SET THEORY

MasterMath 2021/22

SECOND LECTURE

20 SEPTEMBER 2021

AXIOMS SO FAR

Ext	Extensionality
Emp	Empty Set
Pair	Pairing
Union	Union
Sep	Separation (Scheme)

THM If $G \models$ Ext + Emp + Pair, then G has infinitely many vertices.

The Axiom Scheme of Separation
Fix a formula φ with $n+1$ free variables

(Sepφ)

$$\forall x \forall p_1 \dots \forall p_n \exists S \; \forall z \, (z \in S \longleftrightarrow z \in x \wedge \varphi(z, p_1, \dots, p_n))$$

FROM LECTURE I

① Comment on Emp.

$\text{Sep} \models \text{Emp.}$

If x is any set, and $\psi(z) := z \neq z$.
Then separating from x by ψ gives us a set without elements.

That argument needs that structures are non-empty.
In logic, by definition, the domain / universe of a structure is non-empty.
If for some reason, you do not wish to exclude the empty structure, add

"Existence axiom" $\exists x\,(x = x)$

and enforce that models of set theory are non-empty.

② Comment on axiom schemes.

An axiom scheme consists of infinitely many formulas and there no implicit →

assumption that it is necessarily not expressible as a single axiom.

If S is an infinite set of sentences, we can say S is finitely expressible if there is φ s.t.

$$\varphi \models S \text{ and } S \models \varphi.$$

If I write a scheme, I do not mean to imply that it is obvious that it can't be finitely expressed.

Do we even care whether Sep is finitely expressible?

No, rather: if T is a "base theory" then S is finitely expressible modulo T if there is φ s.t.

$$T+\varphi \models S \text{ and } T+S \models \varphi.$$

These questions are interesting from the point of view of logic, not so much from the point of view of set theory.

FROM LECTURE I

Next time

Definition If $G = (V, E)$ is a graph, we call $v \in V$ a universal vertex if for all $w \in V$, $w E v$.

Theorem If G satisfies the Axiom Scheme of Separation, then G has no universal vertex.

Remark Often expressed as "there is no set of all sets".

Proof. Proof borrows from Russell's theorem. Assume, towards a contradiction, that there is a universal vertex: U.
Consider the Russell formula $\boxed{z \notin z}$ and separate from U by the Russell formula.

$$\forall x \, \exists s \, \forall z \, (z \in s \leftrightarrow z \in x \wedge z \notin z)$$

U $\qquad$ U

Set $z := s$: $\quad s \in s \leftrightarrow s \in U \wedge s \notin s$

Since U is universal: $\quad s \in s \leftrightarrow s \notin s$.

CONTRADICTION. $\qquad$ q.e.d.

Remark 1.

This proof tells us for every x that there is a concrete set which is not an element of x:

$$z \in S \longleftrightarrow z \in x \wedge z \notin z$$

So, $\{ z \in x ; z \notin z \}$ cannot be an element of x.

Remark 2. We immediately get:

if $\mathfrak{G} \models$ Sep + Pair + Union, then there is no set of all singletons:

Suppose v is the set of all singletons, i.e., $\circledast$ $x \in v \longleftrightarrow \exists w \, (x = \{w\})$.

By the union axiom, form the union of v. Claim: This is a universal vertex.

[Take any vertex z. By Pair, we get a singleton of z and thus by $\circledast$ is an element of v. So z is an elt of the union.]

POWER SET AXIOM.

What is "the power set"?
What is a subset?

$$x \subseteq y \;:\Longleftrightarrow\; \underbrace{\forall z (z \in x \longrightarrow z \in y)}_{\text{formula in LST}}$$

If G is a directed graph and v, w are vertices, then v is a G-subset of w iff

$$\forall z \in V \,(zEv \longrightarrow zEw)$$

vertices

$v, w \in V$ $\quad G \frac{v\,w}{x\,y} \models x \subseteq y$

That is equivalent to $G \models v \subseteq w$

Q: Is this notion the same as our intuitive notion of "subset"?

Properties
1. Any vertex is a G-subset of itself.
2. If w is an empty set, then w is a G-subset of every vertex

Examples:

①
$$\begin{tikzcd} \overset{a}{\bullet} \arrow[loop below] \end{tikzcd} = \mathbb{G}$$

What are the $\mathbb{G}$-subsets of a:

Clearly, a is a subset of a.

Note: This is a vertex that represents a one-element set, with precisely one subset.

[This is in contrast to a basic theorem: if x has n elements, it has 2^n subsets.]

The problem here seems to be the lack of an empty set.

②
$$\begin{tikzcd} \overset{a_0}{\bullet} \arrow[r] \arrow[rr, bend right] \arrow[rrr, bend right=50] & \overset{a_1}{\bullet} \arrow[r] \arrow[rr, bend left] & \overset{a_2}{\bullet} \arrow[r] & \overset{a_3}{\bullet} \end{tikzcd}$$

	Predecessors	Subsets	
a_0	—	a_0	
a_1	a_0	a_1, a_0	
a_2	a_0, a_1	a_2, a_1, a_0	$3 \neq 2^2$
a_3	a_0, a_1, a_2	a_3, a_2, a_1, a_0	$4 \neq 2^3$

Summary In very weak set theories, the number of subsets of an n-element set may be different from 2^n.

Remark 1. Ext will imply that it is $\leq 2^n$.

Remark 2. Pair and Union / Sep will give you $\geq 2^n$.

The power set is the set of all subsets.

(Pow) $\forall x \exists p$
$$\forall z \left(z \in p \longleftrightarrow z \subseteq x \right)$$

Powerset Axiom.

Weird example

$\mathfrak{G}$

In this model a is the only $\mathfrak{G}$-subset of a, thus a is the powerset of a in $\mathfrak{G}$.

Therefore: $\mathfrak{G} \models \text{Pow}$.

With this, we can now define our first axiom system of set theory:

FST FINITE SET THEORY

consisting of

Ext, Pair, Union, Pow, Sep.

Why FST?

It does NOT imply that everything is finite. But it cannot prove that infinite sets exist; so it is consistent with "everything is finite".

While it is weak in that respect, it is surprisingly strong in terms of "abstract mathematics", allowing us to prove essentially everything we want, except for existence of concrete infinite objects such as $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Goal for part 2 of today's lecture: DO THIS RECONSTRUCTION OF ABSTRACT MATHS

Which formulas are allowed in Sep?

Precisely the LST-formulas, so just logical symbols, $\in$, and $=$.

E.g., not an LST-formula is

$\boxed{\{}x\boxed{\}} \in z \qquad \boxed{\emptyset} \in z \qquad \cup, \subseteq, \ldots$

technically not allowed

Once you have Ext + Pair, we know that there is a unique object with x as predecessor, so we can take

$\boxed{\{x\} \in z}$

as abbreviation for

$$\forall w\,(\forall v\,(v \in w \leftrightarrow v = x) \longrightarrow w \in z)$$

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

[An aside.]

What does it mean to say

FST cannot prove that infinite sets exist?

There is no obvious candidate for an LST-formula φ s.t. φ expresses "there is an infinite set".

[Later in more detail.]

We interpret this informally:

If G is a graph, we call it locally-finite if every vertex has finitely many predecessors.

So, intuitively G has no vertices representing infinite sets.

Theorem (HW #2 (6))

There is a locally finite graph G s.t.

$$G \models FST.$$

Reconstruction of abstract maths in FST

First observation

If $\mathbb{G} \models FST$ and $v \in V$ with n predecessors, then the powerset of v in $\mathbb{G}$ has 2^n many predecessors.

$\mathbb{G} = (V, E)$

[By Ext, 2^n is an upper bound. Let $v_1, \dots, v_n$ be the n $\mathbb{G}$-predecessors of v and let $i_1, \dots, i_k \subseteq \{1, \dots, n\}$. Show that there is a vertex w s.t. $v_{i_1}, \dots, v_{i_k}$ are the $\mathbb{G}$-predecessors of w!

Take the formula φ with $k+1$ free variables

$$\varphi(x, x_1, \dots, x_k) :=$$

$$x = x_1 \lor x = x_2 \lor \dots \lor x = x_k$$

Now separate by Sep from v with formula φ with parameters $v_{i_1}, \dots, v_{i_k}$. $\longrightarrow w$

Then w has precisely $v_{i_1}, \dots, v_{i_k}$ as predecessors.]

If $G \models FST$, we can expand the language LST with numerous (uniquely defined) abbreviations:

$\{x\}$ "the unique w s.t. x is the only pred. of w"

$\{x,y\}$ ...

unordered pair

$x \cup y$

$\bigcup x$

$P(x)$ power set of x

$\{\underline{z \in x}; \varphi(z, \vec{p})\}$

$\in x$ important

Intersection? $x \cap y := \{z \in x; z \in y\}$

$x = \emptyset$ $\bigcap x := \{z \in y;\ \forall w (w \in x \to z \in w)\}$

Let $y \in x$

What we don't have yet:

the ordered pair (x,y) HW#2 (7)

$(x,y) = (x',y') \iff x = x' \wedge y = y'$

The traditional definition:
the KURATOWSKI PAIR

$$(x,y) := \{\underline{\{x\}, \{x,y\}}\}$$

Check that it satisfies the requirement for ordered pairs.

Just to illustrate how complex LST-formulas can look like:

$OP(p, X, Y)$

p is an ordered pair with first component in X and second component in Y.

$$\begin{aligned}
:\Longleftrightarrow\ & \exists s \exists d \exists x \exists y \\
& [\forall z (z \in s \longleftrightarrow z = x) \wedge \\
& \forall z (z \in d \longleftrightarrow z = x \vee z = y) \\
& x \in X \wedge \\
& y \in Y \wedge \\
& \forall z (z \in p \longleftrightarrow z = s \vee z = d)]
\end{aligned}$$

Note that this does not immediately give us the set of ordered pairs with first comp. from X & second comp from Y.

Because we need to find a set to use as basis to separate from by formula $OP(p, X, Y)$.

Note that if $x \in X$, then $\{x\} \subseteq X$ $\subseteq X \cup Y$.

$x \in X$, $y \in Y$, then $\{x, y\} \subseteq X \cup Y$

$$\{x\}, \{x, y\} \in \mathcal{P}(X \cup Y)$$

$$\{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(X \cup Y)$$

$$\{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(X \cup Y))$$

Thus, we define

$$X \times Y := \{ p \in \mathcal{P}(\mathcal{P}(X \cup Y)) ; OP(p, X, Y) \}$$

Thus: FST proves that for any two sets, their cartesian product exists.

Definition.

(1) If $R \subseteq X \times Y$, we write

domain

$$\mathrm{dom}(R) := \{x \in X\,;\, \exists y\,((x,y) \in R)\} \text{ and}$$
$$\mathrm{ran}(R) := \{y \in Y\,;\, \exists x\,((x,y) \in R)\}.$$

range

(2) We say that R is *functional* or *a partial function* if

$$\forall x \forall y \forall z \big((x,y) \in R \wedge (x,z) \in R) \to y = z\big).$$

(3) We say that R is *injective* if

$$\forall x \forall y \forall z \big((x,z) \in R \wedge (y,z) \in R) \to x = y\big).$$

(4) We say that R is *total* if $\mathrm{dom}(R) = X$.

(5) We say that R is *surjective* if $\mathrm{ran}(R) = Y$.

(6) If R is functional and $x \in \mathrm{dom}(R)$, we write $R(x)$ for the unique y such that $(x,y) \in R$.

(7) If $X' \subseteq X$, we write $R{\restriction}X' := \{(x,y) \in R\,;\, x \in X'\}$.

(8) If $R \subseteq X \times Y$, we say that R is a *function from X to Y* (in symbols: $R\colon X \to Y$) if R is functional and total.

If $R \subseteq X \times Y$, we say R is a relation between X and Y.

We deduce that if $G \models FST$ and $x, y \in V$,
$G = (V, \in)$
then "the set of relations between x & y" is a vertex in G;
"the set of all functions from x to y" is a vertex in G;
similarly: set of a injection/surjections/bijection etc. from x to y.

Definition. Let $R \subseteq X \times X$ be a binary relation on X.

(1) The relation R is called *reflexive* if $\underline{\forall x(x \in X \rightarrow (x,x) \in R)}$. φ

(2) The relation R is called *irreflexive* if $\forall x(x \in X \rightarrow (x,x) \notin R)$.

(3) The relation R is called *symmetric* if $\forall x \forall y\big((x,y) \in R \rightarrow (y,x) \in R\big)$. ψ

(4) The relation R is called *antisymmetric* if $\forall x \forall y\big(((x,y) \in R \wedge (y,x) \in R) \rightarrow x = y\big)$.

(5) The relation R is called *transitive* if $\underline{\forall x \forall y \forall z\big(((x,y) \in R \wedge (y,z) \in R) \rightarrow (x,z) \in R\big)}$. χ

(6) The relation R is called *total* if $\forall x \forall y\big((x,y) \in R \vee (y,x) \in R \vee x = y\big)$.

(7) The relation R is called an *equivalence relation* if it is <u>reflexive, symmetric, and transitive</u>.

(8) The relation R is called a *partial preorder* if it is reflexive and transitive.

(9) The relation R is called a *partial order* if it is reflexive, antisymmetric, and transitive.

(10) The relation R is called a *total preorder* if it is reflexive, transitive, and total.

(11) The relation R is called a *total order* if it is reflexive, antisymmetric, transitive, and total.

(12) The relation R is called a *strict total order* if it is irreflexive, transitive, and total.

We obtain:

If $\underset{(V,E)}{\underset{\shortparallel}{G}} \models \mathrm{FST}$ and $x \in V$, then there is a vertex w representing "the set of equivalence relations on x".

$$\{R \in P(x \times x) \,;\, \varphi(R) \wedge \psi(R) \wedge \chi(R)\}$$

Doing some basic algebra in FST:

What is a group?

A group is an ordered pair (G, f) where G is the universe/domain and f is a binary function

$$f : G \times G \longrightarrow G$$

satisfying the axioms: associativity, existence of neutral element, existence of inverses.

Φ

Ψ

Ξ

$$\boxed{\forall x \forall y \forall z \; f(x, f(y,z)) = f(f(x,y),z)}$$

expressible in LST [in FST-models] with parameter f

A group is an ordered pair (a, b) s.t.

$$b : a \times a \longrightarrow a$$

s.t. $\Phi(b) \wedge \Psi(b) \wedge \Xi(b)$.

Doing quotients:

If X is a set and R is an equivalence relation

C is an R-equivalence class

$$\iff \forall x \forall y \, (x \in C \rightarrow (y \in C \leftrightarrow xRy)) \wedge C \neq \emptyset.$$

Formula $EC(C,R)$.

And separate from $P(X)$ those subsets of X that are equivalence classes.

$$X/R := \{ C \in P(X) ;\ EC(C,R) \}.$$

So, we can reconstruct all abstract operations in FST. If we now add another axiom that guarantees the existence of, say, $\mathbb{N}$, then we can reconstruct all of (ordinary) mathematics.

INFINITY

We desire to have infinite sets, i.e., $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, etc in our models. How could we express a set theoretic axiom that states their existence.

Approach 1. X is infinite if there is an inj. from $\mathbb{N}$ into X.

[Doesn't help since we don't have the natural numbers yet.]

Approach 2. X is infinite if there is $Y \subsetneq X$ and a bijection $f: X \to Y$.

This by our earlier work is easily expressible in LST

So: "an axiom of infinity" could be

$$\exists x \exists y \big(y \subseteq x \wedge y \neq x \wedge \exists f \big(f: x \to y \wedge f \text{ is a bijection}\big)\big)$$

Axiom of Dedekind-Infinity.

We're not going to use it, since it is not very concrete about the infinite sets that exist and one needs AC to prove that it is equivalent to the one we are going to use.

<u>Approach 1'.</u> Define a property of sets that will make the sets "infinite" and allows us to extract $\mathbb{N}$ easily.

<u>DEFINITION</u> A set I is called <u>INDUCTIVE</u> if

$$\emptyset \in I \wedge \forall x \, (x \in I \longrightarrow \underbrace{x \cup \{x\}}_{\substack{\text{"successor of } x\text{"} \\ s(x)}} \in I)$$

[This only makes sense in FST.]

<u>Remark.</u> A slight modification of our proof that models of Emp + Pair cannot be finite shows that if $\mathfrak{B} \models$ FST and $I \in V$ s.t. $\mathfrak{B} \models I$ is inductive, then I has infinitely many predecessors.

Thus any $\mathfrak{B}$ with such an I cannot be locally finite.

(Inf) Axiom of Infinity

$$\exists I \, (I \text{ is inductive})$$

Our second axiom system is

Z Zermelo set theory

FST + Inf.

We can now see that in every model of Z there is a unique smallest inductive set, i.e., some x s.t.

x is inductive and

for all I, if I is inductive, then $x \subseteq I$.

<u>Def.</u> We call this set the natural numbers, in symbols, $\mathbb{N}$.

<u>Proof of claim</u>. Let I be any inductive set. Define

$$\hat{I} := \{ z \in I ; \forall J \, (J \text{ is inductive} \rightarrow z \in J) \}$$

Clearly, if I, I' are inductive, then $\hat{I} = \hat{I'}$.

By definition of $\hat{I}$, if J is inductive, $\hat{I} \subseteq J$.

Since $\mathbb{N}$ are the smallest inductive set, we obtain:

If I is inductive and $I \subseteq \mathbb{N}$, then $I = \mathbb{N}$.

This is

THEOREM The Principle of Induction

If $X \subseteq \mathbb{N}$ s.t.

$\emptyset \in X$ and

$\forall x \, (x \in X \longrightarrow s(x) \in X)$

Then $X = \mathbb{N}$.

This allows us to prove statements about $\mathbb{N}$ by induction.

EXAMPLES

(1) For every $x \in \mathbb{N}$ either $x = \emptyset$ or $\emptyset \in x$.

Proof:

$$Z := \{ z \in \mathbb{N} ;\ \underline{z = \emptyset} \text{ or } \emptyset \in z \}$$

Show that Z is inductive.

Then the claim follows from Theorem.

(a) $\emptyset \in Z$. ✓

(b) Suppose $x \in Z$.

<u>Case 1.</u> $x = \emptyset$. Then $s(x) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$

But then $\emptyset \in s(x)$. ✓

<u>Case 2.</u> $\emptyset \in x$. Then $s(x) = x \cup \{x\} \supseteq x$.

So $\emptyset \in s(x)$. ✓

<u>Def.</u> A set x is called <u>transitive</u> if for all y, z if $z \in y \wedge y \in x \longrightarrow z \in x$.

[Equivalently: if every element of x is a subset of x]

(2) Every $x \in \mathbb{N}$ is transitive.

Proof: $Z := \{ z \in \mathbb{N} ;\ z \text{ is transitive} \}$

Claim: Z is inductive

Two things to check:

(a) $\emptyset$ is transitive.

[Trivial.]

(b) Suppose $x \in Z$, so x is transitive.

Show that $s(x) = x \cup \{x\}$ is transitive.

$z \in y \in x \cup \{x\}$ $\boxed{\text{N.T.S. } z \in x \cup \{x\}}$

<u>Case 1.</u> $y \in x \xRightarrow[\text{of } x]{\text{Transitivity}} z \in y \in x \longrightarrow z \in x \subseteq s(x)$ ✓

Case 2. $y = x$. $z \in y = x \subseteq x \cup \{x\}$.

$\Rightarrow z \in s(x)$. ✓