and

$B \to A$, by hypothesis $v(B) = T$ and

$v(B \to A) = T$ and so by observation

$v(A) = T$ $\square$.

4.6 Completeness

Completeness theorem:

If $\Gamma \vDash A$ then $\Gamma \vdash A$.

definition:

Γ is consistent if $\Gamma \nvdash \bot$. $\square$

clear that if Γ is consistent and $\Gamma \vdash A$

then $\Gamma, A = \Gamma \cup \{A\}$ is also consistent.

for if $\Gamma, A \to \bot$ then $\Gamma \vdash A \to \bot$.

but then $\because \Gamma \vdash A$ we must have $\Gamma \vdash \bot$

by MP.

Model existence theorem:

If Γ is consistent then $\exists$ a

valuation v with $v(C) = T$ $\forall C \in \Gamma$

proof:

by ZL take Φ a maximal consistent

set containing Γ. how does ZL apply here???

note that by maximality, Φ is

deductively closed, $\Phi \vdash A$ then $A \in \Phi$.

define a valuation v by

$$v(p) \begin{cases} T & \text{if } p \in \Phi \\ \ldots \end{cases}$$

$\bot$ if $p \notin \Phi$.

claim $\forall A$, $v(A) = T$ iff $A \in \Phi$.

true for atomic propositions p by definition of v

it is true for $\bot$ $\because$ $v(\bot) = \bot$ and $\bot \notin \Phi$.

so using induction on the structure of formulae, it suffices to show $A \to B \in \Phi$ iff $(A \in \Phi \Rightarrow B \in \Phi)$

$(\Rightarrow)$, suppose $A \to B \in \Phi$ then if $A \in \Phi$, $\Phi \vdash B$ by MP so $B \in \Phi$.

$(\Leftarrow)$, in case $B \in \Phi$, then we have $\vdash B \to (A \to B)$ and so by MP $\Phi \vdash A \to B$ so $A \to B \in \Phi$.

in case $A \notin \Phi$, then $\Phi, A \vdash \bot$.

recall $\bot \vdash B$ $\forall B$.

so $\Phi, A \vdash B$ and so $\Phi \vdash A \to B$.

now $\because \Gamma \subseteq \Phi$ we see that $v(C) = T \ \forall C$ $\square$.

<u>proof of completeness theorem:</u>

suppose $\Gamma \nvdash A$.

then $\Gamma, \neg A$ is consistent, for if $\Gamma, \neg A \vdash \perp$

by deduction theorem

then $\Gamma \vdash \neg A \to \perp$ i.e. $\Gamma \vdash \neg\neg A$ but

$\neg\neg A \to A$ so $\Gamma \vdash A$. by MP.

now by model existence $\Gamma, \neg A$ has

a model.

but $v(A) = \perp$, so $\Gamma \nvDash A$ $\square$.

consequence, the question "is A provable"

is decidable, $\because \vdash A \Leftrightarrow \vDash A$, check by

checking all valuations on the finite

# of letters in A.

<u>Compactness theorem:</u>

If Γ is a set of propositions s.t.

any finite $\Delta \subseteq \Gamma$ has a model then Γ

has a model.

~~proof~~:

if Γ is inconsistent, then for some finite $\Delta \subseteq \Gamma$, $\Delta \vdash \perp$ $\because$ proofs are of finite length and so can only use finitely many elements of Γ as hypothesis.

so if all $\Delta \subseteq \Gamma$ are consistent then Γ is consistent.

if all $\Delta \subseteq \Gamma$ have models they are certainly consistent so Γ is consistent so Γ has a model by model existence $\square$.

application, let $(A, \leq)$ be a poset and take atomic propositions P_{xy}, $x, y \in X$.

consider Γ to be

$$\{P_{xy} : x \leq y \in X\} \cup \{\neg(P_{xy} \wedge P_{yx}) : x \neq y\}$$

$$\cup \{P_{xy} \wedge P_{yz} \to P_{xz}\}$$

$\cup \{P_{xy} \vee P_{yx}\}$

consider $\Delta \subseteq \Gamma$ finite, then $\exists\, Y \subseteq X$ finite s.t. propositions Δ mention only elements Y.

any finite partial order extends to a total order.

doing this for $(Y, \leq)$ gives a model for Δ.

so all finite subsets of Γ have a model.

hence Γ has a model which provides a total order on X extending $\leq$ $\square$

Lecture 14 ?

16 February 2008
09:03

write $\Gamma \vDash \Delta$ for whenever v is a valuation making all of Γ true then it makes one of Δ true.

note then that $\Gamma \vDash \Delta$ iff $\Gamma, \neg\Delta \vDash \bot$

iff $\vDash \neg\Gamma, \Delta$

now think of the valuations $v : \{p_0, \ldots\} \to 2$ as the points of a space $2^{\mathbb{N}}$.

think of the propositions A as basic open sets in a topology where $v \in A$ iff $v(A) = \top$.

$\vDash \Gamma$ says that Γ covers the space.

completeness theorem says if $\vdash \Gamma$ then $\vdash \Delta$ for some finite $\Delta \subseteq \Gamma$, i.e. it is the statement that $2^{\mathbb{N}}$ is compact.

aside, we can perfectly well know

model existence by enumerating $p_0, p_1, \ldots$ and adding them to Γ just when they are consistent with what we already have.

Chapter 5, predicate calculus

5.1 Terms and equational logic

a signature Σ consists of function symbols f to each of which is associated its arity $\# f \in \mathbb{N}$.

constants are of arity 0.

take a countable set V of variables, then we define the set $\text{Terms}(V)$ from Σ by recursion

- each $x \in V$ is a term.
- $f \in \Sigma$, $\# f = n$, $t_1, \ldots, t_n$ terms, then $f t_1 \ldots t_n$ is a term.

$\mathrm{Terms}(\emptyset)$ are the closed terms.

if there are no constants there are no closed terms.

a structure for a signature Σ consists of a set A and for each $f \in \Sigma$ with $\# f = n$, an n-ary function

$$[\![f(\underline{x})]\!] : A^n \mapsto A.$$

we can evidently extend to an interpretation of terms $t \in \mathrm{Terms}(\underline{x})$, then

$$[\![t(\underline{x})]\!] : A^n \mapsto A$$

we could write $\underline{a} \in A^n \mapsto [\![t(\underline{a})]\!]$

allow for t to contain fewer variables than $x_1, \dots, x_n$. ???

equational logic is concerned with deductions between equations.

take a relation symbol $=$, and equations are $t = s$ where t, s are terms.

given a structure A, we say $A \models t = s$,

i.e. $t = s$ is true in A, just when

$$[\![t(\underline{x})]\!] = [\![s(\underline{x})]\!] : A^n \mapsto A$$

$\underline{x}$ includes all the variables in s, t, and

maybe more.

note, if there are no constants in Σ,

then $A = \emptyset$ inevitable choice of interpretation

is a structure

then $A \models t = s \quad \forall t, s$.

let Γ be a set of equations and $t = s$

an equation, say $\Gamma \models t = s$ just when

$\forall$ structures A for Σ, if $A \models u = v$

$\forall u = v \in \Gamma$, then $A \models t = s$.

aside, logic of equations $t = s$ thought

of as universaly quantified.

$\forall x_1, \dots, x_n, \quad t = s.$

equational logic is given by

axiom $\quad t = t$

rule $\quad \dfrac{t = s \qquad u(s) = v(s)}{u(t) = v(t)}$

special cases,

$$\frac{t = s \qquad s = s}{s = t} \qquad\qquad \frac{t = s \qquad s = r}{t = r}$$

inductively form the easy consequence

$$\frac{t_1 = s_1, \dots, t_n = s_n}{f(t_1, \dots, t_n) = f(s_1, \dots, s_n)} \qquad (t)$$

we could restrict axiom to the case where t is a variable.

if Γ a set of equations, $t = s$ an equation in Σ, we say $\Gamma \vdash t = s$ just when $t = s$ follows from Γ using axiom and rule.

soundness, if $\Gamma \vdash t = s$ then $\Gamma \vDash t = s$.

soundness, if $\Gamma \vdash t = s$ then $\Gamma \vDash t = s$.

completeness, if $\Gamma \vDash t = s$ then $\Gamma \vdash t = s$.

proof:

let $\underline{x}$ be the variables in $t = s$.

consider $Terms(\underline{x})$ factored out by

the equivalence relation $u \sim v$ iff

$\Gamma \vdash u(\underline{x}) = v(\underline{x})$.

define for each $f \in \Sigma$,

$$[\![f]\!]([\![t_1]\!], \ldots, [\![t_n]\!]) = [\![f(t_1, \ldots, t_n)]\!]$$

well defined by $\oplus$.

now in this structure all equations of

Γ hold. WHY?

so if $\Gamma \vDash t = s$ then $t = s$ holds and

so $\Gamma \vdash t = s$ WHY?

$\Gamma \vdash t = s$, $\Gamma \vDash t = s$ hold just if $t = s$

is true when evaluated at elements

$[\![x_1]\!], \ldots, [\![x_n]\!]$ in the free model for Γ ?

generated by $\{x_1, \ldots, x_n\}$.

Lecture 15

19 February 2008
09:06

<u>5.2 The language of predicate calculus</u>

a signature for a first order language consists of

i.) a functional signature, i.e. a set of function symbols f with arities $\#f \in \{0, 1, 2, \ldots\}$;

ii.) a relational signature, i.e. a set of relation symbols R with arities $\#R \in \{0, 1, 2, \ldots\}$;

iii.) a special relation symbol $=$ of equality of arity 2.

atomic formulae, if R is a relation symbol of arity n, $t_1, \ldots, t_n$ are terms, then $R(t_1, \ldots, t_n)$ is an atomic formula.

N.B. this depends very much on what the terms are

▷ the atomic formulae are all formulae.

▷ $\perp$ is a formula, if ϕ, ψ are formulae then so is $(\phi \to \psi)$.

▷ if x is a variable and ϕ is a formula then $\forall x\, \phi$ is a formula.

the new feature is $\forall x$.

in $\forall x\, \phi$ we say x is bound.

we define the free variables $FV(\phi)$, $FV(t)$ of formulae and of terms.

terms, $FV(x) = \{x\}$

$$FV(f(t_1, \dots, t_n)) = FV(t_1) \cup \dots \cup FV(t_n)$$

atomic formulae,

$$FV(R(t_1, \dots, t_n)) = FV(t_1) \cup \dots \cup FV(t_n).$$

formulae, $FV(\perp) = \emptyset$

$$FV(\phi \to \psi) = FV(\phi) \cup FV(\psi).$$

$$FV(\forall x\, \phi) = FV(\phi) \setminus \{x\}.$$

recall that we get all boolean operations

$[\wedge, \vee, \neg]$ from $\to$, $\perp$, and we had normal forms which arose from the de Morgan laws and the double negation law.

in particular, $A \vee B$ equivalent to $\neg(\neg A \wedge \neg B)$.

by analogy we define $\exists x\, \phi(x)$ to be

$$\neg \forall x (\neg \phi(x))$$

5.3 Models and satisfaction.

let $\mathcal{L}$ be a first order language.

a structure $\mathcal{M}$ for $\mathcal{L}$ consists of a set M together with

i.) for each function symbol f with # n an n-ary function $[\![f]\!] : M^n \mapsto M$;

ii.) for each relation symbol with # n an n-ary relation $[\![R]\!] \subseteq M^n$ or $[\![R]\!] : M^n \mapsto \{\top, \perp\}$.

N.B. we will always use symbol $=$ as honest equality in M.

recall that we extend the interpretation of a functional signature to an interpretation of terms with possibly dummy variables.

we have $[\![t(\underline{x})]\!] : M^n \mapsto M$.

we extend this to an interpretation $[\![\phi(\underline{x})]\!]$ of a formula ϕ where variables $\underline{x} = x_1, \dots, x_n$ include $FV(\phi)$, but there may be dummy variables.

thus $\underline{a} \in [\![R(t_1, \dots, t_k)]\!]$

$$\text{iff } ([\![t_1(\underline{a})]\!], \dots, [\![t_n(\underline{a})]\!]) \in [\![R]\!] \subseteq M^k.$$

$$[\![R(t_1, \dots, t_k)]\!](\underline{a}) = [\![R]\!]([\![t_1(\underline{a})]\!], \dots, [\![t_k(\underline{a})]\!]).$$

$$[\![\bot]\!](\underline{a}) = \bot$$

$$[\![\phi \to \psi]\!](\underline{a}) = \top \text{ iff } ([\![\phi]\!](\underline{a}) \text{ implies } [\![\psi(\underline{a})]\!] = \top)$$

$$[\![\forall x\, \phi(x)]\!](\underline{a}) = \top \text{ iff } (\forall c \in M\ [\![\phi]\!](c, \underline{a}) = \top).$$

Tarski's definition of truth.

"the grass is green" is true if and only if

the grass is green.

Lecture 16

21 February 2008
09:26

[first half missed].

when we have a class of structures for $\mathcal{L}$ s.t. $\exists$ a set of sentences Γ s.t. the class is exactly the collection of all structures in which Γ is true, we say that the class is axiomatizable in first order logic.

<u>5.4 Applications of completeness and compactness</u>

there is a notion of proofs of ϕ from Γ, and we have analogous theorems.

completeness theorem, if $\Gamma \models \phi$ then $\Gamma \vdash \phi$.

model existence, if $\Gamma \nvdash \perp$ then Γ has a model.

compactness theorem, if all finite $\Delta \subseteq \Gamma$ have models then so does Γ.

model existence extends to say that if

L is countable then Γ has a countable model.

<u>application 1:</u>

completeness and decidability.

Γ is complete if and only if $\forall$ sentences ϕ, $\Gamma \vdash \phi$ or $\Gamma \vdash \neg\phi$.

if I can completely enumerate Γ, then the notion of proof gives a way to generate consequences computably.

and so I can effectively decide whether ϕ follows from Γ or not.

generate consequences until either ϕ or $\neg\phi$ turns up.

assuming Γ is consistent.

let Γ be $\{\forall x_1, \dots, x_n, \exists y\ x_1 \neq y \wedge \dots \wedge x_n \neq y\}$.

????

suppose Γ not complete.

then we have ϕ s.t. Γ, ϕ and $\Gamma, \neg\phi$

are both consistent.

each of them has a countable model.

any two such are isomorphic.

so can't have ϕ true in one and false

in the other. ← ???

N.B. for any M, $\{\phi \mid M \models \phi\}$ is a complete

theory $\square$.

<u>application 2:</u>

axiomatizability.

the class of finite groups are not

axiomatizable. $\eta_n = \{\forall x_1, \dots, x_n, \exists y \ x_1 \neq y, \dots, x_n \neq y\}$

suppose Γ such a theory.

consider $\Pi = \Gamma \cup \{\eta_n : n = 1, 2, \dots\}$

any finite subset Δ of Π contains only

finitely many η_n and if $m >$ all the n's in question then C_m is a model of Δ.

so by compactness Π has a model.

it is a finite group and it's infinite ※ $\square$.

Lecture 18

(?)

26 February 2008
09:08

background, a sub-structure $N \hookrightarrow M$ of a structure M is given by $N \subseteq M$ closed under the defined functions and with the restricted interpretation of the relation symbols

$[\![R]\!]_N = [\![R]\!]_M \cap N^n$.

???

① suppose $\phi(\underline{x})$ is a quantifier free formula. if $N \hookrightarrow M$ and $\underline{a} \in N^n$, then

$$N \models \phi(\underline{a}) \text{ iff } M \models \phi(\underline{a})$$

② suppose $\forall \underline{y}\ \phi(\underline{x}, \underline{y})$ is a formula with ϕ QF then

$$M \models \forall \underline{y}\, \phi(\underline{a}, \underline{y}) \Rightarrow N \models \forall \underline{y}\, \phi(\underline{a}, \underline{y}).$$

③ suppose M is a structure for $\mathcal{L}$, then M has a minimal structure M_0 where

$$M_0 = \{ [\![t]\!]_M \mid t \text{ closed terms of } \mathcal{L} \}$$

???

e.g. minimal substructure of $\mathbb{R}$ as an ordered field is $\mathbb{Z}$.

④ let $\mathcal{M}$ be a structure of $\mathcal{L}$.

$$Th(\mathcal{M}) = \{\phi \mid \phi \text{ is a sentence and } \mathcal{M} \models \phi\}$$

$Th(\mathcal{M})$ is consistent, deductively closed, and complete.

$\phi \to \psi \in Th(\mathcal{M})$ iff $(\phi \in Th(\mathcal{M}) \Rightarrow \psi \in Th(\mathcal{M}))$

⑤ if in addition $M = M_0$ then

(†) $\forall x\, \phi(x) \in Th(\mathcal{M})$ iff $\phi(t) \in Th(\mathcal{M})$ all closed t.

⑥ if T is a collection of sentences in $\mathcal{L}$ satisfying the above then $\exists$ a model for T, $\mathcal{M}$ with $M = M_0$.

let $M = \{t \mid t \text{ closed term}\}/\sim$

$$t \sim s \text{ iff } t = s \in T.$$

given Γ consistent in a language $\mathcal{L}$, we extend to $\bar{\Gamma}$ as in ⑥ in a language $\bar{\mathcal{L}}$ with the even stronger property that

$\forall x \phi(x) \in \bar{\Gamma}$ iff $\phi(c) \in \bar{\Gamma}$ all constants c ?

$\exists x \phi(x) \in \bar{\Gamma}$ iff $\phi(c) \in \bar{\Gamma}$ some c.

first take a maximal consistent extension

Γ_1 of Γ.

for all $(\exists x \phi(x) \in \Gamma_1)$ add a constant c_ϕ

and $\phi(c_\phi)$ giving $\bar{\Gamma}_1$ in $\mathcal{L}_1$.

$\bar{\Gamma}_1$ still consistent.

repeat.

$\bar{\Gamma} = \bigcup \bar{\Gamma}_i$ in $\bar{\mathcal{L}} = \bigcup \mathcal{L}_i$.

done.

Chapter 6. formal set theory.

6.1 Hierarchy V_α of pure sets.

define $V : On \to$ "sets" by recursion.

$V_0 = 0$ [empty set $\emptyset$].

$V_{\alpha+1} = \mathcal{P}(V_\alpha)$

$V_\lambda = \bigcup_{\beta<\lambda} V_\beta$, λ limit.

early stages, $V_0 = 0$

$V_1 = \{0\}$

$V_2 = \{0, \{0\}\}$

$V_3 = \{0, \{0\}, \{\{0\}\}, \{0, \{0\}\}\}$

$\vdots$

every set is a set of sets, i.e. pure sets.

definition:

A pure set x is transitive when

$z \in y \in x \Rightarrow z \in x$. $\square$.

two equivalent interpretations,

① $\{z \mid \exists y \in x \ \ z \in y\} = \bigcup \{y \mid y \in x\} = \bigcup x$

so x is transitive iff $\bigcup x \subseteq x$.

lemma:

Suppose $\{x_i : i \in I\}$ is an indexed family of transitive sets. Then $\bigcup_{i \in I} x_i$ is transitive.

proof:

$\bigcup \bigcup \{x_i : i \in I\} = \bigcup \{\bigcup x_i : i \in I\}$

$\subseteq \bigcup \{x_i : i \in I\}$ $\square$.

② $z \in y \in x \Rightarrow z \in x$

is $y \in x \Rightarrow y \subseteq x$.

so x is transitive iff $x \subseteq \mathcal{P}(x)$.

lemma:

If x is transitive, so is its power set.

proof:

if $x \subseteq \mathcal{P}x$ then $\mathcal{P}x \subseteq \mathcal{P}\mathcal{P}x$ $\square$.

proposition:

For all α, V_α is transitive.

proof:

by induction using the lemmas $\square$.

proposition:

For $\alpha \leq \gamma$ we have $V_\alpha \subseteq V_\gamma$.

proof:

by induction on $\gamma \geq \alpha$.

for $\gamma = \alpha$, $V_\gamma = V_\alpha$.

for $\gamma = \lambda > \alpha$, $V_\alpha \subseteq \bigcup_{\beta<\lambda} V_\beta = V_\lambda$

if $V_\alpha \subseteq V_\gamma$ then $\because V_\gamma$ is transitive,

$$V_\alpha \subseteq V_\gamma \subseteq \mathcal{P}(V_\gamma) = V_{\gamma+1} \ \square.$$

$V := \bigcup_{\alpha \in On} V_\alpha$.

just as On is not itself an ordinal, V is

not itself a pure set = elements of some V_α.

we shall axiomatize the properties of $(V, \in)$.

sets = members of V or $x \in V$ then it represents

$\{y \in V \mid V \models y \in x\}$.

we also consider classes, subcollections of V

defined,

Lecture 19

28 February 2008
09:07

recall we aim to axiomatize the structure $V = \bigcup V_\alpha$ with the relation $\in$.

the official language has, in addition to =, just one binary relation symbol $\in$.

for practical purposes we need definitional extensions.

① suppose $\mathcal{L}$ a lang and T a theory and

$\phi(\underline{x})$ a formula.

add to $\mathcal{L}$ a relation symbol R, get $\mathcal{L}'$.

add to T, $\forall \underline{x} R(\underline{x}) \leftrightarrow \phi(\underline{x})$. get T'.

then T' proves for any formula in $\mathcal{L}'$ that

it's $\equiv$ to a formula in $\mathcal{L}$, and ??? T' proves

in $\mathcal{L}$ just what T does. ⓣ

② $\mathcal{L}$, T as above and $\phi(\underline{x}, y)$ formula s.t.

$$T \vdash \forall \underline{x} \, \exists! y \, \phi(\underline{x}, y)$$

$$T \vdash \forall \underline{x} \, \exists y \, \phi(\underline{x}, y) \land \forall \underline{x}, y, y' \, (\phi(\underline{x}, y) \land \phi(\underline{x}, y') \to y = y')$$

add to $\mathcal{L}$ a function symbol $f(\underline{x})$, get $\mathcal{L}'$.

add to T $\forall \underline{x}, y \left(f(\underline{x}) = y \leftrightarrow \phi(\underline{x}, y) \right)$ then ⓣ

still holds.

"basic axiom", sets are determined by their members.

extensionality,

$$\forall x, y\, (\forall z, z \in x \leftrightarrow z \in y) \rightarrow x = y$$

set existence axioms,

empty set, $\exists z\, \forall y\; \neg y \in z$.

by extensionality such a z is unique and so we can introduce constant 0, and $\forall y\; \neg y \in 0$.

pairing, $\forall x, y\; \exists z\; \forall w\;\; w \in z \longleftrightarrow w = x \vee w = y$.

by extensionality for all x, y such a z is unique and so we can introduce a function symbol $\{\ ,\ \}$, and

$$\forall x, y\;\; \forall w\;\, w \in \{x, y\} \longleftrightarrow w = x \vee w = y$$

pairing enables us to encode the notion

of an order pair.

set $(x,y) = \{\{x\},\{x,y\}\}$, where $\{x\} = \{x,x\}$

lemma:

$$(x,y) = (u,v) \text{ iff } x = u \text{ and } y = v.$$

proof:

$(\Leftarrow)$ trivial.

we have $\{\{x\},\{x,y\}\} = \{\{u\},\{u,v\}\}$

either $\{x\} = \{u,v\}$, so $x = u = v$, so

$$\text{RHS} = \{\{u\}\}$$

so $\{x,y\} = \{u\}$

so $y = u$, so $x = u$, $y = v$.

or, $\{x,y\} = \{u\}$, argue similarly.

or, $\{x\} = \{u\}$ and $\{x,y\} = \{u,v\}$.

so $x = u$.

either $y = u$, argue as before, or $y = v$, done $\square$.

unions, $\forall x\ \exists z\ \forall w\ w \in z \longleftrightarrow (\exists y,\ w \in y \wedge y \in x)$

by extensionality we can introduce a function symbol $\bigcup$, and

$$\forall x \ \forall w \ w \in \bigcup x \longleftrightarrow \exists y, w \in y \wedge y \in x$$

put together we get $x \cup y = \bigcup\{x, y\}$.

power set,

$$\forall x \ \exists z \ \forall y \ y \in z \longleftrightarrow (\forall w \ w \in y \rightarrow w \in x)$$

introduce $y \subseteq x$ for $\forall w \ w \in y \rightarrow w \in x$

by extensionality, introduce function symbol $\mathcal{P}$, and $\forall x \ (\forall y \ y \in \mathcal{P}x \longleftrightarrow y \subseteq x)$.

separation, let $\phi(y, \underline{w})$ be a formula.

$$\forall \underline{w} \ \forall x \ \exists z \ \forall y \ y \in z \longleftrightarrow y \in x \wedge \phi(y, \underline{w}).$$

by extensionality, introduce function symbol $\{y \in x \mid \phi(y, \underline{w})\}$, and

$$\forall \underline{w}, x, \ y \in \{y \in x \mid \phi(y, \underline{w})\} \longleftrightarrow y \in x \wedge \phi(y, \underline{w}).$$

conceptual explanation,

let $\phi(y, \underline{w})$ be a formula and $\underline{a}$ are sets.

i.e. in V.

then $\{y \mid \phi(y, \underline{a})\}$ is a class.

it might be [represented by] a set, e.g.

$\{y \mid y \neq y\}$ "=" 0.

it might not, e.g. $\{y \mid y = y\} = V$.

separation says, if x is a set and A a

class, then $x \cap A$ is a set.

<u>example:</u>

x, y sets, $x \times y := \{(a, b) \mid a \in x, b \in y\}$ is

a class.

consider $x \cup y = \bigcup \{x, y\}$ $[a, b \in -]$

$\mathcal{P}(x \cup y)$ $[\{a\}, \{a, b\} \in -]$

$\mathcal{P}\mathcal{P}(x \cup y)$ $[\{\{a\}, \{a, b\}\}]$

so $x \times y = \mathcal{P}\mathcal{P}(x \cup y) \cap x \times y$, this is a set

by separation

Lecture 20

01 March 2008
09:05

axiom of infinity, set $Sx = x \cup \{x\}$,

$$\exists z \; 0 \in z \wedge \forall y \; y \in z \to Sy \in z$$

this is not unique.

however, with separation we can find a unique minimal such as follows.

say that z is a $(0, S)$-algebra iff $0 \in z$ $\wedge \forall y \in z \; Sy \in z$.

consider $A = \bigcap \{z \mid z \text{ is an } (0, S)\text{-algebra}\}$, a class.

the axiom gives us some $(0, S)$-algebra z_0.

we can consider by separation $z_0 \cap A$ a set.

this is A and A is a $(0, S)$-algebra,

so it is the minimal such.

what is it?

$$\left.\begin{aligned} &0 \in A \\ &S0 = 0 \cup \{0\} = \{0\} = 1 \in A \\ &S1 = \{0\} \cup \{1\} = \{0,1\} = 2 \in A \\ &\quad\vdots \end{aligned}\right\} \Rightarrow A = \omega$$

with separation the axiom amounts to

$$0 \in \omega \wedge \forall y \in \omega \ Sy \in \omega$$

$$\forall z \ 0 \in z \wedge \forall y \in z \ Sy \in z \to \omega \subseteq z$$

this is principle of mathematical induction. ???

axiom of replacement, intuitively the image of a set under a definable function is itself a set.

for any formula $\phi(x, y, \underline{z})$,

$$\forall \underline{z} \left(\forall x \ \exists! y \ \phi(x, y, \underline{z}) \right)$$

$$\to \left(\forall u \ \exists v \ \forall y \left(y \in v \right.\right.$$

$$\left.\left. \leftrightarrow \exists x \in u \ \phi(x, y, \underline{z}) \right)\right)$$

equivalently, for any $\phi(x, y, \underline{z})$,

$$\forall \underline{z} \ \forall u \ \forall x \in u \ \exists! y \ \phi(x, y, \underline{z})$$

$$\to \exists v \ \forall y \ y \in v \leftrightarrow \exists x \in u \ \phi(x, y, \underline{z}).$$

$\rightarrow \exists v \; \forall y \; y \in v \leftrightarrow \exists x \in u \; \phi(x, y, \underline{z})$.

alternative formulation, let F be a class.

F is a function $\forall x \exists ! y \; (x, y) \in F$.

F is a relation $\forall z \in F \; \exists x, y \; z = (x, y)$.

F is a function on u $\forall x \in u \; \exists ! y \; (x, y) \in F$.

$\forall u$ F is a function on u

$\rightarrow$ Image F is a set.

ZF [Zermelo-Fraenkel] is the full axiom system.

Zermelo set theory is without replacement.

<u>6.3 Sets and classes</u>

in ZF, the varables denote sets.

there are no variables for classes.

we talk directly only about sets, it refers to classes indirectly and class by class.

remarks,

① if x and y are sets then so is $x \times y$.

then $Rel(x,y) = \mathcal{P}(x \times y)$ is a set.

and $Func(x,y)$ and $Ptl(x,y)$ are

definable subcollections, and so sets by

separation.

the collections of partial orders or well-

orders on a set x are definable sub-

collections of $Rel(x,x)$, $PO(x)$, $WO(x)$.

a partially ordered or well-ordered set is

a pair $(x,<)$ where $< \in \begin{matrix} PO(x) \\ WO(x) \end{matrix}$.

the collection of such are class.

② if X and Y are classes then

$$X \times Y = \{(a,b) \mid a \in X \ \ b \in Y\}$$

is also a class.

but we cannot go on as in ①.

but we cannot go on as in ①.

$\{B \mid B \subseteq A\}$ makes no sense in the language,

no variable B.

we handle relations from X to Y relation

by relation.

if R is another class,

$$\forall z \in R \ \exists x \in X \ y \in Y \quad z = (x, y)$$

says that R is a relation from X to Y.

if F is a relation from X to Y then

$$\forall x \in X \ \exists! y \in Y \ (x, y) \in F$$

says F is a function.

we can also take R a relation from X

to X, and say that R well-orders X,

$$\forall x \neq \emptyset \quad x \subseteq X \ \exists a \in X \ a \text{ is } R\text{-minimal in } x.$$

this is a safe definition just when R is

local on X in the following sense

$\forall a \in X$ $\{b \in X \mid bRa\}$ is a set.

Lecture 21

04 March 2008
09:09

③ if A is a class then $\mathcal{P}_s(A) = \{x \mid x \subseteq A\}$

is a class.

in the same spirit if X, Y are classes

we have

$$\mathrm{Rels}(X, Y) = \mathcal{P}_s(X \times Y)$$

$$\mathrm{Ftls}(X, Y) = \{\phi \in \mathrm{Rels}(X, Y) \mid \forall a \in \mathrm{dom}\,\phi \ \exists!\, b \ (a, b) \in \phi\}$$

they are classes.

6.4 Recursion theorems

Theorem 1:

Let $(x, <)$ be a well-ordered set.

Let $g : x \times \mathrm{Ftl}(x, y) \mapsto y$. Then there is

a unique $f : x \mapsto y$ s.t. $\forall a \in x$,

$$f(a) = g(a, f|_{x_{<a}})$$

Theorem 2:

Let $(x,<)$ be a well-ordered set.

Let $G: x \times \mathrm{Ptl}(x,V) \mapsto V$ be a function.

Then there is a unique $f: x \mapsto V$ s.t.

$\forall a \in x,\ f(a) = G(a, f|_{x_{<a}})$

Theorem 3:

Let $(A,<)$ be a local well-ordered class. Let $G: A \times \mathrm{Ptl}(A,V) \mapsto V$ be a function. Then $\exists$ a unique function F s.t.

$$\forall a \in A \quad F(a) = G(a, F|_{A_{<a}}).$$

proof of 3:

let $\phi \in \mathrm{Ptl}(A,V)$ be an attempt iff $\mathrm{dom}\,\phi \in A$ is a $<$ initial segment and

$$\forall a \in \mathrm{dom}\,\phi \quad \phi(a) = G(a, \phi|_{A_{<a}})$$

show by induction.

if ϕ, ψ are attempts then $\forall a \in \mathrm{dom}\,\phi \cap \mathrm{dom}\,\psi$, $\phi(a) = \psi(a)$.

so define F by $F(a) = b$ iff $\exists\ \phi$ attempt and $\phi(a) = b$.

r.t.p. F is defined on all of A.

if not take a least where $F(a)$ is not defined.

$F|_{A_{<a}}$ is an attempt and we extend to an attempt with domain $A_{\leq a}$: $a \mapsto G(a, F|_{A_{<a}})$ ~~※~~ $\square$.

<u>6.5 van Neumann ordinals</u>

recall that an ordinal α is canonically represented by $On_{<\alpha}$.

make this happen.

take $(x, <)$ a well-ordered set and define by recursion

$$f : x \mapsto V, \quad f(a) = \{ f(b) \mid b < a \text{ in } x \}$$

consider $\operatorname{im} f$.

① if $y \in f(a) \in \operatorname{im} f$ then $y = f(b)$ for some

$b<a$ in x and so $y \in \operatorname{im} f$, thus $\operatorname{im} f$ is transitive.

② $b<a$ in x iff $f(b) \in f(a)$ in $\operatorname{im} f$.

so $f:(x,<) \mapsto (\operatorname{im} f, \in)$ is an order isomorphism, and $\operatorname{im} f$ is well-ordered by $\in$.

<u>definition</u>

$On = \{\alpha \mid \alpha$ is transitive and well-ordered by $\in\}$. □

observations,

1.) if $\gamma \subseteq \alpha$ is an initial segment of $\alpha \in On$, then $\gamma \in On$.

if $b \in \alpha$ then $\alpha_{<b} = \{c \in \alpha \mid c \in b\} = \{c \mid c \in b\} = b$.

thus every member of α is an ordinal.

2.) put $(\alpha, \in)$, $\alpha \in On$ in the above recursion.

$$f(a) = \{f(b) \mid b \in a \text{ in } \alpha\}$$
$$= \{f(b) \mid b \in a\}$$

and inductively $f(a) = \{b \mid b \in a\} = a$.

same thing happens if we consider $f : \alpha \mapsto \beta$

which is an order isomorphism to an initial

segment, $a \in b \in \alpha$ iff $f(a) \in f(b) \in \operatorname{im} f$.

then we deduce inductively

$$f(a) = \{f(b) \mid b \in a\} = \{b \mid b \in a\} = a.$$

recall that for any two well-ordered sets,

one is order-isomorphic uniquely to an initial

segment of the other.

so if $\alpha, \beta \in On$ then $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.

note that if $\alpha \subseteq \beta$ it is either a proper

initial segment, and then $\beta_{<\alpha} = \alpha$ and

$\alpha \in \beta$, or $\alpha = \beta$.

so for $\alpha, \beta \in On$, $\alpha \in \beta$ or $\alpha = \beta$ or $\beta \in \alpha$.

thus On is totally ordered by $\in$.

claim On is a local well-ordered class by $\in$.

local $\because On_{<\alpha} = \alpha$.

let $X \subseteq On$ be a non-empty class.

pick $\alpha \in X$, either α is $\in$-minimal, or

$\alpha \cap X \neq \emptyset$ and by the well-orderedness of

α we can take β $\in$-minimal in it, then

β is $\in$-minimal in X $\square$.

Lecture 22

06 March 2008
09:04

6.6 Axiom of foundation

$On = \{\alpha \mid \alpha$ transitive well-ordered by $\in\}$

by theorem 3 we have justification for the definitions of $\alpha+\beta$, $\alpha\cdot\beta$, α^β by recursion on $\beta \in On$.

equally we have justified the recursion

$$V_0 = 0$$

$$V_{\alpha+1} = \mathcal{P}(V_\alpha)$$

$$V_\lambda = \bigcup_{\beta<\lambda} V_\beta.$$

$V : On \rightsquigarrow (V)$ is a function.

propositions such as $\forall\alpha\ V_\alpha$ is transitive, $\forall\beta\leq\alpha\ V_\beta \subseteq V_\alpha$, are all theorems of ZF.

our idea was that every set should be in $V = \bigcup_\alpha V_\alpha$.

we need an axiom to make this happen.

axiom of foundation, suppose $A \neq 0$ is a non-empty class, then A contains a $\in$-minimal element.

$\forall z \; \exists a \; a \in A \to \exists a \; a \in A \wedge \forall x \in a \; x \notin A$. ???

equivalent formulation, axiom of $\in$-induction.

$$\forall x \left(\forall y \in x \; \phi(y) \to \phi(x) \right) \to \forall x \; \phi(x).$$

full ZF is usually the system with foundation.

Theorem:

It follows from the axioms that

$$\forall x \; \exists \alpha \; x \in V_\alpha.$$

proof:

suppose not, i.e. $A = \{ x \mid \neg \exists \alpha \; x \in V_\alpha \} \neq 0$.

by foundation take $a \in A$ $\in$-minimal.

then $\forall x \in a$, $x \in V_\alpha$ for some α.

so there is a function

$x \mapsto$ least α, $x \in V_\alpha$

which is functional on a.

by replacement it follows that there is

a $z \subseteq On$ and

$\forall x \in a\ \exists \alpha \in z\ x \in V_\alpha$

let $\gamma = \sup z$. ← EXISTENCE??

then $\forall x \in a\ x \in V_\gamma$ i.e. $a \subseteq V_\gamma$ so $a \in V_{\gamma+1}$ ~~$\not\ni$~~ $\square$.

aside, the least α s.t. $x \in V_\alpha$ is always

a successor ordinal.

<u>definition:</u>

The rank $rk(x)$ of a pure set x

is the least α s.t. $x \subseteq V_\alpha$. $\square$.

<u>lemma:</u>

$rk(0) = 0$

Suppose $(x_i \mid i \in I)$ is a family of pure

sets. Then $rk(\bigcup_i x_i) = \sup_i rk(x_i)$

$$= \bigcup_i rk(x_i).$$

<u>proof:</u>

$x_i \subseteq \bigcup_i x_i \subseteq V_{rk \bigcup x_i}$.

so $rk(x_i) \leq rk(\bigcup_i x_i)$ $\forall i$ and so

$$\sup_i rk(x_i) \leq rk(\bigcup_i x_i).$$

also $x_i \subseteq V_{rk(x_i)} \subseteq V_{\sup rk(x_i)}$.

so $\bigcup_i x_i \subseteq V_{\sup rk(x_i)}$.

so $rk(\bigcup_i x_i) \leq \sup rk(x_i)$ $\square$.

recall $S(x) = x \cup \{x\}$ and note that if

$\alpha \in On$ then $S(\alpha) = \alpha \cup \{\alpha\} = \alpha + 1$

<u>lemma:</u>

$$rk(S(x)) = rk(x) + 1.$$

<u>proof:</u>

$x \subseteq V_{rk(x)}$ so $x \in V_{rk(x)+1}$ and both $x, \{x\}$

are $\subseteq V_{rk(x)+1}$ so $S(x) \subseteq V_{rk(x)+1}$.

thus $rk(S(x)) \leq rk(x) + 1$

also $x \cup \{x\} = Sx \subseteq V_{rk(S(x))}$ so $x \in V_{rk(S(x))}$.

it follows that $x \subseteq V_\beta$ for some $\beta < rk(S(x))$.

so $rk(x) < rk(S(x))$, so $rk(x)+1 \leq rk(S(x))$ □.

<u>proposition:</u>

$$rk(\alpha) = \alpha.$$

<u>proof:</u>

by induction □.

<u>6.7 Recursion theorem for V</u>

we have principle of $\in$-induction for V

and so expect to have a corresponding

recursion theorem.

aside, for pure sets $x \subseteq V_\alpha$ for some α

and V_α is transitive and so

$$x \subseteq V_\alpha \cap (\bigcap \{y \mid y \text{ transitive } \supseteq x\})$$

more instructive is the following.

for a set x, define by recursion on ω

$$T_x : \omega \mapsto V$$

$$T_x(0) = x$$

$$T_x(n+1) = T_x(n) \cup (\bigcup T_x(n))$$

by replacement $\{T_x(n) \mid n \in \omega\}$ is a set,

and taking unions,

$$TC(x) = \bigcup_{n \in \omega} T_x(n)$$

is a set.

claim $TC(x)$ is the least transitive set

$\supseteq x$.

take $z \in y \in TC(x)$.

then $y \in T_x(n)$ for some n and so $z \in T_x(n+1)$.

so $z \in TC(x) \Rightarrow TC(x)$ is transitive.

let t be transitive and $t \supseteq z$.

Then $\bigcup z \subseteq \bigcup t \subseteq t$, so $z \cup (\bigcup z) \subseteq t$.

Lecture 24

11 March 2008
09:04

Theorem:

For any $\phi(x)$, there is a sentence ψ s.t. $ZF \vdash \psi \leftrightarrow \phi(\#\psi)$.

proof:

guess ψ is $\chi(\#\chi)$, and take $\chi(x)$ to be $\phi(\sigma(x,x))$.

then ψ is $\phi(\sigma(\#\chi, \#\chi))$.

but $ZF \vdash \sigma(\#\chi, \#\chi) = \#(\chi(\#\chi))$.

so $ZF \vdash \psi \longleftrightarrow \phi(\#\chi(\#\chi))$

$\vdash \psi \longleftrightarrow \phi(\#\psi)$ $\square$.

7.5 Incompleteness theorem

take ψ s.t. $ZF \vdash \psi \leftrightarrow \neg \mathrm{Pble}(\#\psi)$.

suppose $ZF \vdash \psi$, then there is a derivation D for ψ and so $ZF \vdash \mathrm{Prf}(\#D, \#\psi)$, so $ZF \vdash \exists x\, \mathrm{Prf}(x, \#\psi)$, so $ZF \vdash \mathrm{Pble}(\#\psi)$.

but also $ZF \vdash \neg \mathrm{Pble}(\# \psi)$, so $ZF \vdash \perp$.

if $ZF \nvdash \perp$, then $ZF \nvdash \psi$. (*)

suppose $ZF \vdash \neg \psi$, i.e. $ZF \vdash \exists x \, \mathrm{Prf}(x, \# \psi)$.

if $ZF \nvdash$, we know $ZF \nvdash \psi$, so for

each derivation D, it is not a derivation

of ψ. and so $ZF \vdash \neg \mathrm{Prf}(\# D, \# \psi)$.

if ZF true, or better if it is ω-consistent

then $\cancel{*}$.

ω-consistent means $ZF \vdash \exists x \in \omega \; \phi(x)$ and

$ZF \vdash \neg \phi(n)$ all n is impossible. ?

Theorem, 1st incompleteness:

There is a ψ s.t. if ZF is consistent

then $ZF \nvdash \psi$ and $ZF \nvdash \neg \psi$.

we showed (*), so

$$ZF \vdash \neg \mathrm{Pble}(\# \perp) \to \neg \mathrm{Pble}(\# \psi)$$

so $ZF \vdash \psi$. ?

so if ZF is consistent then $ZF \nvdash (\text{ZF consistent})$.

this is 2nd incompleteness.

7.5 Löb's theorem

Theorem:

If $\vdash \mathrm{Pbl}(\#\phi) \rightarrow \phi$ then $\vdash \phi$.

proof:

by FPT, take ψ with

$$\vdash \psi \leftrightarrow \Box(\psi \leftrightarrow \phi)$$

claim $\vdash \Box p \to \Box\Box p$.

then $\vdash \psi \to \Box\psi$.

so by MP $\vdash \psi \to \Box\phi$.

so using assumption, $\vdash \psi \to \phi$.

so $\vdash \Box(\psi \to \phi)$.

so $\vdash \psi$, so $\vdash \phi$ $\Box$.