Pure Math Student Seminar: Russell's Paradox and Polynomials

Riley Moriss

April 23, 2023

Contents

1 Outline **1**

2 A Logic **1**

3 Sequent Calculus **2**

4 Russells Paradox **3**

5 Light Affine Set Theory **4**

6 What can you do in LAST? **5**

Outline

So what is a logic, why naive set theory failed, possible replacement, another reason to care about the replacement (ZFC vs LAST)

A Logic

One might consider logic to be THE correct rules of thought. Such a thing does not exist, in its place we have a plethora of logics. In the field of proof theory a logic is three things:

Definition:

A sequent calculus is

1. A collection of terms (or formulas)
2. A collection of types
3. Deduction rules (provability)

Sequent Calculus

Definition:

The intuitionistic sequent calculus (LJ)

- A single type (ignore)
- A countable collection of atomic propositions $\{A, B, ...\}$
- Inductively define the rest of the propostitions by: If X is a proposition then so is $\neg X$ and if X, Y are propositions then so is $X \implies Y$
- Deduction rules below

$$\frac{}{A \vdash A}\text{Ax}$$

$$\frac{\Gamma_1 \vdash A \qquad \Gamma_2, A \vdash C}{\Gamma_1, \Gamma_2 \vdash C}\text{cut}$$

$$\frac{\Gamma_1 \vdash A \qquad \Gamma_2, B \vdash C}{\Gamma_1, \Gamma_2, A \implies B \vdash C}\text{LI}$$

$$\frac{A, \Gamma \vdash B}{\Gamma \vdash A \implies B}\text{RI}$$

$$\frac{\Gamma \vdash C}{A, \Gamma \vdash C}\text{weak}$$

$$\frac{\Gamma \vdash}{\Gamma \vdash A}\text{weak right}$$

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash}$$

$$\frac{A, A, \Gamma \vdash B}{A, \Gamma \vdash C}\text{Con}$$

$$\frac{A, \Gamma \vdash}{\Gamma \vdash \neg A}$$

The deduction rules introduce the sequent and the turnstile. This is all syntax however it can be motivated through maybe a more familiar concept of logic, truth evaluations and formulas where a sequent can be read as: sequences of formulas on the left can be read as "and'ed" together and sequences on the right are "or'ed" together.

$$A, B, C \vdash D, E, F \approx A \wedge B \wedge C \implies D \vee E \vee F$$

The horizontal line can also be read as saying that if we have a proof of the sequents on the top line then we have a proof of the sequent on the bottom (implication).

There is a subtlety about what you take as foundations and where this discussion is taking place. If its inside ZFC then the sequent can be thought of multisets with labels left and right or some such thing. However that would be dishonest as ultimately ZFC is formalised as a language or sequent calculus.

Then a proof in a sequent calculus is a tree of sequents where one node is connected to another by a deduction rule. This is if you feel more comfortable in ZFC. A proof may also be taken to be foundational.

Definition:

If A is a proposition with set variable x then

$$A[S/x]$$

is the proposition obtained by replacing all occurences of x with S (symbolically)

To enrich this logic (a calculus of truth) to a set theory (a calculus of truths about sets) we need to distinguish between terms and formulas.

Definition:

Naive set theory will be the sequent calculus LJ with the following additions

- A new type (sets)
- Terms of the new type will be generated beginning with a countable set of variables $\{x, y, ...\}$
- Then if A is a proposition and x is a set variable then $\{x|A\}$ is a set
- If X, Y are sets then $X \in Y$ is a proposition

Finally we add two new deduction rules called comprehension

$$\frac{A[t/x], \Gamma \vdash C}{t \in \{x|A\}, \Gamma \vdash C} \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash t \in \{x|A\}}$$

Russells Paradox

The set theory above is called naive because our comprehension is unrestricted. Any formula allows us to define a set. At the turn of the century mathematicians were using this theory until Russell pointed out that there was a set $R = \{x|x \notin x\}$ such that $R \in R \iff R \notin R$. This is a clear contradiction.

Definition:

A contradiction in a sequent calculus is a proof of the empty sequent

$$\vdash$$

Consider the following wff in naive set theory

$$A := x \notin x, \qquad R := \{x : A(x)\} = \{x : x \notin x\}$$

Combining these with our deduction rules from comprehension we get the following

$$\frac{\Gamma \vdash \Delta, A[R/x] \quad (= R \notin R)}{\Gamma \vdash \Delta, R \in \{x : A(x)\} \quad (= R \in R)} \text{(comp1)} \qquad \frac{\Gamma, A[R/x] \quad (= R \notin R) \vdash \Delta}{\Gamma, R \in \{x : A(x)\} \quad (= R \in R) \vdash \Delta} \text{(comp2)}$$

Which putting it all together we get the following proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{R \in R \vdash R \in R}\,(\text{ax})}{R \in R, R \notin R \vdash}\,(\neg)}{R \in R, R \in R \vdash}\,(\text{comp1})}{R \in R \vdash}\,(\text{con})}{\vdash R \notin R}\,(\neg)}{\vdash R \in R}\,(\text{comp}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{R \notin R \vdash R \notin R}\,(\text{ax})}{R \notin R, R \in R \vdash}\,(\neg)}{R \in R, R \in R \vdash}\,(\text{comp2})}{R \in R \vdash}\,(\text{con})}{\vdash}\,(\text{cut})}{\vdash B}\,(\text{weak})$$

Because B is an arbitrary formula this is a clear contradiction.

What went wrong here? How can we stop such a construction from taking place. The classical answer given by Zermelo and others was to restrict the unrestricted comprehension. You are now only allowed to form subsets of preexisting sets with comprehension, not quantify over the universe of sets. We can see however that there are many things at play in this proof. Is it possible that we could limit one of the other rules and retain our naive comprehension?

Light Affine Set Theory

Definition:

The sequent calculus LAST is LJ + Naive set theory with the following modifications

- If A is a formula then so is $!A$ and $\S A$.

And the deduction rules are modified for these new modalities

$$\dfrac{B \vdash A}{!B \vdash !A}$$

$$\dfrac{!A, !A, \Gamma \vdash B}{!A, \Gamma \vdash C}\,\text{Con}$$

$$\dfrac{\Gamma, \Delta \vdash A}{!\Gamma, \S\Delta \vdash \S A}$$

Its clear that the proof above of Russells paradox does not go through because we are unable to contract hence cutting will result merely back at the axiom rule. Notice that contraction is not removed but simply restricted through the use of "modalities".

How can we convince ourselves that this system doesnt have some other pathalogical proof that will result in another paradox?

Definition:

A sequent calculus satisfies cut elimination if every sequent that is provable is provable without the use of cut.

Theorem

LAST satisfies cut elimination

Proof. This proof is quite technical and long.

Theorem

(Subformula property) Every formula above the line must be a subformula of those below the line (in a proof)

Proof. Cut is the only rule that removes a formula. Hence if a formula appears above the line it must appear below the line.

Theorem

LAST is consistent.

Proof. A proof of the empty sequent will have a cut free version. Then by the subformula property it must be an axiom however there is no such axiom.

One must be careful here, why doesnt this contradict Godels incompleteness theorem? It shows the consistency using the tools of ZFC to make inductive arguments and hence the consistency of LAST is dependent on the consistency of ZFC (cut elimination uses induction).

What can you do in LAST?

The modality § is an example of a general idea in Linear Logic called stratification. It allows one to more carefully manage the other modalities ! and its dual ? by keeping track of their depth in the proof. LL is the classic example of a substructural logic that distinguishes between the finite A and the infinite $!A$. This is a resource aware logic, the perfect place to discuss issues of resources of computation.

Theorem

$$\text{A function is computable in polynomial time} \iff \text{it is representable in LAST}$$

Proof. The proof is very long and technical. I aim only to explain the statement.

Definition:

a set T (in ZFC) is represented by a set t (in LAST) iff there is a bijection (in ZFC) between

$$T \xrightarrow{\sim} \{x \in \text{ LAST terms } :\vdash x \in t \text{ is provable}\}$$

Definition:

A function (set in ZFC) $F : U \to C$ is then represented by a set f (in LAST) if U and C are represented by u and c respectively and

$$\vdash \forall x \in u.\S^d(\exists^! y.\langle x, y\rangle \in f)$$

is provable.

We can ignore for clarity the paragraph to see that this simply says that there is some domain-codomain pair such that $f(x) = y$.

Definition:

A TM is a triple (States, tape alphabet, transition function). A function Φ is polynomial time if there is some turing machine M and some monotone polynomial p such that after $p(|w|)$ steps M gives $\Phi(w)$.

Hopefully now we can read the theorem. If we were to prove it we would need to discuss many more things like lambda calculus, curry howard, normalisation etc. The idea of the proof is:

- ($\Rightarrow$): You show that each of the small pieces that make up a polytime TM are representable and show that the composition of representable functions are representable (step function is the main one).
- ($\Leftarrow$): You show that ever proof in LAST can be assigned a term in a strongly polynomial normalising lambda calculus (and notice that a function is represented when something is provable hence you identify the representability with that proof).