Foundations for Formal Mathematics

Peter Koepke, University of Bonn, Germany

Mathematical Institute

5th Colloquium of HCM Research Area KL

Bonn, June 19, 2015

universitätbonn

The Naproche system (2011)

Axiom 1. For all x, y, z, $(x*y)*z = x*(y*z)$.

Axiom 2. For all x, $1*x = x$ and $x*1 = x$.

Axiom 3. For all x, $x*f(x) = 1$ and $f(x)*x = 1$.

Lemma 1. If $u*x = x$ then $u = 1$.

Proof. Suppose that $u*x = x$. Then $(u*x)*f(x) = x*f(x)$. By axiom 1, $u*(x*f(x)) = x*f(x)$. So by axiom 3 $u*1 = 1$. Then $u = 1$ by axiom 2. Qed.

Lemma 2. If $x*y = 1$ then $y = f(x)$.

Proof. Assume $x*y = 1$. Then $f(x)*(x*y) = f(x)*1$, i.e. $(f(x)*x)*y = f(x)$. Hence $1*y = f(x)$, i.e. $y = f(x)$. Qed.

Theorem 1. $f(x*y) = f(y)*f(x)$.

Proof. Let $u = (x*y)*(f(y)*f(x))$. Then $u = x*((y*f(y))*f(x))$ by axiom 1. So $u = x*(1*f(x)) = x*f(x) = 1$. Thus $(x*y)*(f(y)*f(x)) = 1$. Hence $(f(y)*f(x)) = f(x*y)$ by lemma 2. Qed.

SAD (System for Automated Deduction) + LaTeX macros (2012/13)

Theorem 1. *The set of prime numbers is infinite.*

Proof. Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. $\operatorname{ran} p \subseteq \mathbb{N}^+$. $\prod_{i=1}^{r} p_i$. Take $n = \prod_{i=1}^{r} p_i + 1$. n is nontrivial. Take a prime divisor q of n .

Let us show that q is not an element of A. Assume the contrary. Take i such that $(1 \leqslant i \leqslant r$ and $q = p_i$). p_i divides $\prod_{i=1}^{r} p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.

Hence A is not the set of prime numbers. $\square$

Foundations of mathematics

- Mathematicians tend to view “mathematical objects” like physical objects: take a number, insert x for y, divide x by y , ...

- Euclid’s elements: geometrical foundations, describing “obvious” geometrical notions, operations and facts

- Definition 1: A point is that which has no part.

- Postulate 1: To draw a straight line from any point to any point.

- In book 5 (Theory of proportions), magnitudes are treated geometrically in terms of lengths and areas

Foundations of mathematics

- Foundations of infinitesimal calculus involve the infinite (infinitesimals, limits, derivatives, ...)

- Non-Euclidean geometry

- Hilbert: geometrical and general axiomatics

Foundations of mathematics

- Dedekind, Cantor: the set concept as basic notion and as a foundation of mathematics

- integer numbers: $0=\emptyset$, $1=\{0\}$, $2=\{0,1\}$, ..., $n+1=\{0,1,\ldots,$ $n\}$, ...

- (positive) rational numbers as pairs $\{m,n\}$ of integers

- real numbers as Dedekind cuts $\{L,\ R\}$ in the set $\mathbb{Q}$ of rationals

Foundations of mathematics

- Frege: mathematical argumentation = formal derivation in a symbolic system

- set = extension of a formula

Foundations of mathematics

- Russell: the naive systems of Cantor and Frege are inconsistent:

$$y = \{x \mid x \notin x\}$$

$$y \in y \leftrightarrow y \notin y$$

- Avoiding the paradoxes: Russell's type theory; in the formula $x \in y$ the variable x needs to have different/lesser type than the variable y

- Avoiding the paradoxes: Zermelo's axiomatic set theory, with a comprehension axiom that does not yield the Russell "set"

Foundations of mathematics in the 20th century

- Zermelo-Fraenkel set theory has become the universally accepted foundation of mathematics; mathematical structures are sets with further components

- Gödel proved the fundamental theorems of mathematical logic

- Gödel completeness theorem: every universally true mathematical statement can be derived in the logical calculus (of Whitehead and Russell)

- Gödel incompleteness theorem(s): axiom systems like Peano arithmetic or Zermelo-Fraenkel set theory cannot prove their own consistency

Relative consistencies

- The consistency of mathematics cannot be proved mathematically (Failure of Hilbert's programme)

- There are *relative* consistency results: if the Zermelo-Fraenkel axioms are consistent, then so are the Zermelo-Fraenkel axioms with the addition of the axiom of choice

Formal mathematics

- Whitehead-Russell proposed to carry out all of mathematics formally

- The completeness theorem vindicates the programme of formal mathematics

- Due to complexity issues formal mathematics is only feasible using electronic computers

Formal mathematics

- Much of mathematics is carried semi-formally, involving intuitions, analogies, omissions, ...

- “Abuse of notation”: the vector space $\{0\}$ containing only the null vector 0 may also be denoted by 0. $0 = \{0\}$ will be inconsistent in most formal systems ($0 = 1$).

- Semi-formal mathematics avoids contradictions by only allowing “informed” abuse of notation

Formal mathematics

- Semi-formality is impossible with automatic computers: most automatic proving algorithms are based on proofs by contradictions and are actively searching for the nearest available contradiction

- Computer-supported formal mathematics requires (relatively) consistent foundations

Formal mathematics

- The language of the standard axioms of set theory is minimal, only involving the non-logical symbol $\in$

- Mathematics develops and needs rich language(s) to capture its many domains: numbers, structures, functions, diagrams, matrices, ...

- Logical calculi studied in mathematical logic only involve a few rules. E.g., resolution with Skolemization and unification is universal for first-order logic

- Mathematics uses many figures of argumentation

- Natural computer-supported formal mathematics requires rich languages and calculi

Marcos Cramer's dissertation: class-map-tuple-number theory

- unrestricted maps also lead to a Russell paradox

$$g(f) := \begin{cases} 1\text{, if } f(f) = 0 \text{ or if undefined} \\ 0, \text{ else} \end{cases}$$

$$g(g) = 0 \text{ iff } g(g) = 1$$

- class-sized maps like $x, y \mapsto \{x, y\}$ or $x \mapsto$ the complement of x are important for mathematics

- use existence axioms as in Ackermann set theory

- $\forall y\ (F(y) \rightarrow L(y)) \rightarrow \exists x\ (C(x) \wedge L(x) \wedge \forall y(y \in x \leftrightarrow F(y)))$, for formulas F which do not contain the symbol L for “limited size”

Marcos Cramer's class-map-tuple-number theory

- type C for classes

- type $M(., n)$ for maps

- $\in$

- types for tuples and maps of various arities

- an inductive type for natural numbers

- a unary “hyper-class” L for “small” classes

- standard axioms for tuples and numbers

Marcos Cramer's class-map-tuple-number theory

- Ackermann-type function existence schema

$$\forall x \in L \exists y \in L\, R(x, y) \rightarrow \exists f \in L \forall x \in L\, R(x, f(x))$$

where the formula R does not contain the symbol L

- this axiom also implies the axiom of choice

Marcos Cramer's class-map-tuple-number theory

- Ackermann-type function existence schema

$$\forall x \in L \exists y \in L\, R(x, y) \rightarrow \exists f \in L \forall x \in L\, R(x, f(x))$$

where the formula R does not contain the symbol L

- motivation for this schema:

For all x there is an a_x such that ...

- This implicitly postulates the existence of a function $a_{\dots}$, in general also assuming the axiom of choice for choosing from the possible candidates for a_x.

Marcos Cramer's class-map-tuple-number theory

- Class-map-tuple-number theory is consistent iff Ackermann set theory with the axiom of choice is consistent

- Ackermann set theory with the axiom of choice is consistent iff Zermelo-Fraenkel set theory is consistent (Levy 1959 and Reinhard 1970)

Thank You!