Computational Logic

Interactive Theorem Proving

Week 9

Cezary Kaliszyk (VO)
Vincent van Oostrom (PS)

December 2, 2016

Summary

So far

Proof Assistants, HOL Light, $\lambda_{\rightarrow}$, λ_P, λ_2

- Paradoxes

Today

- Girard's paradox
- Foundations of set theory

What is a set?

- Sets are commonly used in mathematical texts
- There can not be a strict definition of a basic concept

Definition (Cantor)

A set, is a gathering into one complete object of clearly distinguished objects in our intuition or thought.

- Materialization of a predicate
  - Given a predicate $P(x)$, instead of talking about all the objects that satisfy it, it is easier co consider only one object

Notation

$$\{x|P(x)\}$$

Naive set theory

- Consider sets as any other objects
- Consequence: sets of sets
- For example

$$S = \{x | x \text{ is a set}\}$$

- Paradoxes for naive set theory

Russell's paradox

$$S = \{x | x \text{ is a set and } x \notin x\}$$

Class theory

Definition [class]

- collection of sets
- unambiguously defined by a property

- Frankel operator only for subsets or power-sets
- Example: Class of all groups
- The NST paradoxes are gone
- More commonly used by mathematicians

Hierarchy induced by cardinality

set, class, multitude, ...

Typed set theory

- Not every predicate is a valid one for every x
- x comes from a certain domain
  - x is of type D (for example $\mathbb{N}$, $\mathbb{B}$, $\mathbb{R}$)
  - Every domain is a set (trivially distinguished)
  - We should have a unique type for any object
- Proper Frankel operator:

$$\{x : D | P(x)\} \text{ or } \{x \in D | P(x)\}$$

Definition [membership]

$$P(y) \iff y \in \{x : D | P(x)\}$$

Notation

$$\{x : A | P(x)\} \text{ means } \{x : D | x \in A \wedge P(x)\}$$

Set inclusion, power-set, equality

- Enumeration, singleton set
- Usual set inclusion definition
- Usual power set definition
- Correspondence between the two
- $x = y$
  - Makes sense only if the two are of the same type
  - Means that the two are different names of the same object
  - Uniqueness property: For $A, B \in P(D)$,

$$A = B \iff \forall z.(z \in A \iff z \in B)$$

  - Consequence

$$\forall A, B : P(D).A = B \iff A \subseteq B \wedge B \subseteq A$$

- Every set has only one empty subset (proved)
  - Denoted $\emptyset$

Usual definitions

- Finite
  - Union
  - Intersection
  - Difference (symmetric)
  - Set complement (!)
  - Symmetric difference
- Infinite
  - Union
  - Intersection

Set theory as a formal system

Basic concepts and their axiomatizations

- ZF (Zermelo-Fraenkel)
  - Most commonly used
  - Optionally with choice (ZFC)
- Various "new foundations"
  - Hierarchies of sets roughly following ideas from type theory
  - Issues with "too big sets"
- Semisets (classes contained in a set)
- Positive set theories
  - Axiom of comprehension is allowed for positive formulas
- TG (Tarski-Grothendieck)
  - Richer thanks to unaccessible cardinals

Axioms of ZF (ZFC)

- Pairing
  - For any two sets, there exists a set that contains the two as elements
- Union
  - Infinite version of pairing
- Power set
  - For any set, there exists a set of all its subsets
- Extensionality
  - If two sets have same elements, they are equal
- Regularity (or Foundation)
  - A nonempty set has an element which is disjoint with itself
- Infinity (ω)
- Schema specification (restricted comprehension)
- Schema replacement
  - Image of a set under a mapping is also a set
  - Needed for infinite sets
- Well ordering or AC

Set theory as a proof system

Many basic properties follow from these definitions:

$$A - B = \emptyset \rightarrow A \subseteq B$$

But how do they follow? We need some meta-logic!

- Very simple logical system
  - First-order predicate logic in Mizar
- Proofs
  - Jaśkowski-style proofs in Mizar

Bootstrapping Mathematics

In HOL

- functions, bool and equality are primitive
- $\rightarrow$ other logical operators and their properties
- individuals $\rightarrow \mathbb{N}$
- quotients $(\epsilon) \rightarrow \mathbb{Z}$, $\mathbb{R}$

In Type Theory (say Coq or Agda)

- Inductive types $\rightarrow$ T, F, $\wedge$, ..., $\mathbb{N}$, $\mathbb{Z}$
- Setoids $\rightarrow \mathbb{R}$

In Set Theory

- Logic?
- Numbers?

Summary

Today

- Introduction to Set Theory

Next time

- Bootstrapping Mathematics
- Mizar