Interactive Theorem Proving

Week 8

Cezary Kaliszyk

May 5, 2015

Summary

So far

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

- Undecidability of λ_P
- Second order propositional logic
- Even more on Curry-Howard
- Order of variables

Today

- 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

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

- 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:

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

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?

Bootstrapping set theory (1/2)

- Ordered pairs, products, relations
  - Fact: $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$ iff $a = c$ and $b = d$
  - Definition of an ordered pair. Notation $< a, b >$
  - Cartesian product of sets
  - Relation: subset of $A \times B$
- Natural numbers
  - inductive definition of a family of sets:

$$\emptyset \in A \wedge (X \in A \rightarrow X \cup \{X\} \in A)$$

  - Theorem: there exists a minimal inductive set
  - Successor denoted as n'
  - Induction for $P \subseteq \mathbb{N}$

$$0 \in P \wedge \forall n. n \in P \rightarrow n' \in P \rightarrow P = \mathbb{N}$$

    follows the definition
  - Notions: $n \in m$ and $n \subseteq m$ instead of $<$

Bootstrapping set theory (2/2)

- Functions are relations which are "functional"
  - If $< a, b_1 >\in f$ and $< a, b_2 >\in f$ then $b_1 = b_2$
  - For any $a \in A$ there exists a $b \in B$ st $< a, b >\in f$
- Domain and range of a function.
- Bijection $\rightarrow$ inverse function.
- Defining functions by induction
- Equivalence relations divide a set $\rightarrow$ quotients like $\mathbb{Z}$
- Equipotence and Cardinality
  - Cardinality equal to n if there exists a bijection to n
  - Countable sets
  - Uncountable sets (diagonalization construction)

Demo

- hidden
- tarski
- xboole0
- sqrtmiz

```
:: W The Irrationality of the Square Root of 2
theorem Th1:
 for p being Element of NAT st p is prime holds
 sqrt p is irrational
proof
 let p be Element of NAT ;
 assume A1: p is prime ;
 then A2: p > 1 by INT_2:def 4;
 assume sqrt p is rational ;
 then consider i being Integer, n being Element of NAT such that
 A3: n <> 0 and
 A4: sqrt p = i / n and
 A5: for i1 being Integer
 for n1 being Element of NAT st n1 <> 0 & sqrt p = i1 / n1 holds
 n <= n1 by RAT_1:9;
 A6: i = (sqrt p) * n by A3, A4, XCMPLX_1:87;
 sqrt p >= 0 by SQUARE_1:def 2;
 then reconsider m = i as Element of NAT by A6, INT_1:3;
 A7: m ^2 = ((sqrt p) ^2) * (n ^2) by A6
 .= p * (n ^2) by SQUARE_1:def 2 ;
 then p divides m ^2 by NAT_D:def 3;
 then p divides m by A1, NEWTON:80;
 then consider m1 being Nat such that
 A8: m = p * m1 by NAT_D:def 3;
 n ^2 = (p * (p * (m1 ^2))) / p by A2, A7, A8, XCMPLX_1:89
 .= p * (m1 ^2) by A2, XCMPLX_1:89 ;
 then p divides n ^2 by NAT_D:def 3;
 then p divides n by A1, NEWTON:80;
 then consider n1 being Nat such that
 A9: n = p * n1 by NAT_D:def 3;
 A10: m1 / n1 = sqrt p by A2, A4, A8, A9, XCMPLX_1:91;
 A11: n1 <> 0 by A3, A9;
 then p * n1 > 1 * n1 by A2, XREAL_1:98;
 hence contradiction by A5, A9, A11, A10;
end;
```

Summary

Today

- Introduction to Set Theory
- Bootstrapping Mathematics

Next time

- Mizar