Proof Theory of Martin-Löf Type Theory

Anton Setzer
Swansea University, Swansea UK
http://www.cs.swan.ac.uk/~csetzer/

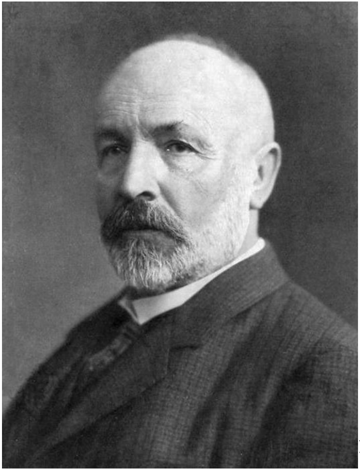
Proof Society Summer School, Swansea 2019
https://www.proofsociety.org/summer-school-2019/

8 September 2019

Foundational Crisis of Mathematics

- Development of axiom systems for mathematics at the end of the 19th/beginning of the 20th century.
- Developent of axiomatisations of mathematics.
- Cantor: Development of set theory.
- Discovery of inconsistencies.

Georg Cantor

 [1]

[1] https://upload.wikimedia.org/wikipedia/commons/e/e7/Georg_Cantor2.jpg

Cantor's Naive Set Theory

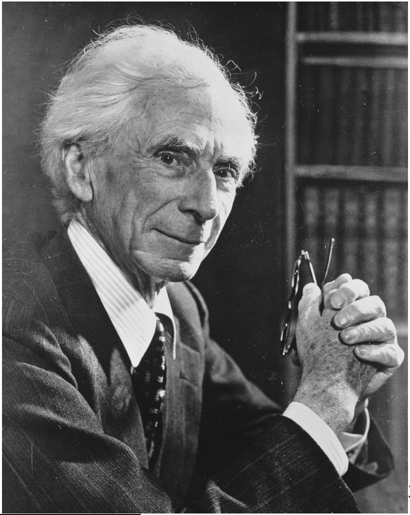
- Cantor [6]: "Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen."
- Translation ([7]) "By an "aggregate" we are to understand any collection into a whole M of definite and separate objects m of our intuition or our thought. These objects are called the "elements" of M."
- Sounds completely intuitive.
- From this one seems to derive full comprehension.
  $\{x \mid \varphi(x)\}$ is a set for any formula φ.
- Most mathematicians are essentially working in this theory (however most will be aware of ZF set theory).
- But it is inconsistent (Russell's paradox).

Bertrand Russell

[2]

[2] https://upload.wikimedia.org/wikipedia/commons/f/fd/Bertrand_Russell_in_1876.jpg

Bertrand Russell a bit older

[3]

[3] https://upload.wikimedia.org/wikipedia/commons/5/5f/Bertrand_Russell_1957.jpg

Hilbert's Program

[4]

- Hilbert: Prove the consistency of axiom systems of mathematics using finitary methods.

[4] https://upload.wikimedia.org/wikipedia/commons/7/79/Hilbert.jpg

Gödel's Second Incompleteness Theorem

[5]

- Gödel: Any consistent theory fulfilling relatively weak assumptions doesn't prove its own consistency.
  - Since finitary methods can be considered as a sub theory of most theories, this means finitary methods cannot prove the consistency of any consistent theory fulfilling the conditions of Gödel's second incompleteness theorem.
- Therefore Hilbert's original program cannot be carried out.

[5] https://upload.wikimedia.org/wikipedia/en/4/42/Kurt_g%C3%B6del.jpg

Gentzen – Reduction of Consistency of PA to Well-Foundedness up to ϵ_0

[6]

- In 1936 Gentzen proved [9] the consistency of Peano Arithmetic by using transfinite induction up to ϵ_0.

[6] https://upload.wikimedia.org/wikipedia/commons/b/bc/Gerhard_Gentzen.jpg

Gentzen – Reduction of Consistency of PA to Well-Foundedness up to ϵ_0

- This is widely regarded as a consistency proof which settles the consistency problem.
  - Reason is that one can easily convince oneself of the well-foundedness of an ordinal notation system up to ϵ_0.
- Gentzen's proof shows that the consistency of Peano Arithmetic follows from the fact that there are no infinite descending sequences in an ordinal notation system of ordertype ϵ_0.
- An argument how to obtain this explicitly using Buchholz' Finitary Derivations can be found in Appendix 6.1.
  - You can program and run it!

Intuitive Well-foundedness Proofs

- One can now see intuitively that there are no infinite descending sequences in an ordinal notation system of order type ϵ_0.
  See Appendix 6.2.
- The author claims this can be extended up to $|(\Pi^1_1 - \mathrm{CA})_0|$ [16, 17], but he has not yet succeeded in pushing this to $|(\Pi^1_1 - \mathrm{CA})|$ (formally one can extend this approach, but without a fully intuitive well-ordering proof).
- However, using ordinal notation systems one gets intuitive well-foundedness proofs for reasonably strong mathematical theories.
- The fact that one has some insight into its well-foundedness might be one essential criteria for having natural well-orderings.
  See the discussion in Appendix 6.3 about a trivial ordinal analysis of any consistent theory fulfilling minimal conditions, which means an ordinal analysis needs to obtain more than just an ordinal notation system of strength the proof theoretic strength of the theory.

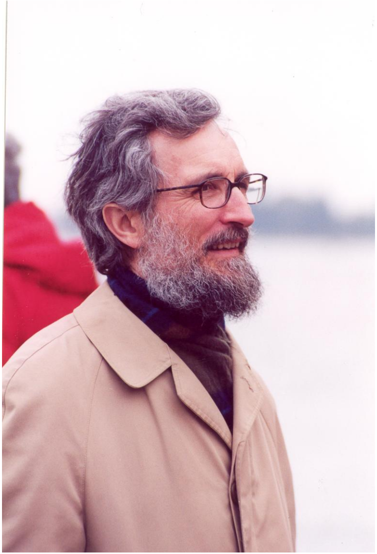
Use of Trustworthy Theories

- The alternative to getting a direct insight into the well-foundedness is to prove the consistency of the theories in question in a second theory, which is more trustworthy.
- One alternative was $\mathrm{PRA} + \mathrm{TI}_\alpha$ for an ordinal notation system of ordertype α with some direct insight.
  - Note that this is a classical theory.
- One theory are Feferman's systems of Explicit mathematics.
- The theory which was developed most for serving as a such a theory is Martin-Löf Type Theory.
  - Martin-Löf told the author something like the following (his words were philosophically much more sophisticated):
    Intuitionistic Type Theory is the most serious attempt to develop a theory such that we have a direct insight into its validity.
- There are other candidates for it, e.g. developed by Dybjer, Aczel.

Revised Hilbert's Program

- So a revised Hilbert's program could be to prove the consistency of large axiom systems for formalising mathematical proofs by reducing it to a theory, for which we have an intuitive understanding into its consistency.
- One candidate for such a theory are extensions of Martin-Löf Type Theory.
- In the appendix 6.4 we will discuss some myths about a revised Hilbert's program such as that one is forced to become a a constructivist.
- See as well the author's article [19].

Per Martin-Löf (Stockholm)



Foundational Approach vs Axiomatic Approach

- Martin-Löf Type Theory (MLTT, [13]) often criticised because of its length of rules.
- Why not shorten it by defining a minimal set of axioms?
- Answer:
  - MLTT is developed to be a foundational theory, such that in each step we are clear about the validity of its judgements.
  - Axiomatic approach is very suitable when formalising a theory the consistency of which one proves in a different theory, often by giving an interpretation in set theory.
  - It turns out that the approach of developing a foundational theory resulted in a theory which is very suitable for implementation in proof assistants.
    - When carrying proofs out by hand we translate intuitively axioms into rules.
    - For instance one usually doesn't use the induction axiom but applies induction as a rule.
    - When carrying out proofs on the machine the machine needs to make those intuitive steps explicit.

Meaning Explanations

- Meaning explanations assign to every derivable judgement of MLTT a sentence expressing its meaning.
- The meaning explanation is essentially a natural language formalisation of a PER model of type theory.
- For each rule one should argue why intuitively, if the statements for the premises is valid, so is the conclusion.
- This way we obtains an intuitive argument why every statement proved in MLTT is valid, without referring to another theory.
- So meaning explanation is a way of showing the validity of all statements provable in MLTT in an absolute way.
- We will not elaborate in these lectures on meaning explanations.

Functional Notation

- Most of the papers related to MLTT refer to proof assistants such as Agda.
- Those proof assistants are based on functional programming and use functional programming notation, i.e. one writes for the successor of a natural number

$$\mathrm{S}\ n$$

instead of

$$\mathrm{S}(n)$$

- We will as well use functional notation.

Judgements of Type Theory

- The statements of type theory are called **"judgements"**.
- There are four judgements of type theory:
  - A is a type written as
$$A : \mathrm{Set}$$
  - A and B are equal types written as
$$A = B : \mathrm{Set}$$
  - a is an element of type A written as
$$a : A$$
  - a, b are equal elements of type A written as
$$a = b : A$$

$s \longrightarrow t$ vs $s = t$

- The notion of reduction
$$s \longrightarrow t$$
corresponds to computation rules where term s evaluates to t.
- In type theory one uses instead
$$s = t$$
which is the reflexive/symmetric/transitive closure of $\longrightarrow$ or equivalence relation containing $\longrightarrow$.
- In most rules when concluding
$$s = t : A$$
it is actually the case that we have a reduction
$$s \longrightarrow t$$

$s \longrightarrow t$ vs $s = t$

- The notion

$$s \longrightarrow t$$

doesn't occur in the formal theory of Martin-Löf Type Theory, but only when implementing it.

Dependent Judgements

- We have as well **dependent judgements**, for instance for expressing

$$\text{if } x : \mathbb{N} \text{ then } \mathrm{S}\ x : \mathbb{N}$$

  which we write

$$x : \mathbb{N} \Rightarrow \mathrm{S}\ x : \mathbb{N}$$

- Examples:

$$\begin{array}{lcl} x : \mathbb{N}, y : \mathbb{N} & \Rightarrow & x + y : \mathbb{N} \\ x : \mathbb{N} & \Rightarrow & x + 0 = x : \mathbb{N} \\ x : \mathrm{List} & \Rightarrow & \mathrm{Sorted}\ x : \mathrm{Set} \\ & \Rightarrow & \mathrm{Sorted}\ [\,] = \mathrm{True} : \mathrm{Set} \end{array}$$

Examples of Dependent Judgements

- In general a dependent judgement has the form

$$x_1 : A_1, x_2 : A_2(x_1), \ldots, x_n : A_n(x_1, \ldots, x_{n-1}) \Rightarrow \theta(x_1, \ldots, x_n)$$

where, if write $\vec{x}$ for $x_1, \ldots, x_n$

$$\theta(\vec{x})$$

is one of the four judgements before

$$\begin{array}{lll} B(\vec{x}) : \mathrm{Set} & \text{or} & B(\vec{x}) = B'(\vec{x}) : \mathrm{Set} \quad \text{or} \\ b(\vec{x}) : B(\vec{x}) & \text{or} & b(\vec{x}) = b'(\vec{x}) : B(\vec{x}) \end{array}$$

Four Kinds of Rules for each Type

For each type A there are 4 kinds of rules:

- **Formation rules:**
  They form a new type e.g.
  $$\mathbb{N} : \mathrm{Set}$$
- **Introduction Rules:**
  They introduce elements of a type, e.g.
  $$0 : \mathbb{N} \qquad \frac{n : \mathbb{N}}{\mathrm{S}\ n : \mathbb{N}}$$

Four Kinds of Rules for each Type

- **Elimination Rules:**
  They allow to construct from an element of one type elements of another type.
  For instance the elimination rule for $\mathbb{N}$ is higher type primitive recursion and corresponds to the rule

$$\frac{\begin{array}{cc} n : \mathbb{N} \Rightarrow B\ n : \mathrm{Set} & \mathit{step}_0 : B\ 0 \\ n : \mathbb{N}, b : B\ n \Rightarrow \mathit{step}_{\mathrm{S}}\ n\ b : B\ (\mathrm{S}\ n) & n : \mathbb{N} \end{array}}{\mathrm{elim}_{\mathbb{N}}\ B\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ n : B\ n}$$

- Here $B\ s$ stands for $B'[n := s]$ for some fixed B', n,
- and B on its own stands for $(n)B'$.
- Similarly $\mathit{step}_{\mathrm{S}}\ n\ b$ stands for $\mathit{step}'_{\mathrm{S}}[x := n, y := b]$ for some $\mathit{step}'_{\mathrm{S}}$, x, y.

Four Kinds of Rules for each Type

- **Equality Rules:**
  They show how if we introduce an element of that type and then eliminate it how it is computed

$$\frac{n : \mathbb{N} \Rightarrow B\ n : \mathrm{Set} \qquad step_0 : B\ 0 \qquad n : \mathbb{N}, b : B\ n \Rightarrow step_{\mathrm{S}}\ n\ b : B\ (\mathrm{S}\ n)}{\mathrm{elim}_{\mathbb{N}}\ B\ step_0\ step_{\mathrm{S}}\ 0 = step_0 : B\ 0}$$

Four Kinds of Rules for each Type

$$\frac{\begin{array}{cc} n:\mathbb{N} \Rightarrow B\ n : \mathrm{Set} & \mathit{step}_0 : B\ 0 \\ n:\mathbb{N}, b : B\ n \Rightarrow \mathit{step}_{\mathrm{S}}\ n\ b : B\ (\mathrm{S}\ n) & n:\mathbb{N} \end{array}}{\begin{array}{l} \mathrm{elim}_{\mathbb{N}}\ B\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ (\mathrm{S}\ n) \\ \qquad = \mathit{step}_{\mathrm{S}}\ n\ (\mathrm{elim}_{\mathbb{N}}\ B\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ n) : B\ (\mathrm{S}\ n) \end{array}}$$

- For readability we will usually omit the premises of the equality rules.

Equality Versions of the Rules

- There are as well equality versions of the above rules.
- They express that if the premises of a rule are equal the conclusions are equal as well.
- For instance the equality version of the rule

$$\frac{n : \mathbb{N}}{\mathrm{S}\ n : \mathbb{N}}$$

is

$$\frac{n = m : \mathbb{N}}{\mathrm{S}\ n = \mathrm{S}\ m : \mathbb{N}}$$

Remarks on the Complexity of the Rules

- The elimination rules are very long because they are generic rules.
- In proof assistants based on MLTT one usually defines just instances of it.
- So we define for instance

$$
\begin{array}{lcl}
n, m : \mathbb{N} \to n + m : \mathbb{N} & & \\
n + 0 & = & n \\
n + \mathrm{S}\ m & = & \mathrm{S}\ (n + m)
\end{array}
$$

Canonical vs Non-Canonical Elements

- The elements introduced by an introduction rule start with a constructor.
- For instance the constructors of $\mathbb{N}$ are

$$0 \quad \text{and} \quad \mathrm{S}$$

- Elements introduced by an introduction rule are called **canonical elements**.
  - Canonical elements of $\mathbb{N}$ are for instance

$$0 \qquad \mathrm{S}\,(0+0)$$

    where + is defined using elimination rules.
- Elements introduced by an elimination rule are **non-canonical** elements. For instance

$$0+0$$

- Using the equality rules, every non canonical element of a type is supposed to evaluate to a canonical element of that type.

Canonical elements of $\mathbb{N}$

- A canonical element of $\mathbb{N}$ can be evaluated further.
- E.g. we have
$$\mathrm{S}\ (0 + 0) \longrightarrow \mathrm{S}\ 0$$
- In case of a function type $\lambda x.t$ is considered to be canonical.
- Note that in
$$\lambda x.x : \mathbb{N} \to \mathbb{N}$$
x doesn't start with a constructor (doesn't even make sense to ask for it, because it is an open term).
So here it is crucial that it is only required that a canonical element starts with a constructor.

Canonical elements of $\mathbb{N}$

- The type checking of equality is based on this notation of canonical element or head normal form.
  - In order to check
    $$s = t : \mathbb{N}$$
    we first reduce s and t to canonical form.
  - If they start with different constructors, s and t are different. E.g. if $s \longrightarrow 0$, $t \longrightarrow \mathrm{S}\ t'$ there is no need to evaluate t'.
  - If they have the same constructor, e.g. $s \longrightarrow \mathrm{S}\ s'$ $t \longrightarrow \mathrm{S}\ t'$ then we compare s' and t'.

Functional Notation and the Logical Framework

- In case of S one could state as an introduction rule

$$\mathrm{S} : \mathbb{N} \to \mathbb{N}$$

- This works for some constructions, but especially for elimination rules (which will be discussed in detail below) treating the operators as functions would require the logical framework (LF).

Functional Notation and the Logical Framework

- For instance the eliminator for the natural numbers (which is higher type primitive recursion) would in the LF have type

$$
\begin{aligned}
\mathrm{elim}_{\mathbb{N}} : & \ (C : \mathbb{N} \to \mathrm{Set}) \to C\ 0 \to ((n : \mathbb{N}) \to C\ n \to C\ (\mathrm{S}\ n)) \\
& \to (n : \mathbb{N}) \to C\ n
\end{aligned}
$$

- But there is no corresponding type in MLTT without LF for this.

Functional Notation and the Logical Framework

- We avoid the LF because it causes foundational problems.
  - The LF doesn't add strength, but the argument requires a reduction of the MLTT with LF to MLTT without LF.
  - Any direct model construction would need to interpret the LF as adding another universe Set to MLTT, but that would add more strength then is needed.
  - We don't know of any meaning explanation which deal with the LF in a good way.
  - Therefore we prefer to work with MLTT as a foundational theory as MLTT without the LF.
  - The goal is use as foundational theory where the insight into its consistency is as immediate as possible without using any complex mathematical argument.
  - For proof assistants and as a programming language MLTT with LF is more suitable.

LF as an Abbreviation

- However we treat the LF as an abbreviation.
- So when writing

$$\frac{\begin{array}{cc} B : \mathbb{N} \to \mathrm{Set} & \mathit{step}_0 : B\ 0 \\ \mathit{step}_{\mathrm{S}} : (n : \mathbb{N}) \to B\ n \to B\ (\mathrm{S}\ n) & n : \mathbb{N} \end{array}}{\mathrm{elim}_{\mathbb{N}}\ B\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ n : B\ n}$$

we mean

$$\frac{\begin{array}{c} n : \mathbb{N} \Rightarrow B\ n : \mathrm{Set} \\ \mathit{step}_0 : B\ 0 \\ n : \mathbb{N}, b : B\ n \Rightarrow \mathit{step}_{\mathrm{S}}\ n\ b : B\ (\mathrm{S}\ n) \\ n : \mathbb{N} \end{array}}{\mathrm{elim}_{\mathbb{N}}\ B\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ n : B\ n}$$

where

- $B\ t$ stands for $B'[n := t]$ for some fixed B', n, and
- B standing alone stands for $(n)B'$.

The Type of Booleans

- One of the simplest types is the type of Booleans.
- **Formation rule:**

$$\mathbb{B} : \mathrm{Set}$$

- **Introduction rules:**

$$\mathrm{tt} : \mathbb{B} \qquad \mathrm{ff} : \mathbb{B}$$

- **Elimination rule:**

$$\frac{C : \mathbb{B} \to \mathrm{Set} \qquad \mathit{step}_{\mathrm{tt}} : C\ \mathrm{tt} \qquad \mathit{step}_{\mathrm{ff}} : C\ \mathrm{ff} \qquad b : \mathbb{B}}{\mathrm{elim}_{\mathbb{B}}\ C\ \mathit{step}_{\mathrm{tt}}\ \mathit{step}_{\mathrm{ff}}\ b : C\ b}$$

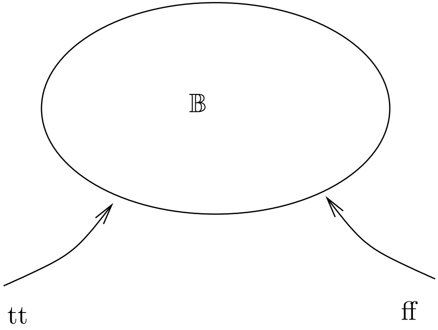
We will in the following omit type arguments such as C in $\mathrm{elim}_{\mathbb{B}}\ C\ \mathit{step}_{\mathrm{tt}}\ \mathit{step}_{\mathrm{ff}}\ b$.

Basic Types: Type of Booleans

- **Equality rules:**

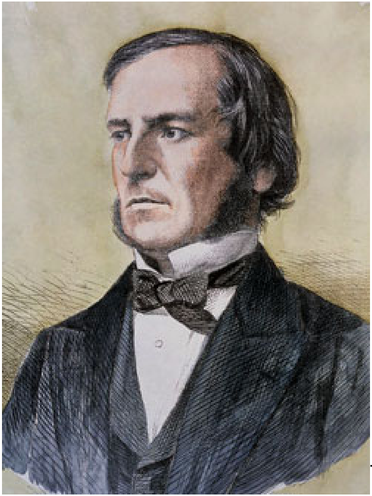
$$\begin{aligned}\mathrm{elim}_{\mathbb{B}}\ \mathit{step}_{\mathrm{tt}}\ \mathit{step}_{\mathrm{ff}}\ \mathrm{tt} &= \mathit{step}_{\mathrm{tt}} : C\ \mathrm{tt} \\ \mathrm{elim}_{\mathbb{B}}\ \mathit{step}_{\mathrm{tt}}\ \mathit{step}_{\mathrm{ff}}\ \mathrm{ff} &= \mathit{step}_{\mathrm{ff}} : C\ \mathrm{ff}\end{aligned}$$

Visualisation (Booleans)



2 Constructors, both no arguments.

George Boole

[7]

[7] https://upload.wikimedia.org/wikipedia/commons/c/ce/George_Boole_color.jpg

Finite Types

- Similar versions for types with $0, 1, 3, 4, \ldots$ elements.
- Special case $\emptyset$.

Empty Type

- **Formation rule:**

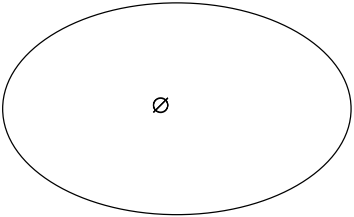
$$\emptyset : \mathrm{Set}$$

- **Introduction rules:**
  There is no introduction rule.
- **Elimination rule:**

$$\frac{x : \emptyset \Rightarrow C\ x : \mathrm{Set} \qquad e : \emptyset}{\mathrm{efq}\ e : C\ e}$$

- **Equality rules:**
  There is no equality rule.

Visualisation ($\emptyset$)



Ancient Picture of the Empty Set

[8]

[8] https://upload.wikimedia.org/wikipedia/commons/f/f1/Enso.jpg

The Disjoint Union

- **Formation rule:**

$$\frac{A : \mathrm{Set} \qquad B : \mathrm{Set}}{A + B : \mathrm{Set}}$$

- **Introduction rules:**

$$\frac{a : A \qquad B : \mathrm{Set}}{\mathrm{inl}\ a : A + B} \qquad \frac{A : \mathrm{Set} \qquad b : B}{\mathrm{inr}\ b : A + B}$$

- Note that we omitted presupposed premises, for instance $A : \mathrm{Set}$ is a presupposition of $a : A$ and therefore omitted.

The Disjoint Union

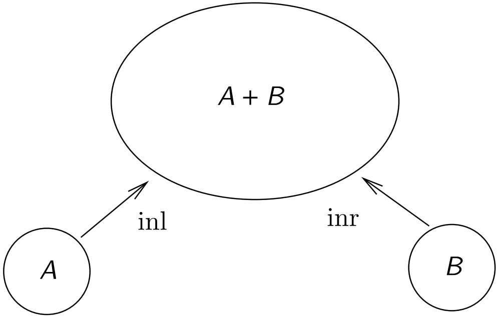
- **Elimination rule:**

$$\frac{\begin{array}{c} C : (A + B) \to \mathrm{Set} \\ \mathit{step}_{\mathrm{inl}} : (x : A) \to C\ (\mathrm{inl}\ x) \\ \mathit{step}_{\mathrm{inr}} : (x : B) \to C\ (\mathrm{inr}\ x) \\ c : A + B \end{array}}{\mathrm{elim}_{+}\ \mathit{step}_{\mathrm{inl}}\ \mathit{step}_{\mathrm{inr}}\ c : C\ c}$$

- **Equality rules:**

$$\begin{array}{rcl} \mathrm{elim}_{+}\ \mathit{step}_{\mathrm{inl}}\ \mathit{step}_{\mathrm{inr}}\ (\mathrm{inl}\ a) & = & \mathit{step}_{\mathrm{inl}}\ a : C\ (\mathrm{inl}\ a) \\ \mathrm{elim}_{+}\ \mathit{step}_{\mathrm{inl}}\ \mathit{step}_{\mathrm{inr}}\ (\mathrm{inr}\ b) & = & \mathit{step}_{\mathrm{inr}}\ b : C\ (\mathrm{inr}\ b) \end{array}$$

Visualisation ($A + B$)



$+$ as $\vee$

- A proof of $A \vee B$ is a proof of A or a proof of B.
- So $A \vee B$ is just $A + B$.

The Σ-Type

- **Formation rule:**
$$\frac{B : A \to \mathrm{Set}}{\Sigma\ A\ B : \mathrm{Set}}$$
Note that $A : \mathrm{Set}$ is a presupposition of $B : A \to \mathrm{Set}$.
- **Introduction rule:**
$$\frac{B : A \to \mathrm{Set} \qquad a : A \qquad b : B\ a}{\mathrm{p}\ a\ b : \Sigma\ A\ B}$$

The Σ-Type

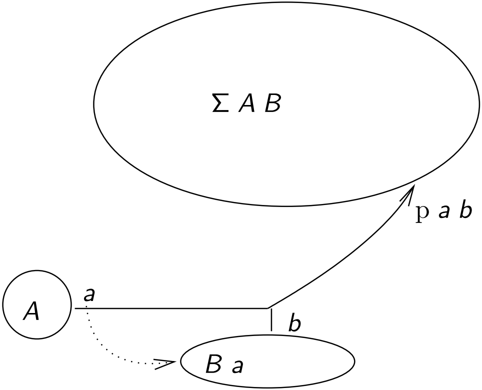
- **Elimination rule:**

$$\frac{\begin{array}{c} C : (\Sigma\ A\ B) \to \mathrm{Set} \\ \mathit{step} : (a : A, b : B\ a) \to C\ (\mathrm{p}\ a\ b) \\ c : \Sigma\ A\ B \end{array}}{\mathrm{elim}_{\Sigma}\ \mathit{step}\ c : C\ c}$$

- **Equality rule:**

$$\mathrm{elim}_{\Sigma}\ (\mathit{step}\ (\mathrm{p}\ a\ b)) = \mathit{step}\ a\ b : C\ (\mathrm{p}\ a\ b)$$

Visualisation ($\Sigma\ A\ B$)



$\exists$ as Σ

- A proof of $\exists\, x : A.B\ x$ is
  - an $a : A$
  - together with a $b : B\ a$
- That's just an element of

$$\Sigma\ A\ B$$

The Π-Type

- **Formation rule:**

$$\frac{B : A \to \mathrm{Set}}{\Pi\ A\ B : \mathrm{Set}}$$

- **Introduction rule:**

$$\frac{B : A \to \mathrm{Set} \qquad x : A \to t : B\ x}{\lambda x.t : \Pi\ A\ B}$$

The Π-Type

- **Elimination rule:**

$$\frac{f : \Pi\ A\ B \qquad a : A}{\mathrm{Ap}\ f\ a : B\ a}$$

- **Equality rule:**

$$\mathrm{Ap}\ (\lambda x.t)\ a = t[x := a] : B\ a$$

- Let $A \to' B := \Pi\ A\ ((x)B)$ for some fresh variable x.

The Small Logical Framework

- The Π-type doesn't really follow the pattern of the other inductive types.
- One way around is to add the small LF dependent function type $(x : A) \to B$ (where $A : \mathrm{Set}$, $x : A \Rightarrow B : \mathrm{Set}$) as a type with essentially the rules of the Π-type.
- The restricted large LF we used above (taking only the first level) could still be used.
- Then we can define an inductive Π-type with introduction rule

$$\lambda : ((x : A) \to B\ x) \to \Pi\ A\ B$$

  That's how the Π-type is considered in MLTT with LF.
- We will in the following refer to MLTT without the small LF.

Natural numbers

- **Formation rule:**

$$\mathbb{N} : \mathrm{Set}$$

- **Introduction rules:**

$$0 : \mathbb{N} \qquad \frac{n : \mathbb{N}}{\mathrm{S}\ n : \mathbb{N}}$$

- **Elimination rule:**

$$\frac{\begin{array}{c} C : \mathbb{N} \to \mathrm{Set} \\ step_0 : C\ 0 \qquad step_{\mathrm{S}} : (n : \mathbb{N}, C\ n) \to C\ (\mathrm{S}\ n) \qquad n : \mathbb{N} \end{array}}{\mathrm{elim}_{\mathbb{N}}\ step_0\ step_{\mathrm{S}}\ n : C\ n}$$

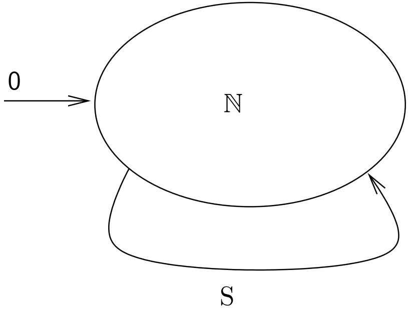
Natural numbers

- **Equality rules:**

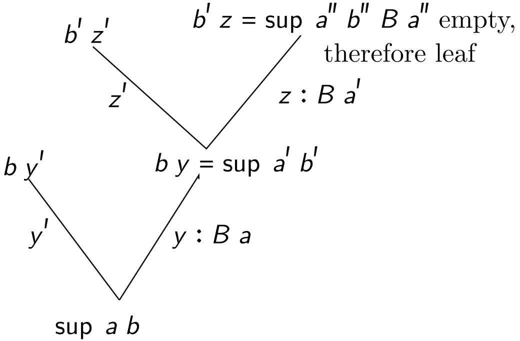
$$\mathrm{elim}_{\mathbb{N}}\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ 0 = \mathit{step}_0 : C\ 0$$

$$\begin{aligned}&\mathrm{elim}_{\mathbb{N}}\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ (\mathrm{S}\ n)\\ &\quad = \mathit{step}_{\mathrm{S}}\ n\ (\mathrm{elim}_{\mathbb{N}}\ \mathit{step}_0\ \mathit{step}_{\mathrm{S}}\ n) : C\ (\mathrm{S}\ n)\end{aligned}$$

Visualisation ($\mathbb{N}$)



W-Type



Assume $A : \mathrm{Set}$, $a : A \to' B \ a : \mathrm{Set}$.

$\mathrm{W}(A, B)$ is the type of well-founded recursive trees with branching degrees $(B \ a)_{a:A}$.

The W-Type

- **Formation rule:**

$$\frac{B : A \to \mathrm{Set}}{\mathrm{W}\ A\ B : \mathrm{Set}}$$

- **Introduction rule:**

$$\frac{a : A \qquad b : (x : B\ a) \to' \mathrm{W}\ A\ B}{\mathsf{sup}\ \ a\ b : \mathrm{W}\ A\ B}$$

The W-Type

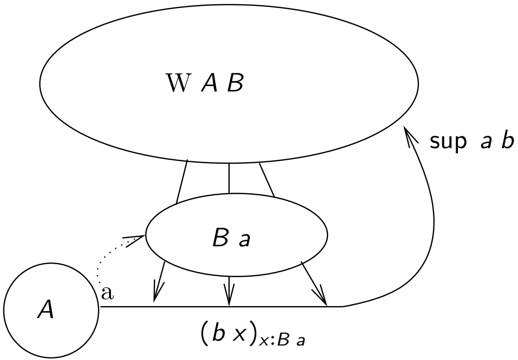
- **Elimination rule:**

$$\frac{\begin{array}{l} C : \mathrm{W}\ A\ B \to \mathrm{Set} \\ step : (a : A) \\ \qquad \to (b : B\ a \to' \mathrm{W}\ A\ B) \\ \qquad \to (ih : \Pi\ (B\ a)\ ((x)(C\ (b\ x)))) \\ \qquad \to C\ (\mathsf{sup}\ \ a\ b) \\ c : \mathrm{W}\ A\ B \end{array}}{\mathrm{elim}_{\mathrm{W}}\ step\ c : C\ c}$$

- **Equality rule:**

$$\begin{array}{l} \mathrm{elim}_{\mathrm{W}}\ step\ (\mathsf{sup}\ \ a\ b) \\ \qquad = step\ a\ b\ (\lambda x.\mathrm{elim}_{\mathrm{W}}\ step\ (b\ x)) : C\ (\mathsf{sup}\ \ a\ b) \end{array}$$

Visualisation ($\mathrm{W}\ A\ B$)



sup has two arguments

- Second argument is indexed over $B\ a$.
- $(B\ a)$ depends on the first argument a.

Universes

- A universe is a family of sets
- Given by
  - an set $\mathrm{U} : \mathrm{Set}$ of **codes** for sets,
  - a **decoding function** $\mathrm{T} : \mathrm{U} \to \mathrm{Set}$.

Universes

- **Formation rules:**

$$\mathrm{U} : \mathrm{Set} \qquad \mathrm{T} : \mathrm{U} \to \mathrm{Set}$$

- **Introduction and Equality rules:**

$$\widehat{\mathbb{N}} : \mathrm{U} \qquad \mathrm{T}\ \widehat{\mathbb{N}} = \mathbb{N}$$

$$\frac{a : \mathrm{U} \qquad b : \mathrm{T}\ a \to \mathrm{U}}{\widehat{\Sigma}\ a\ b : \mathrm{U}}$$

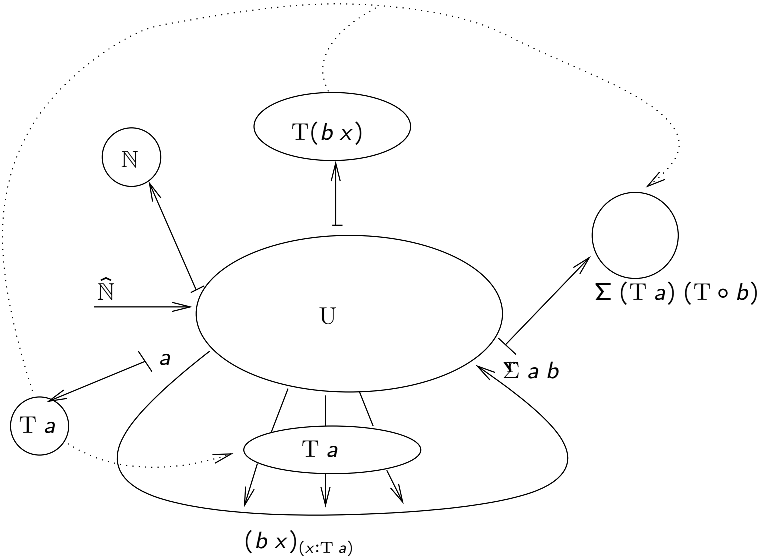
$$\mathrm{T}(\widehat{\Sigma}\ a\ b) = \Sigma\ (\mathrm{T}\ a)\ ((x)(\mathrm{T}\ (b\ x)))$$

Similarly for other type-formers (except for U).

Elimination Rules for U

- Elimination rule for U can be defined.
- Not very useful (e.g. one cannot define an embedding of U into itself using elimination rules).

Visualisation (U)



Analysis

- Elements of U are defined **inductively**, while defining $(\mathrm{T}\ a)$ for $a : \mathrm{U}$ **recursively**.
- Index set $(\mathrm{T}\ a)$ for second argument of Σ depends on the T applied to its first argument a.
- $\mathrm{T}(\Sigma\ a\ b)$ is defined from
  - $(\mathrm{T}\ a)$,
  - $(\mathrm{T}\ (b\ x))_{(x:\mathrm{T}\ a)}$.
- Principles for defining a universe can be generalised to **higher type universes**, where $(\mathrm{T}\ a)$ can be an element of any type, e.g. $\mathrm{Set} \to \mathrm{Set}$.

Literature for this Part

- Main article by the author [15] extracted from his PhD thesis [14].
- Overview article by the author [18]
- Ordinal notation system by Buchholz: [3].
- Method of distinguished sets: book by Buchholz and Schütte [5].

Kurt Schütte


[9]

[9] https://upload.wikimedia.org/wikipedia/commons/b/b5/Kurt_Schuette.jpg

Wilfried Buchholz


[10]

[10] https://opc.mfo.de/photoNormal?id=14841

Main Approach

- Typically
  - for axiomatic (usually classical) theories the upper bound is more important
    (how to harness the power of an axiom system?).
  - for foundational (usually constructive) theories the lower bound is more important
    (how to prove that the theory reaches that strength).
- Lower bound obtained by carrying a direct well-ordering proof in MLTT.

Ordinal Notation System with one Inaccessible

- Let $\#$ be the natural sum on ordinals.
- $\Omega_0 := 0$, $\Omega_\sigma := \aleph_\sigma$ for $\sigma > 0$.
- $\mathrm{I} := \min\{\sigma \mid \sigma \text{ regular Cardinal } \wedge \Omega_\sigma = \sigma\}$, the first weakly inaccessible cardinal.
- $\mathrm{I}^+ := \sup\{\zeta_n \mid n < \omega\}$, where $\zeta_0 := \Omega_{\mathrm{I}+1}$, $\zeta_{n+1} := \Omega_{\zeta_n}$,
- $\mathrm{Ord} := \{\alpha \mid \alpha \text{ ordinal }, \alpha < \mathrm{I}^+\}$,
- $\mathrm{R} := \{\sigma \in \mathrm{Ord} \mid \omega < \sigma \wedge \sigma \text{ regular }\} = \{\mathrm{I}\} \cup \{\Omega_{\sigma+1} \mid \sigma < \mathrm{I}^+\}$.

Remark: Cardinals can be replaced by their recursive analogue, admissibles – you just need to invest more work.

Ordinal Notation System with one Inaccessible

- By transfinite recursion on α, we define simultaneously for all κ ordinals $\psi_\kappa\alpha$ ($\kappa \in \mathrm{R}$) and sets $\mathrm{C}(\alpha,\beta) \subseteq \mathrm{Ord}$ as follows:

$$\psi_\kappa\alpha := \min\{\beta \mid \kappa \in \mathrm{C}(\alpha,\beta) \wedge \mathrm{C}(\alpha,\beta) \cap \kappa \subseteq \beta\} \ ,$$

$$\mathrm{C}(\alpha,\beta) := \left\{ \begin{array}{l} \text{the closure of } \beta \cup \{0, \mathrm{I}\} \text{ under the functions} \\ +,\ \varphi,\ \sigma \mapsto \Omega_\sigma,\ (\pi,\xi) \mapsto \psi_\pi\xi\ (\pi \in \mathrm{R}, \xi < \alpha) \end{array} \right. \quad .$$

- We define $\psi_\kappa : \mathrm{Ord} \longrightarrow \mathrm{Ord}$, $\psi_\kappa(\alpha) := \psi_\kappa\alpha$.
  $\mathrm{C}_\kappa(\alpha) := \mathrm{C}(\alpha, \psi_\kappa\alpha)$.

Structure of the Ordinal Operations

- We have the following operations for generating ordinals $< \mathrm{I}^+$:
  - Constants 0, I.
  - Operations +, ϕ, $\lambda\alpha.\Omega_\alpha$.
  - $(\pi, \xi) \mapsto \psi_\pi \xi$, where $\pi \in \mathrm{R}$.
- Regular ordinals are $\Omega_{\alpha+1}$ and I.
- $\lambda\xi.\psi_{\Omega_{\alpha+1}}\xi$ generates ordinals in $[\Omega_\alpha, \Omega_{\alpha+1}]$.
- $\lambda\xi.\psi_{\mathrm{I}}\xi$ generates non-regular fixed points of $\lambda\alpha.\Omega_\alpha$ between 0 and I.

Remark: Use of the Veblen function φ can be avoided (take $\lambda\alpha.\omega^\alpha$ instead).

Ordinal Notation System

- Using standard machinery we can now form an ordinal notation system OT denoting certain ordinals up to I^{+}.
- Problems to overcome:
  Add ordinals only if they are in normal form.

Ordinals up to Ω_1

0
$1 = \varphi_0 0 = 1$
$2 = 1 + 1$
$\cdots$
$\omega = \varphi_0 1$
$\cdots$
$\epsilon_0 = \varphi_1 0$
$\cdots$
$\Gamma_0 = \psi_{\Omega_1} 0$ first fixed point of $\lambda\alpha\varphi_\alpha 0$
$\cdots$
$\psi_{\Omega_1} 1$ 2nd fixed point of $\lambda\alpha\varphi_\alpha 0$
$\cdots$
$\psi_{\Omega_1} \alpha$ α can be $> \Omega_1$
$\cdots$
Ω_1

Ordinals up to Ω_{Ω_1}

Ω_1

$\cdots$

$\psi_{\Omega_2}\alpha$

$\cdots$

Ω_2

$\cdots$

$\psi_{\Omega_3}\alpha$

$\cdots$

Ω_3

$\cdots$

Ω_ω non regular

$\cdots$

Ω_{Ω_1} non regular

Ordinals up to $\psi_{\mathrm{I}}1$

Ω_{Ω_1} non regular

$\cdots$

$\psi_{\Omega_{\Omega_1+1}}\alpha$

$\cdots$

Ω_{Ω_1+1}

$\cdots$

$\Omega_{\Omega_{\Omega_1}}$ non regular

$\cdots$

$\psi_{\mathrm{I}}0$ first (non-regular) fixed point > 0 of $\lambda\alpha.\Omega_\alpha$

$\cdots$

$\psi_{\Omega_{\psi_{\mathrm{I}}0+1}}\alpha$

$\cdots$

$\Omega_{\psi_{\mathrm{I}}0+1}$

$\cdots$

$\psi_{\mathrm{I}}1$

Ordinals up to $\Omega_{\mathrm{I}+\omega}$

$\psi_{\mathrm{I}}1$

$\cdots$

$\psi_{\mathrm{I}}\alpha$

$\cdots$

I

$\cdots$

$\Omega_{\mathrm{I}+1}$

$\cdots$

$\Omega_{\mathrm{I}+\omega}$ $\quad$ ($\psi_{\Omega_1}(\Omega_{\mathrm{I}+\omega}) =$ strength of MLTT)

Method of Distinguished Sets (Buchholz) Step 1

- For $X \subseteq \mathrm{OT}$ let $\mathrm{Acc}(X)$ the largest well ordered segment of X.
  - Can be defined inductively by

$$(\alpha \in \mathrm{OT} \wedge \forall\, \beta < \alpha \in \mathrm{OT}) \to \alpha \in \mathrm{OT}$$

- For analysing a small impredicative theory such as ID_1 or MLTT with only one unnested W-type and a microcosmic universe (precise strength of the latter needs to be worked out) we can form

$$\mathrm{W}_0 := \mathrm{Acc}(\mathrm{OT} \cap [0, \Omega_1[)$$

Method of Distinguished Sets (Buchholz) Step 1

$$\mathrm{W}_0 := \mathrm{Acc}(\mathrm{OT} \cap [0, \Omega_1[)$$

- W_0 is well-ordered
- We can show W_0 is closed under the basic operations 0, +, φ.
- For showing closure under collapsing function we need to add ordinals above Ω_1 to it.
- In case of ID_1 we could add Ω_1 and Cantor normal forms with basis ω and obtain W_0^+.
- Using Gentzen's trick we can show that any proper initial segment of W_0^+ is well-ordered (this can be done in ID_1 or MLTT with one unnested W-type).
- Now we show that

$$(\alpha \in \mathrm{W}_0^+ \wedge \mathrm{NF}(\psi_{\Omega_1}\alpha)) \Rightarrow \psi_{\Omega_1}\alpha \in \mathrm{W}_0$$

Method of Distinguished Sets (Buchholz) Step 1

- By
$$\omega^{\cdot^{\cdot^{\cdot^{\omega^{\Omega_1+1}}}}} \in \mathrm{W}_0^+$$
it follows
$$\alpha_n := \psi_{\Omega_1}(\omega^{\cdot^{\cdot^{\cdot^{\omega^{\Omega_1+1}}}}}) \in \mathrm{W}_0$$
and therefore
$$\mathrm{ID}_1 \vdash \mathrm{TI}(\alpha_n)$$
$$\mathrm{ID}_1 \vdash \mathrm{TI}_{<\psi_{\Omega_1}(\epsilon_{\Omega_1+1})}$$

Method of Distinguished Sets (Buchholz) Step 2

- For analysing two inductive definitions or MLTT with up to twice nested W-type We can form W_0 as before and next

$$\mathrm{W}_1' = \mathrm{Acc}(\{\alpha \in \mathrm{OT} \cap [\Omega_1, \Omega_2[\mid \mathrm{K}_{\Omega_1}(\alpha) \subseteq \mathrm{W}_0\}$$

- $\mathrm{W}_1 := \mathrm{W}_0 \cup \mathrm{W}_1'$ is well-ordered.
- Let W_1^+ be formed from W_1 using Ω_2, Cantor normal form.
- In ID_2 one can show
  - Using Gentzen-trick that initial segments of W_1^+ are well-ordered.
  - W_1^+ is closed under 0, Ω_1, Ω_2, +, $\varphi\restriction_{\Omega_2}$, CNF, ψ_{Ω_1}, ψ_{Ω_2}.
  - Therefore

$$\alpha_n := \psi_{\Omega_1}(\omega^{\cdot^{\cdot^{\cdot^{\omega^{\Omega_2+1}}}}}) \in \mathrm{W}_1 \cap \Omega_1 = \mathrm{W}_0$$

    and therefore
    $\mathrm{TI}(\alpha_n)$ provable in ID_1.
  - Therefore $\mathrm{ID}_2 \vdash \mathrm{TI}_{<\psi_{\Omega_1}(\epsilon_{\Omega_2+1})}$.

Method of Distinguished Sets (Buchholz) Step 3

- In order to obtain well-ordering proofs for stronger ordinal notation systems Buchholz introduced the notion of distinguished sets.
- Distinguished sets are sets which are formed by generalising the way $\mathrm{W}_0, \mathrm{W}_1$ and obvious extensions are formed.
- So if A is distinguished we need that

$$A \cap [\Omega_\alpha, \Omega_{\alpha+1}[$$

  is the accessible part of the ordinals which have components $< \Omega_\alpha$ in A.
    - But only provided A has reached that far.
    - W_0 should be distinguished, even though it doesn't contain e.g. Ω_1.
- However, the cardinals Ω_α need to be well-ordered as well.

$\mathrm{C}^a(A)$

We define for $A \subseteq \mathrm{OT}$ the set of ordinals $\mathrm{C}^a(A) \subseteq \mathrm{OT}$ formed from ordinals in $A \cap a$:

- $0, \mathrm{I} \in \mathrm{C}^a(A)$.
- $((d =_{\mathrm{NF}} \varphi_b c \lor d =_{\mathrm{NF}}' b + c \lor (d =_{\mathrm{NF}} \Omega_b \land b = c)))$
  $\Rightarrow (d \in \mathrm{C}^a(A) \Leftrightarrow (d \in A \cap a \lor \{b, c\} \subseteq \mathrm{C}^a(A)))$.
- Assume $d =_{\mathrm{NF}} \psi_\kappa c$.
  If $a < \kappa$, then $d \in \mathrm{C}^a(A) \Leftrightarrow (d \in A \cap a \lor \{\kappa, c\} \subseteq \mathrm{C}^a(A))$.
  If $\kappa \leq a$, then $d \in \mathrm{C}^a(A) \Leftrightarrow d \in A \cap a$.

$\mathrm{M}(A)$, $\tau^A(a)$, $\mathrm{W}(A)$, $\mathrm{D}(A)$

- $\tau^A(a) := \mathrm{C}^a(A) \cap a$.
- $\mathrm{M}(A) := \{y \in \mathrm{OT} \mid y \in \mathrm{C}^y(A)\}$.
- $\mathrm{W}(A) := \bigcap\{Y \subseteq \mathrm{OT} \mid \forall\, x \in \mathrm{M}(A).\tau^A(x) \subseteq Y \to x \in Y\}$.
- $\mathrm{D}(A) := A \subseteq \mathrm{OT} \land A \sqsubseteq \mathrm{W}(A)$.
  $\mathrm{D}(A)$ means "A is a distinguished set". [11]
- $\mathcal{W} = \bigcup\{A \subseteq \mathrm{OT} \mid \mathrm{D}(A)\}$ which is a class.

[11] In [15] we used $\mathrm{Ag}(A)$ for $\mathrm{D}(A)$ using the German word "ausgezeichnete Menge" for distinguished set.

Properties

- If $\mathrm{D}(A)$ then A is well-ordered.
- If $\mathrm{D}(A)$ then $A \cap \Omega_1 \sqsubseteq \mathrm{OT}$.
- If $\mathrm{D}(A)$ then A is closed under $0, +, \varphi, \lambda x.\Omega_x, \psi$ bounded by A, provided the result is in NF.
- Distinguished sets are segments of each other, constructively expressed as
  If $\mathrm{D}(A)$, $\mathrm{D}(B)$, $b \leq A$, $b \leq B$, then $A \cap b = B \cap b$.
- $\mathrm{D}(\mathcal{W})$.
- $x \in \mathcal{W} \cap \mathrm{I} \to \Omega_x \in \mathcal{W}$.

Classes above $\mathcal{W}$

Define

- $\mathcal{W}_0 := \mathcal{W} \cap \mathrm{I}$.
- $\mathcal{W}_{i+1} := \mathrm{W}(\mathcal{W}_i) \cap \Omega_{I+i+1}$.

We have

- $\mathrm{D}(\mathcal{W}_i)$.
- $\mathcal{W}_i$ closed under $\lambda\alpha.\psi_I\alpha$ provided in NF.
- $\Omega_{I+i} \in \mathcal{W}_i$.
- $\psi_{\Omega_1}(\Omega_{\mathrm{I}+i}) \in \mathcal{W}_0$.
- $\mathrm{TI}(\psi_{\Omega_1}(\Omega_{\mathrm{I}+i}))$.
- $\mathrm{TI}_{<\psi_{\Omega_{\mathrm{I}+\omega}}}$.

Definition in MLTT

- $\mathrm{W}(A)$ can be defined using W-type:
  Take the trees in
  $$\mathrm{W} A' B$$
  with
  $$\begin{array}{lcl} A' & = & \Sigma x : \mathbb{N}. x \in OT \wedge x \in \mathrm{M}(A) \\ B\ (\mathrm{p}\ x\ y) & = & \Sigma y : \mathbb{N}. y \in \mathrm{OT} \wedge y \in \tau^{A}(x) \end{array}$$
- $\mathrm{label}(w) = a$ if $w = \mathrm{sup}(\langle a, x \rangle, f)$ for some x, f.
- $x \in \mathrm{W}(A)$ iff
  $x \in \mathrm{OT}$
  and there exists $w \in \mathrm{W}\ A'\ B$ s.t.
  $\mathrm{label}(w) = a$
  and the $\langle b, c \rangle$th subnode of any subtree w' has label b.
- Let the powerset of $\mathbb{N}$ be $\mathbb{N} \to \mathrm{U}$.

Definition in MLTT

- Now you can define $\mathcal{W}$ as

$$x \in \mathcal{W} := \Sigma X : \mathbb{N} \to \mathrm{U}.\mathrm{D}(X) \wedge \mathrm{T}(X\ x)$$

.

- $\mathcal{W}_i$ can now be defined using nested W on top of U.

Theorem (Lower Bound of $|MLTT|$)

Theorem

Let MLTT *be MLTT with* W*-type and one universe. Then*

$$|\mathrm{MLTT}| \geq \psi_{\Omega_1}(\Omega_{\mathrm{I}+\omega})$$

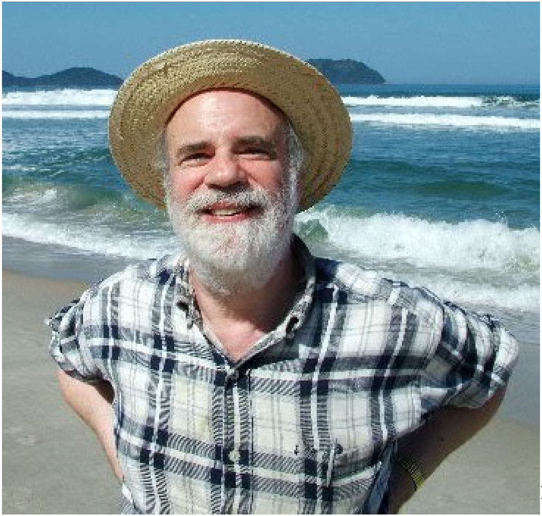
Main Approach

- Upper bound obtained by modelling MLTT in an extension of Kripke-Platek Set Theory.

Kripke-Platek Set Theory ($\mathrm{KP}\omega$)

- $\mathrm{KP}\omega$ is a restricted version of set theory, developed originally in order to formulate recursion theory.
- ω stands for the addition of the natural numbers.
- Standard presentation is the book by Barwise [1].
- The Schütte school, especially Gerhard Jäger [11] developed it into a system for developing reference systems of different proof theoretic strength.

Saul Kripke

[12]

[12] https://upload.wikimedia.org/wikipedia/commons/d/d4/Kripke.JPG

Gerhard Jäger

 13

13 http://www.inf.unibe.ch/e58700/e58702/e203661/e771254/jaeger_eng.jpg

Kripke-Platek Set Theory ($\mathrm{KP}\omega$)

- Language consists of $\in$ and a predicate Ad.
  - Ad was added by Jäger in order to develop extensions of $\mathrm{KP}\omega$ of different proof theoretic strength.
  - $\mathrm{Ad}(a)$ means that a is an admissible containing ω, i.e. a transitive inner model of $\mathrm{KP}\omega$.
  - Admissible ordinals

$$\bigcup\{\alpha \mid \mathrm{Ord}(\alpha) \land \alpha \in a\}$$

    for an admissible a are the recursive analogues of cardinals.
  - For instance the smallest admissible ordinal $> \omega$ is the height of Kleene's O, which is as well the height of

$$\mathrm{W}\ \{0, 1, \widehat{\mathbb{N}}\}\ B$$

where

$$\begin{array}{lcl} B\ 0 & = & \emptyset \\ B\ 1 & = & \{*\} \text{ the set containing one element} \\ B\ \widehat{\mathbb{N}} & = & \mathbb{N} \end{array}$$

Abbreviations

$\mathrm{trans}(u) :\equiv \forall\, x \in u.\, \forall\, y \in x. y \in u,$
$\mathrm{infinite}(u) :\equiv \exists\, x \in u.(x = x) \wedge \forall\, x \in u.\, \exists\, y \in u. x \in y.$
$\mathrm{Inacc}(x) :\equiv \mathrm{Ad}(x) \wedge \forall\, y \in x.\, \exists\, z \in x. y \in z \wedge \mathrm{Ad}(z).$

$$
\begin{aligned}
\mathrm{Inacc}_n(x) :\equiv \exists\, x_0, \ldots, x_n.\ & \\
& \mathrm{Inacc}(x_0) \\
& \wedge \mathrm{Ad}(x_1) \wedge \mathrm{Ad}(x_2) \wedge \cdots \wedge \mathrm{Ad}(x_n) \\
& \wedge x_0 \in x_1 \wedge x_1 \in x_2 \wedge \cdots \wedge x_{n-1} \in x_n \wedge x = x_n .
\end{aligned}
$$

ψ a formula, then ψ^u means the replacing of every unbounded quantifier $\forall\, v$ by $\forall\, v \in u$ and $\exists\, v$ by $\exists\, v \in u$.
$\mathrm{Inacc}(x)$ expresses, that x is an admissible, closed under admissibles, the ordinal of which is an inaccessible.
$\mathrm{Inacc}_n(x)$ expresses that x is an admissible, which is at least the nth admissible above an x s.t. $\mathrm{Inacc}(x)$.

Axioms of $\mathrm{KP}\omega$

$$
\begin{array}{ll}
(\mathrm{Ext}) & \forall x.\forall y.\forall z.x = y \to (x \in z \to y \in z) \\
 & \qquad\qquad \wedge\ (\mathrm{Ad}(x) \to \mathrm{Ad}(y)) \\
(\mathrm{Found}) & \forall \vec{z}.[\forall x.(\forall y \in x.\phi(y,\vec{z}) \to \phi(x,\vec{z})) \to \forall x.\phi(x,\vec{z})] \\
 & \quad (\phi \text{ an arbitrary formula }) \\
(\mathrm{Pair}) & \forall x.\forall y.\exists z.x \in z \wedge y \in z. \\
(\bigcup) & \forall x.\exists z.\forall y \in x.\forall u \in y.u \in z. \\
(\Delta_0 - \mathrm{sep}) & \forall \vec{z}.\forall w.\exists y.[(\forall x \in y.(x \in w \wedge \phi(x,\vec{z}))) \\
 & \qquad \wedge\ \forall x \in w.\phi(x,\vec{z}) \to x \in y] \\
 & \quad (\phi \text{ a } \Delta_0\text{-formula}). \\
(\Delta_0 - \mathrm{coll}) & \forall \vec{z}.\forall w.[(\forall x \in w.\exists y.\phi(x,y,\vec{z})) \\
 & \qquad \to \exists w'.\forall x \in w.\exists y \in w'.\phi(x,y,\vec{z})] \\
 & \quad (\phi \text{ a } \Delta_0\text{-formula }).
\end{array}
$$

Axioms for Ad

$$(\mathrm{Ad}.1)\forall x.\mathrm{Ad}(x) \to \mathrm{trans}(x) \wedge \exists w \in x.\mathrm{infinite}(w).$$
$$(\mathrm{Ad}.2)\forall x. \forall y.\mathrm{Ad}(x) \wedge \mathrm{Ad}(y) \to x \in y \vee x = y \vee y \in x.$$
$$(\mathrm{Ad}.3)\forall x.\mathrm{Ad}(x) \to \psi^x,$$
$$(\psi \text{ an instance of } (\mathrm{Pair}), (\bigcup), (\Delta_0 - \mathrm{sep}), (\Delta_0 - \mathrm{coll})).$$

Axioms for KPI^{+}

The strength of MLTT with W-type and one universe will be $|\mathrm{KPI}^{+}|$, which is given by adding

(Lim) $\forall x. \exists y. \mathrm{Ad}(y) \land x \in y$.
(inf) $\exists x. \mathrm{infinite}(x)$.
($+_n$) $\exists x. \mathrm{Inacc}_n(x)$.

Main Idea

- Define a set $\mathrm{Term}_{\mathrm{Cl}}$ of closed terms and $[\![\, \mathrm{Set} \,]\!]$ of closed types, which are expressions formed from term and type constructors without any type checking.
- We will identify α-equivalent terms.
- For $A \in [\![\, \mathrm{Set} \,]\!]$ we define an interpretation

$$[\![\, A \,]\!] \subset \mathrm{Term} \times \mathrm{Term}$$

  and an ordinal $\mathrm{o}(A)$
- $\langle r, s \rangle \in [\![\, A \,]\!]$ means that r and s are equal elements of type A.
- Furthermore we demand $[\![\, A \,]\!] \in \mathrm{L}_{\mathrm{o}(A)}$.

Main Idea

- We will show:
  - $\mathrm{MLTT} \vdash \Gamma \Rightarrow A : \mathrm{Set}) \Rightarrow$
    $\mathrm{KPI}^{+} \vdash \forall(\rho, \rho') \in [\![\, \Gamma \,]\!].\mathrm{PER}([\![\, A\rho \,]\!]) \wedge [\![\, A\rho \,]\!] = [\![\, A\rho' \,]\!]$.
  - $\mathrm{MLTT} \vdash \Gamma \Rightarrow A = A' : \mathrm{Set}) \Rightarrow$
    $\mathrm{KPI}^{+} \vdash \forall(\rho, \rho') \in [\![\, \Gamma \,]\!].\mathrm{PER}([\![\, A\rho \,]\!]) \wedge [\![\, A\rho \,]\!] = [\![\, A'\rho' \,]\!]$.
  - $\mathrm{MLTT}(\vdash \Gamma \Rightarrow r \in A) \Rightarrow$
    $\mathrm{KPI}^{+} \vdash \forall\langle\rho, \rho'\rangle \in [\![\, \Gamma \,]\!].\langle [\![\, r\rho \,]\!], [\![\, r\rho \,]\!]\rangle \in [\![\, A\rho \,]\!]$.
  - $\mathrm{MLTT}(\vdash \Gamma \Rightarrow r = r' \in A) \Rightarrow$
    $\mathrm{KPI}^{+} \vdash \forall\langle\rho, \rho'\rangle \in [\![\, \Gamma \,]\!].\langle [\![\, r\rho \,]\!], [\![\, r' \,]\!]\rho\rangle \in [\![\, A\rho \,]\!]$.
  - If $\mathrm{MLTT} \vdash \Gamma \Rightarrow \theta$
    the above statements hold as well for all presuppositions of $\Gamma \Rightarrow \theta$.
- Here $\mathrm{PER}(X)$ means that X is a partial equivalence relation on terms (i.e. transitive and symmetric)
  upward and downward closed under $\longrightarrow$, i.e.
  $(\langle r, r'\rangle \in X \wedge (s \longrightarrow r \vee r \longrightarrow s) \wedge (s' \longrightarrow r' \vee r' \longrightarrow s'))$.
  $\Rightarrow \langle s.s'\rangle \in X$

Basic Definitions

- $\mathrm{Clos}(X) := \{\langle s, s' \rangle \mid \langle r, r' \rangle \in X \wedge (s \longrightarrow r \vee r \longrightarrow s) \wedge (s' \longrightarrow r' \vee r' \longrightarrow s')\}$.
- $\mathrm{Flat}(X) := \{r \mid \exists\, s.\langle r, s \rangle \in X \vee \langle s, r \rangle \in X\}$.
- We will always define $[\![A\rho]\!] := \mathrm{Clos}([\![A\rho]\!]^{\mathrm{bas}})$, where $[\![A\rho]\!]^{\mathrm{bas}}$ are the set of basic elements of A.

Examples

- $[\![\, \mathbb{B} \,]\!]^{\mathrm{bas}} := \{\langle \mathrm{tt}, \mathrm{tt}\rangle, \langle \mathrm{ff}, \mathrm{ff}\rangle\}$
  $\mathrm{o}(\mathbb{B}) := 3.$
- $[\![\, \varnothing \,]\!]^{\mathrm{bas}} := \varnothing.$
  $\mathrm{o}(\varnothing) := 3.$
- $$[\![\, A+B \,]\!]^{\mathrm{bas}} := \{\langle \mathrm{inl}\ r, \mathrm{inl}\ r'\rangle \mid \langle r, r'\rangle \in [\![\, A \,]\!]\} \cup \{\langle \mathrm{inl}\ s, \mathrm{inl}\ s'\rangle \mid \langle s, s'\rangle \in [\![\, B \,]\!]\}$$
  $\mathrm{o}((A+B)) := \max\{\mathrm{o}(A), \mathrm{o}(B)\} + 2.$
- $[\![\, \Sigma\ A\ B \,]\!]^{\mathrm{bas}} :=$
  $\{\langle \mathrm{p}\ r\ s, \mathrm{p}\ r'\ s'\rangle \mid \langle r, r'\rangle \in [\![\, A \,]\!] \wedge \langle s, s'\rangle \in [\![\, B\ r \,]\!]\}$.
  $\mathrm{o}(\Sigma\ A\ B) := \max(\{\mathrm{o}(A)\} \cup \{\mathrm{o}(B\ s) \mid s \in \mathrm{Flat}([\![\, A \,]\!])\}) + 2$
- $[\![\, \Pi\ A\ B \,]\!]^{\mathrm{bas}} :=$
  $\{\langle \lambda x.t, \lambda x'.t'\rangle \mid \forall \langle r, r'\rangle \in [\![\, A \,]\!].\langle t[x := r], t'[x' := r']\rangle \in [\![\, B\ r \,]\!]\}$.
  $\mathrm{o}(\Pi\ A\ B) := \max(\{\mathrm{o}(A)\} \cup \{\mathrm{o}(B\ s) \mid s \in \mathrm{Flat}([\![\, A \,]\!])\}) + 2$

Interpretation of $\mathrm{W}\ A\ B$

- $[\![\ \mathrm{W}\ A\ B\ ]\!]$ is defined as the least set X such that

$$\mathrm{Clos}(X) \subseteq X$$

  and

$$(([\![\ r, r'\ ]\!] \in [\![\ A\ ]\!] \wedge [\![\ s, s'\ ]\!] \in [\![\ B\ s\ ]\!]\ [\![\ \rightarrow'\ ]\!]\ X) \\ \rightarrow \langle \mathrm{sup}\ \ r\ s, \mathrm{sup}\ \ r'\ s' \rangle \in X\ \ .$$

- This can be defined by iterating an operator up to

$$\alpha := (\max(\{\mathrm{o}(A)\} \cup \{\mathrm{o}(B\ s) \mid s \in \mathrm{Flat}([\![\ A\ ]\!])\}))^+$$

$$\mathrm{o}(\mathrm{W}\ A\ B) := \alpha + 1$$

Interpretation of U and $\mathrm{T}\ s$

- $[\![\, \mathrm{U} \,]\!]$ and $[\![\, \mathrm{T}\ s \,]\!]$ for s s.t. $s \in \mathrm{Flat}([\![\, \mathrm{U} \,]\!])$ are defining inductively the elements of $[\![\, U \,]\!]$ while recursively defining $[\![\, \mathrm{T}\ s \,]\!]$ for any $s \in \mathrm{Flat}([\![\, \mathrm{U} \,]\!])$
- This can be defined by iterating an operator defining X (approximating $[\![\, \mathrm{U} \,]\!]$) and Y (defining $\lambda x \in \mathrm{Flat}(X).[\![\, \mathrm{T}\ x \,]\!]$) up to a recursively admissible.
- This will be done in such a way that the αth iteration of the operator is in the $\mathrm{L}_{\kappa+3}$ for the αth admissible κ.

Examples Definition of $[\![\mathrm{U}]\!]$, $[\![\mathrm{T}\ s]\!]$

- $\langle \widehat{\mathbb{N}}, \widehat{\mathbb{N}} \rangle \in [\![\mathrm{U}]\!]$. $\mathrm{T}\ \widehat{\mathbb{N}} := [\![\mathbb{N}]\!]$.
- If
$$\langle r, r' \rangle \in [\![\mathrm{U}]\!]$$
and for
$$\langle s, s' \rangle \in [\![\mathrm{T}\ r]\!]\ [\![\to]\!]\ [\![U]\!]$$
then
$$\langle \widehat{\Sigma}\ r\ s, \widehat{\Sigma}\ r'\ s' \rangle \in [\![\mathrm{U}]\!]$$
and
$$[\![\mathrm{T}(\widehat{\Sigma}\ r\ s)]\!] := [\![\Sigma]\!]\ [\![\mathrm{T}\ a]\!]\ (\lambda x \in [\![\mathrm{T}\ a]\!].[\![\mathrm{T}\ (s\ x)]\!])$$
- Similarly for the other set constructions.

Examples Definition of $[[\, \mathrm{U} \,]]$, $[[\, \mathrm{T}\ s \,]]$

- In case of W this requires after the αth iteration an operator up to $\kappa + 1$, where κ is the αth admissible.
- So the closure ordinal for this construction is the first rec. inaccessible, $\mathrm{o}(\mathrm{U}) = \mathrm{I} + 1$ for the first rec. inaccessible I, $\mathrm{o}(\mathrm{T}\ r)$ is $\kappa + 1$ where κ is the αth admissible and α is minimal such that r occurs in the flatting of the αth iteration of the operator for defining U

Final Statement

- In order to interpret U we need one rec. inaccessible.
- In order to interpret $\mathrm{W}\ A\ B$ we need an admissible above the ordinals needed for interpreting A and B.
- So in total we need finite admissibles above the first rec. inaccessible.
  - For every statement $\Gamma \Rightarrow A : \mathrm{Set}$ we can find an n s.t. $\mathrm{o}(A\rho) \in \mathrm{L}_{\kappa+2}$ for the nth admissible κ above I.
  - Possible since we have elimination only into sets not into Set itself.

Final Statement

- The correctness statements mentioned above hold.
- By extending the above by adding non-recursive terms, we can show the preservation of the statement of Transfinite induction, for elements in $[\![\mathbb{N} \to \mathrm{U}]\!]$.
- If $\mathrm{MLTT} \vdash \mathrm{TI}(\alpha)$, then $\mathrm{KPI}^{+} \vdash \mathrm{TI}(\alpha)$ as well (restricted to elements in L_{I}.
- Therefore $|\mathrm{MLTT}| \leq |\mathrm{KPI}^{+}|$.

Theorem (Upper Bound of $|MLTT|$)

Theorem

Let MLTT *be MLTT with* W*-type and one universe. Then*

$$|\mathrm{MLTT}| \leq \psi_{\Omega_1}(\Omega_{\mathrm{I}+\omega})$$

Steps Towards Mahlo

- First step beyond standard universe
  - The super universe (Palmgren).
  - He introduced a universe V,
  - together with a universe operator $\mathrm{U} : \mathrm{Fam}(\mathrm{V}) \to \mathrm{V}$,
    - $\mathrm{Fam}(\mathrm{V})$ is the set of families of sets in V indexed over elements of V, roughly speaking

$$\{(B_x)_{x:B} | B : \mathrm{V}, \quad x : B \Rightarrow B_x : \mathrm{V}\}$$

  - s.t. for any family of sets A in V, $\mathrm{U}(A)$ is a universe containing all elements of A.

Steps Towards Mahlo

- A Universe is a family of sets closed under constructions for forming sets.
- We can now form a universe, closed under the formation of the next universe above a family of sets.
- (The next slide doesn't exhaust the strength, it shows only universes containing one set, not universes containing family of sets)

Illustration of the Super Universe

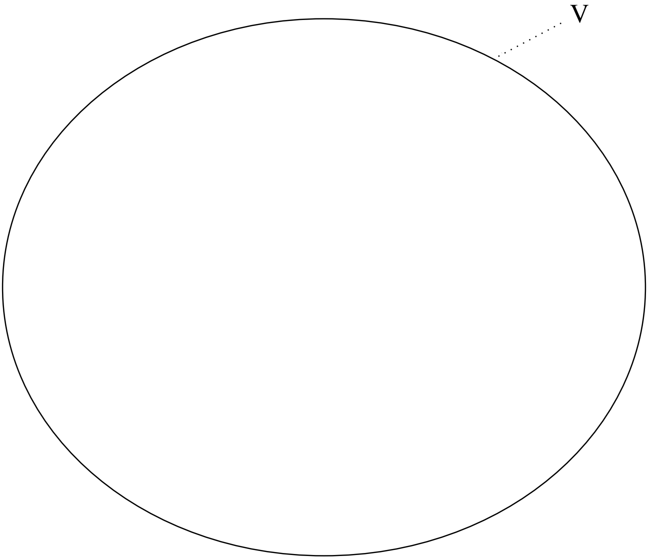


Illustration of the Super Universe

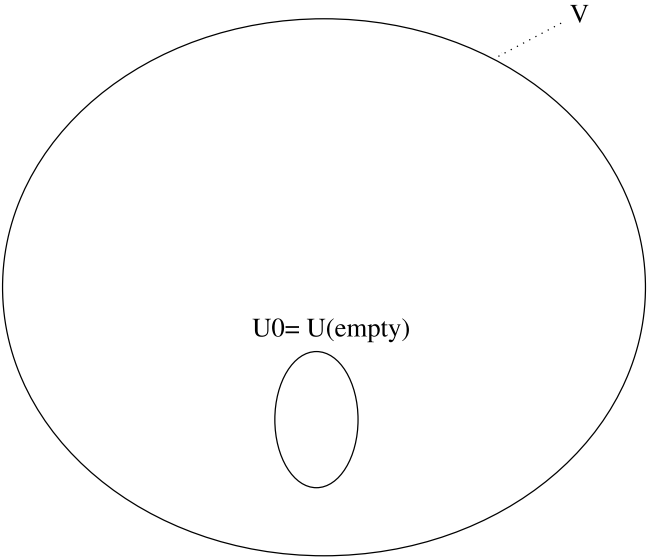


Illustration of the Super Universe

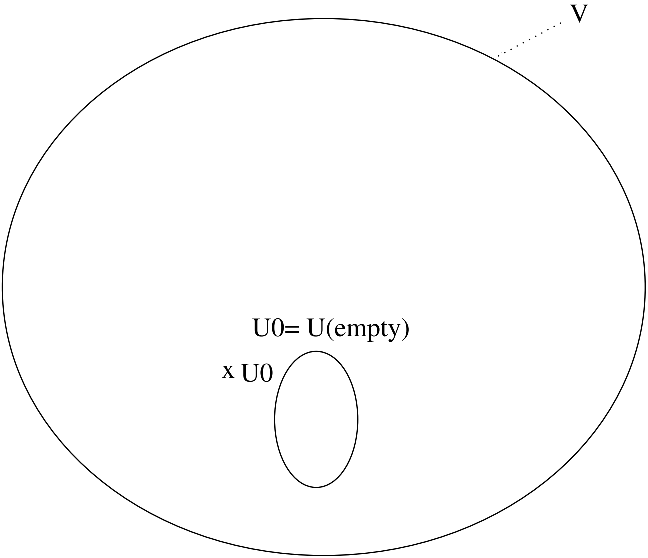


Illustration of the Super Universe

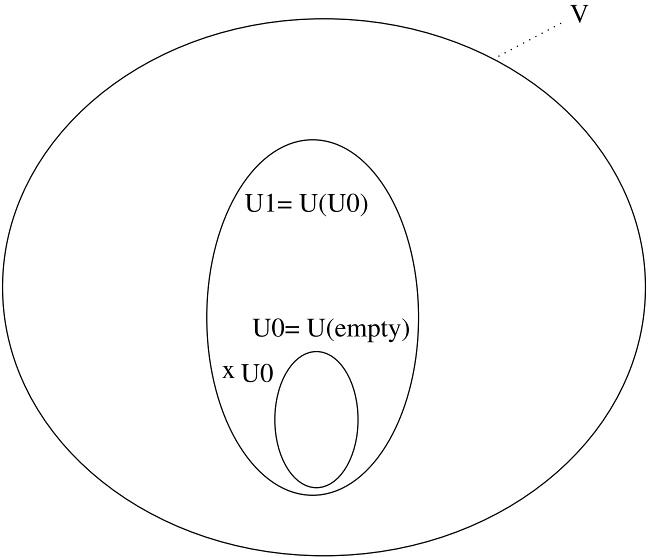


Illustration of the Super Universe

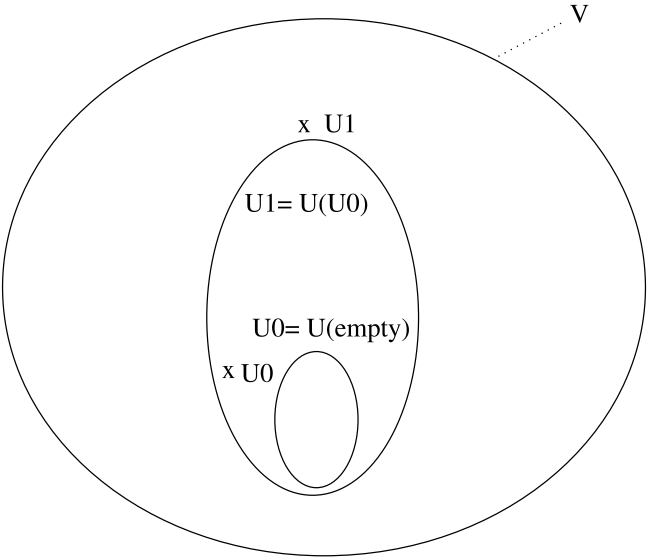


Illustration of the Super Universe

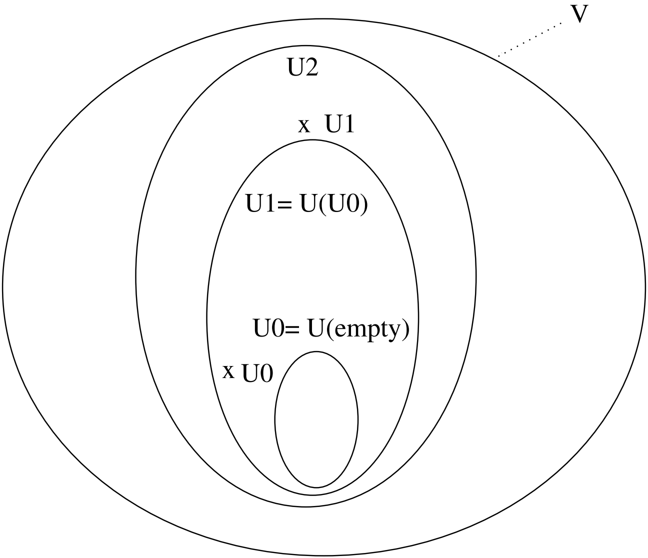
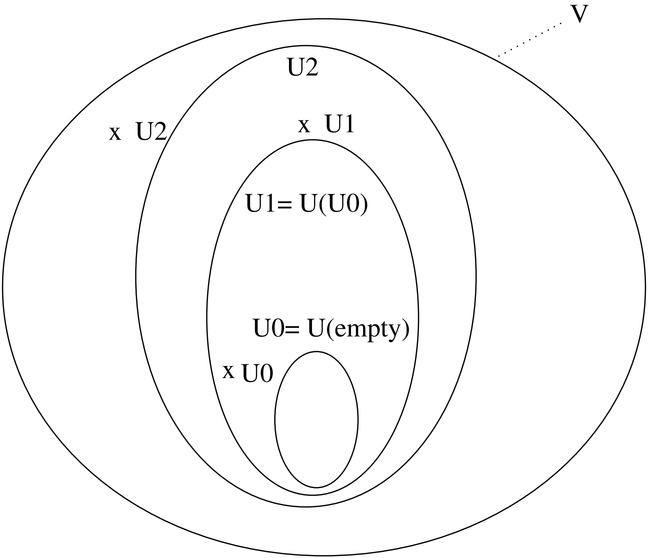


Illustration of the Super Universe



Super^n-Universes

- The above can be continued: We can form a
  - super^2-universe V,
  - closed under a super-universe operator, forming a super universe above a family of sets in V.
- And we can iterate the above n-many times, and even go beyond.
- Up to now everything was inductive-recursive

Mahlo Universe

- The Mahlo universe is
  - a universe $\underset{\sim}{\mathrm{V}}$,
  - which has not only subuniverses corresponding to some operators, but subuniverses corresponding to all operators it is closed under:
  - for every universe operator on V,
    - i.e. every $f : \mathrm{Fam}(\mathrm{V}) \to \mathrm{Fam}(\mathrm{V})$,
  - there exists a universe $\underset{\sim}{\mathrm{U}_f}$ closed under f.

Illustration of the Mahlo Universe

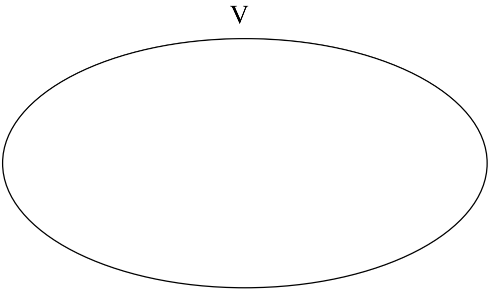


Illustration of the Mahlo Universe

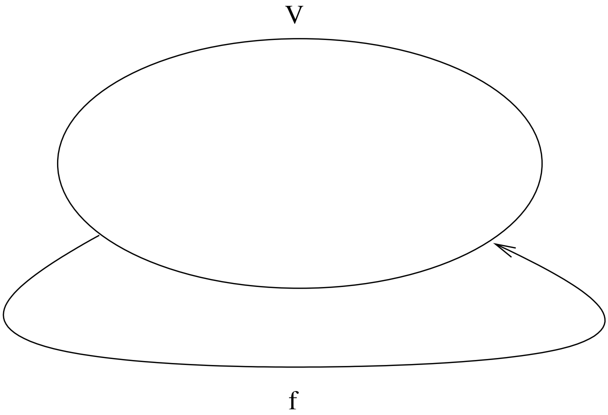


Illustration of the Mahlo Universe

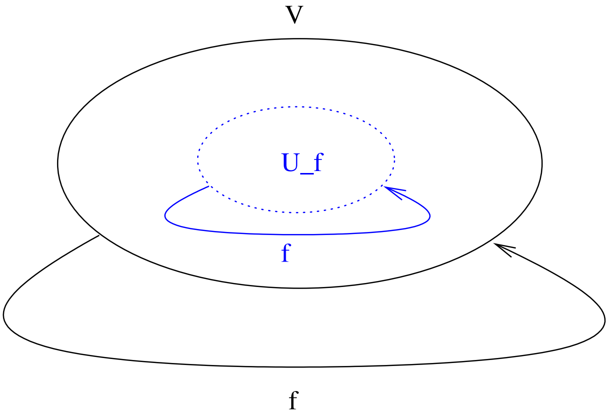
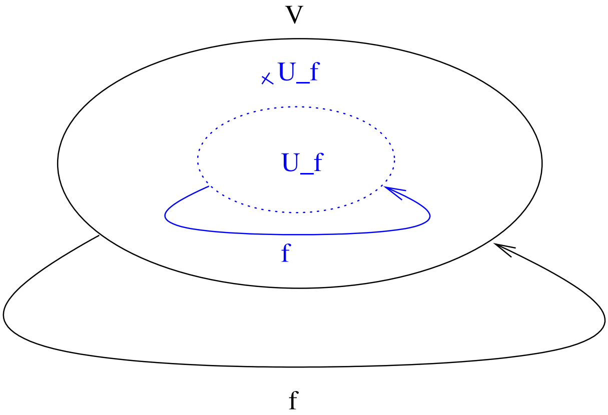


Illustration of the Mahlo Universe



Formulation of Mahlo Universe

$$
\begin{array}{l}
\mathrm{mutual} \\
\quad \mathrm{data}\ \mathrm{V} : \mathrm{Set}\ \mathrm{where} \\
\qquad \widehat{\Pi} \quad : \quad (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to \mathrm{V} \\
\qquad \cdots \\
\qquad \widehat{\mathrm{U}} \quad : \quad (f : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to \mathrm{V}) \\
\qquad\qquad\quad \to (g : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to (\mathrm{T_V}\ (f\ x\ y) \to \mathrm{V}) \to \mathrm{V}) \\
\qquad\qquad\quad \to \mathrm{V}
\end{array}
$$

$$
\begin{array}{lcl}
\mathrm{T_V} : \mathrm{V} \to \mathrm{Set} & & \\
\mathrm{T_V}\ (\widehat{\Pi}\ a\ b) & = & (x : \mathrm{T_V}\ a) \to \mathrm{T_V}\ (b\ x) \\
\cdots & & \\
\mathrm{T_V}\ (\widehat{\mathrm{U}}\ f\ g) & = & \mathrm{U}\ f\ g
\end{array}
$$

Mahlo Universe in Agda

$$
\begin{array}{l}
\mathrm{data}\ \mathrm{U}\ (f : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to \mathrm{V}) \\
\qquad\quad (g : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to (\mathrm{T_V}\ (f\ x\ y) \to \mathrm{V}) \to \mathrm{V}) \\
\qquad\quad : \mathrm{Set\ where} \\
\quad \widehat{\Pi} \quad : \quad (x : \mathrm{U}_{f,g}) \to (\mathrm{T}_{f,g}\ x \to \mathrm{U}_{f,g}) \to \mathrm{U}_{f,g} \\
\quad \cdots \\
\quad \widehat{\mathrm{f}} \quad : \quad (x : \mathrm{U}_{f,g}) \to (\mathrm{T}_{f,g}\ x \to \mathrm{U}_{f,g}) \to \mathrm{U}_{f,g} \\
\quad \widehat{\mathrm{g}} \quad : \quad (x : \mathrm{U}_{f,g}) \\
\qquad\qquad \to (y : \mathrm{T}_{f,g}\ x \to \mathrm{U}_{f,g}) \\
\qquad\qquad \to \mathrm{T_V}\ (f\ (\widehat{\mathrm{T}}_{f,g}\ x)\ (\widehat{\mathrm{T}}_{f,g} \circ y)) \\
\qquad\qquad \to \mathrm{U}_{f,g}
\end{array}
$$

Mahlo Universe in Agda

$$
\begin{array}{lcl}
\multicolumn{3}{l}{\widehat{\mathrm{T}}\ (f : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to \mathrm{V})} \\
\multicolumn{3}{l}{\quad (g : (x : \mathrm{V}) \to (\mathrm{T_V}\ x \to \mathrm{V}) \to (\mathrm{T_V}\ (f\ x\ y) \to \mathrm{V}) \to \mathrm{V})} \\
\multicolumn{3}{l}{\quad : \mathrm{U}_{f,g} \to \mathrm{V}} \\
\widehat{\mathrm{T}}_{f,g}\ (\widehat{\Pi}\ a\ b) & = & \widehat{\Pi}\ (\widehat{\mathrm{T}}_{f,g}\ a)\ (\widehat{\mathrm{T}}_{f,g} \circ b) \\
\cdots & & \\
\widehat{\mathrm{T}}_{f,g}\ (\widehat{\mathrm{f}}\ a\ b) & = & f\ (\widehat{\mathrm{T}}_{f,g}\ a)\ (\widehat{\mathrm{T}}_{f,g} \circ b) \\
\widehat{\mathrm{T}}_{f,g}\ (\widehat{\mathrm{g}}\ a\ b\ c) & = & g\ (\widehat{\mathrm{T}}_{f,g}\ a)\ (\widehat{\mathrm{T}}_{f,g} \circ b)\ c
\end{array}
$$

Buchholz' Finitary Derivations

- In [2, 4] gave an elegant and intuitive way of viewing Gentzen's cut elimination proof.
- Buchholz starts by introducing a notation system for proofs in Peano Arithmetic.
- Then he interprets each proof as an infinitary proof using the ω-rule.
- This means that for every proof term he can determine
  - the height of the tree measured by an ordinal (precisely element of an ordinal notation system of strength ϵ_0)
  - its cut degree,
  - the sequent it derives,
  - the last rule, which may have 0, 1, 2 or ω-many subderivations,
  - for each index of a subderivation a notation for the subderivation, which has smaller ordinal height.

Buchholz' Finitary Derivations (Cont.)

- Then Buchholz adds operators corresponding to the steps in the cut elimination.
- In order to be total without referring to the well-foundedness of the ordinal notation system, he has one special rule (**Rep** rule), which derives a sequence from itself.
- Again the above components can be derived, for the proof terms extended by the cut elimination operations.
- All the above can be done in PRA, primitive recursive arithmetic, which is considered as a formalisation of Hilbert's finitary methods.
- Buchholz uses it to extract programs from proofs.

Buchholz' Finitary Derivations (Cont.)

- For us more important here is what it says about consistency.
  - There is no cut-free rule deriving falsity, except for the Rep rule.
  - Therefore if you have a proof of falsity in PA, it must be derived by the Rep rule. The premise is a proof of the Rep rule with smaller ordinal height.
  - Everything is primitive recursive, so from a proof of falsity you get a primitive recursive infinite descending sequence of ordinal notations from an ordinal notation system of order type ϵ_0.
  - And this is provable in PRA.
- So in order to convince ourselves of the consistency of PA, all we need is to convince ourselves that there is no primitive recursive infinite descending sequence of ordinal notations in an ordinal notation system of strength ϵ_0.
- We will however in the arguments need to refer to that there is no infinite descending sequence of ordinals at al.

Intuitive Well-foundedness: $\mathbb{N}$, $A \uplus B$

- $(\mathbb{N}, <_{\mathbb{N}})$ is an ordinal notation system of order type ω.
  It is easy to see there is no infinite descending sequence of ordinals in $\mathbb{N}$:

$$\begin{array}{cccccc} 0 & n_0 & n_1 & n_2 & n_3 & \cdots \\ \end{array}$$

  if you go down you will eventually hit 0.
- If A and B are well founded so is the notation system $A \uplus B$

$$\begin{array}{cccccccccc} a_0 & a_1 & a_2 & a_3 & \cdots & b_0 & b_1 & b_2 & b_3 & \cdots \end{array}$$

Ordinal Notation System $A \uplus B$

- Formally, if $(A, \prec_A)$ and $(B, \prec_B)$ are ordinal notation systems, $(A \uplus B, \prec_{A \uplus B})$ is the one with elements

$$A \uplus B := \{\mathrm{inl}(a) \mid a \in A\} \cup \{\mathrm{inr}(b) \mid b \in B\}$$

and ordering

$$\begin{array}{lcl}
\mathrm{inl}(a) \prec_{A \uplus B} \mathrm{inl}(a') & \Leftrightarrow & a \prec_A a' \\
\mathrm{inr}(b) \prec_{A \uplus B} \mathrm{inl}(b') & \Leftrightarrow & b \prec_B a' \\
\mathrm{inl}(a) \prec_{A \uplus B} \mathrm{inr}(b) & & \\
\mathrm{inr}(a) \not\prec_{A \uplus B} \mathrm{inr}(b) & &
\end{array}$$

Intuitive Well-foundedness: $A \times B$

- If A and B are well founded so is the ordinal notation system $A \times B$ with elements ordered lexicographically ($b^k_i \prec_B b^k_{i+1}$, $a_i \prec_A a_{i+1}$)

$$
\begin{array}{ccccccc}
(a_0, b^0_0) & \prec & (a_0, b^0_1) & \prec & (a_0, b^0_2) & \prec & \cdots \\
\prec & & & & & & \\
(a_1, b^1_0) & \prec & (a_1, b^1_1) & \prec & (a_1, b^1_2) & \prec & \cdots \\
\prec & & & & & & \\
\cdots & & & & & & \\
\prec & & & & & & \\
(a_{n-1}, b^{n-1}_0) & \prec & (a_{n-1}, b^{n-1}_1) & \prec & (a_{n-1}, b^{n-1}_2) & \prec & \cdots \\
\prec & & & & & & \\
(a_n, b^n_0) & \prec & (a_n, b^n_1) & \prec & (a_n, b^n_2) & \prec & \cdots
\end{array}
$$

Intuitive Well-foundedness: $A \times B$

- If A and B are well founded so is the ordinal notation system $A \times B$ with elements ordered lexicographically ($b^k_i \prec_B b^k_{i+1}$, $a_i \prec_A a_{i+1}$)

$$
\begin{array}{ccccccc}
(a_0, b^0_0) & \prec & (a_0, b^0_1) & \prec & (a_0, b^0_2) & \prec & \cdots \\
\curlywedge & & & & & & \\
(a_1, b^1_0) & \prec & (a_1, b^1_1) & \prec & (a_1, b^1_2) & \prec & \cdots \\
\curlywedge & & & & & & \\
\cdots & & & & & & \\
\curlywedge & & & & & & \\
(a_{n-1}, b^{n-1}_0) & \prec & (a_{n-1}, b^{n-1}_1) & \prec & (a_{n-1}, b^{n-1}_2) & \prec & \cdots \\
\curlywedge & & & & & & \\
(a_n, b^n_0) & \prec & (a_n, b^n_1) & \prec & (a_n, b^n_2) & \prec & \cdots
\end{array}
$$

Intuitive Well-foundedness: $A_{\rm dec}$

- If $(A, \prec_A)$ is well founded so is the $(A_{\rm dec}, \prec_{\rm dec})$ where $A_{\rm dec}$ are the set of finite strictly $\prec_A$ descending sequences and $\prec_{\rm dec}$ is the lexicographic ordering.
- **Note:** $(A^*, \prec)$ is not well-founded if A has at least two elements: In $(\{0,1\}^*)$ we have the infinite descending sequence

$$(1) \succ (0,1) \succ (0,0,1) \succ (0,0,0,1) \succ \cdots$$

$$
\begin{array}{cccccccc}
(& a_{n_0}^0 & , & a_{n_1}^1 & , & a_{n_1-1}^2 & , & \cdots a_{n_1-1}^{k_{n_1-1}}) \\
 & = & & = & & \succeq & & \\
(& a_{n_0}^0 & , & \color{blue}{a_{n_1}^1} & , & a_{n_1}^2 & , & \cdots\ a_{n_1}^{k_{n_1}}) \\
 & = & & \succeq & & & & \\
 & & & \cdots & & & & \\
 & = & & \succeq & & & & \\
(& a_{n_0}^0 & , & a_{n_0-1}^1 & , & a_{n_0-1}^2 & , & \cdots a_{n_0-1}^{k_{n_0-1}}) \\
 & = & & \succeq & & & & \\
(& \color{blue}{a_{n_0}^0} & , & a_{n_0}^1 & , & a_{n_0}^2 & , & \cdots\ a_{n_0}^{k_{n_0}}) \\
 & \succeq & & & & & & \\
 & \cdots & & & & & & \\
 & \succeq & & & & & & \\
(& a_{n-1}^0 & , & a_{n-1}^1 & , & a_{n-1}^2 & , & \cdots a_{n-1}^{k_{n-1}}) \\
 & \succeq & & & & & & \\
(& a_n^0 & , & a_n^1 & , & a_n^2 & , & \cdots\ a_n^{k_n})
\end{array}
$$

$$
\color{blue}{a_{n_0}^0} \succ \color{blue}{a_{n_1}^1} \succ \color{blue}{a_{n_2}^2} \succ \cdots
$$

Intuitive Well-foundedness: $A \subseteq B$

- If $(A, \prec_A)$ is well founded, $B \subseteq A$ then $(B, \prec_A \restriction (B \times B))$ is well-founded as well.

Intuitive Well-foundedness: ω^A and ϵ_0

- Terms for Cantor Normal form with basis ω

$$\omega^{\alpha_1} n_1 + \cdots + \omega^{\alpha_k} n_k$$

  can be viewed as descending sequences

$$((\alpha_1, n_1), \ldots, (\alpha_k, n_k))$$

  and which are ordered by lexicographic ordering, and pairs (α, n) are again ordered lexicographically.
- Let the corresponding ordinal notation system ω^A.
- ω^A is a subset of of $(A \times \mathbb{N})_{\mathrm{dec}}$ and, if A is well-founded, well-founded.
- So $\mathbb{N}$ is well founded, and if A is well founded so is ω^A.
- So ϵ_0 is well founded, since any infinite descending sequences will be a sequence in $\omega^{\omega^{\cdots^{\mathbb{N}}}}$.

Intuitive Well-foundedness Proofs

- So we obtain an intuitive well foundedness proof for an ordinal notation system of order type ϵ_0 and therefore an intuitive consistency proof for Peano Arithmetic.
- In our papers [16, 17] on ordinal systems we have extended this approach.
  - Up to $|(\Pi^1_1 - \mathrm{CA})_0|$ we were able to obtain intuitive well-ordering proofs.
  - For theories Beyond $|(\Pi^1_1 - \mathrm{CA})_0|$ up to KPI we were able to get good abstract descriptions and mathematical well-foundedness proofs which are as close as possible to an intuitive argument, but that wasn't fully satisfactory.
  - No surprise that something is happening when on the step towards $|(\Pi^1_1 - \mathrm{CA})|$
  - Relationship to Girard's Π^1_2-logic, which starts with criticism that well-foundedness is a $\Pi^!_1$-concept and for analysing stronger theories one needs a Π^1_2 or higher concept.

A Trivial Ordinal Analysis of Every Consistent Theory (Fulfilling basic Assumptions)

- There is a proof theoretic analysis for all consistent theories which allow to formalise the basics of the following:
- We define a recursive ordinal notation system.
- Elements of it are pairs $\langle n, a \rangle$ where
  - n is an encoding of
    - Partial recursive functions for defining a subset of the natural numbers and an ordering,
    - a proof that the theory shows that those partial recursive functions are computable, i.e. the subset and its ordering is decidable,
    - a proof that the theory shows that this ordering is linear,
    - a proof that the theory shows that it is a well-ordering,
  - a is this element of the ordering encoded in a,
  - pairs $\langle n, a \rangle$ are ordered lexicographically,
    where the first component are ordered as natural numbers and
    a is ordered by the ordering encoded in n.

A Trivial Ordinal Analysis of Every Consistent Theory (Fulfilling basic Assumptions)

- This ordering is linear and decidable.
- Ordinals below some $\langle n, a \rangle$ are the union of the finitely many well-orderings encoded by some $n' < n$ and together with the ordinals below a in the ordering encoded by n.
- Since all of them are provable well orderings , the union is as well a well-ordering, provable in the theory, so the theory proves transfinite induction for every element of it.
- Therefore the ordering has strength ≤ the proof theoretic strength of the theory.
- Every provable well-ordering in this theory is a segment of this ordering, so the ordering has strength ≥ the proof theoretic strength of the theory.
- So we obtain an ordinal analysis of every theory.

A Trivial Ordinal Analysis of Every Consistent Theory (Fulfilling basic Assumptions)

- So in order to gain something from an ordinal analysis we need to get more than just an ordinal notation system of strength the proof theoretic strength.
- Therefore it is often claimed that one needs a "natural well-ordering".
- In the light of Hilbert's program one could say that one criteria for being a natural well-ordering is that it gives some more direct insights into its well-foundedness.

Myths about a Revised Hilbert's Program

- **Myth No. 1**: We need to redo mathematics in a constructive way.
  - The Hilbert's program is about proving the consistency of mathematical theories to allow us to work in those theories.
  - All you need is to develop suitable theories with a direct consistency argument, carry out that argument and prove that it allows to prove the consistency of large mathematical theories (usually via ordinal analysis).
  - Constructivisation of mathematics is not wrong.
    It has lots of benefits.
    - A constructive proof gives more information about the theorem than just it's validity.
    - A constructive proof often gives a deeper intuition about the validity of the theorem.
    - Constructivism has resulted in excellent proof assistants and dependently typed programming languages, including the biggest ones Agda and Coq.
  - However, a constructive underpinning of a theory gives to some extend a constutictivisation of everything ever being proved in this theory.

Myths about a Revised Hilbert's Program

- **Myth No. 2**: We get absolute truth.
  - We cannot avoid Gödel's 2nd Incompleteness Theorem.
  - Any consistency proof will be based on principles of equal strength.
  - However, a consistency proof should at least make it very surprising if the underlying theory is inconsistent.
    - Example: Naive Set Theory.
      It is inconsistent, and it was very surprising. But there were no consistency arguments explored at that time.
    - Example: Quine's New Foundation:
      If an inconsistency were found, people would say: yes there was just a flaw.
    - Example Zermelo-Fraenkel Set Theory
      It would be surprising but not inconceivable.
    - If you find an inconsistency in Peano Arithmetic, you must find an infinite descending sequence in the ordinal notation system of strength ϵ_0 - that would be very surprising.
      It cannot be excluded because there is some hand waving in any direct consistency argument.

Myths about a Revised Hilbert's Program

- **Myth No. 3**: Once we have an intuitive consistency argument we can rely on it and don't need to model the theory in question.
  - We need to be at least as good as theories developed and analysed before.
  - Intuitive arguments can have flaws.
  - Formalising them makes them more precise and exposes any weaknesses.
  - If you develop a theory in which you put your trust, it is good to carry out a consistency proof in some accepted mathematical theory such as ZF set theory.

Myths about a Revised Hilbert's Program

- **Myth No. 4**: Having worked in ZF set theory (or some other theory) so long we know it is consistent.
  - We have not exploited the full strength of it yet.
    A proof theoretic analysis is to some extend the first time one fully exploits what is given in a theory.
  - When reaching beyond $(\Pi^1_2 - \mathrm{CA})$ phenomena start to occur which indicate that there may be a potential problem (we don't know of course).
  - In mathematics there have been long standing conjectures which turned out to be false.

Myths about a Revised Hilbert's Program

- **Myth No. 5**: Because of Gödel's 2nd Incompleteness Theorem it is a waste of time to try to prove the consistency of mathematical theories.
  - We need to secure it, in order to find an inconsistency if it exists.
  - The hope is that if an inconsistency if found we will find it if trying to prove the consistency.
  - We need to test it, as any physical theory is tested in many ways by experiments, by analysing it.
  - And in the way of analysing it we make marvellous discoveries, because we are constructivising proof theoretically strong theories – we get deep insights into how these theories actually work.

Myths about a Revised Hilbert's Program

- **Myth No. 6**: If we carry out this program for an inconsistent theory we will discover the inconsistency.
  - A good counter example is Martin-Löf's inconsistent type theory [12], which included $\mathrm{Set} : \mathrm{Set}$ (inconsistent by Girard's paradox [10], see as well [8]).
  - Martin Löf had a normalisation proof, which was carried out in an inconsistent theory.
  - Therefore a consistency proof does not reveal an inconsistency.

Myths about a Revised Hilbert's Program

- **Myth No. 7**: We know the consistency of Peano Arithmetic inconsistency.
  - It would be very surprising if it were inconsistent.
  - It is highly unlikely that it is inconsistent.
  - But we cannot get around Gödel's Incompleteness theorem.
  - Any argument for its consistency will at some point refer to intuition, hand waving – because there is no absolute consistency proof.
  - When first exposed to induction, the teacher will argue, hand wave, but will not be able to prove that it is correct.
  - However,it is highly, highly, highly unlikely that it is inconsistent – we just will never know absolutely.
  - If there is an inconsistency it will probably occur much higher in an area of theories which haven't been analysed proof theoretically.

Myths about a Revised Hilbert's Program

- **Myth No. 8**: The Platonic Universe proves the consistency of ZF set theory.
  - It is easy to imagine a Platonic universe for naive set theory.
    But this universe doesn't exist.
  - Axiom systems about the infinite are obtained by taking properties which hold in the finite and then extrapolating it to the infinite.
    - Some of this analogies failed in the past, and we hope that know we have systems which are consistent.
    - But we don't know and will never know.
    - There is no 100% rational argument which proves the consistency of any reasonably strong mathematical theory directly.

J. Barwise.
Admissible sets and structures.
Berlin Springer, 1975.

W. Buchholz.
Notation systems for infinitary derivations.
Archive for Mathematical Logic, 30:277–296, 1991.
http://dx.doi.org/10.1007/BF01621472.

W. Buchholz.
A simplified version of local predicativity.
In P. Aczel, H. Simmons, and S. S. Wainer, editors, Proof Theory. A selection of papers from the Leeds Proof Theory Programme 1990, pages 115 – 147. Cambridge University Press, 1992.
https://pdfs.semanticscholar.org/bf88/86fefc5184ba40b45d831389b9bc108cd343.pdf.

W. Buchholz.
Explaining Gentzen's proof with infinitary proof theory.
In G. Gottlob, A. Leitsch, and D. Mundici, editors, Computational logic and proof theory. 5th Kurt Gödel Colloquium, KGC '97, pages 4 – 17. Springer Lecture Notes in Computer Science, 1289, 1997.
https://link.springer.com/content/pdf/10.1007%2F3-540-63385-5_29.pdf.

W. Buchholz and K. Schütte.
Proof Theory of Impredicative Subsystems of Analysis.
Studies in Proof Theory, Monographs, Vol 2. Bibliopolis, Naples, 1989.

G. Cantor.
Beiträge zur Begründung der transfiniten Mengenlehre.
Mathematische Annalen, 46:481–512, 1895.
https://doi.org/10.1007/bf02124929,
https://zenodo.org/record/1428392#.XXAyNPzTV_s.

G. Cantor.
Contributions to the founding of the theory of transfinite numbers.
Dover, New York, 1915.
Translated and provided with an introduction and notes by Philip E. B. Jourdain M.A. (Cantab.).
https://www.maths.ed.ac.uk/~v1ranick/papers/cantor1.pdf.

T. Coquand.
An analysis of Girard's paradox, 1986.
RR-0531, INRIA. inria-00076023.
https://hal.inria.fr/inria-00076023/document.

G. Gentzen.
Die Widerspruchsfreiheit der reinen Zahlentheorie.
Mathematische Annalen, 112(1):493 – 565, December 1936.
https://doi.org/10.1007/BF01565428,
https://gdz.sub.uni-goettingen.de/id/PPN235181684_0112?tify=%7B%22view%22:%22info%22,%22pages%22:%5B497%5D%7D.

J.-Y. Girard.
Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur.
PhD thesis, Université Paris VII, Paris, 1972.
http://www.cs.cmu.edu/afs/cs.cmu.edu/user/kw/www/scans/girard72thesis.pdf.

G. Jäger.
Theories for Admissible Sets: A Unifying Approach to Proof Theory.
Studies in Proof Theory Lecture Notes, Vol 2. Humanities Pr, 1987.

Martin-Löf.
A theory of types.
Unpublished Manuscript, 1971.

P. Martin-Löf.
Intuitionistic type theory, volume 1 of Studies in Proof Theory.
Bibliopolis, 1984.
https://archive-pml.github.io/martin-lof/pdfs/Bibliopolis-Book-retypeset-1984.pdf.

A. Setzer.
Proof theoretical strength of Martin-Löf Type Theory with W-type and one universe.
PhD thesis, Mathematisches Institut, Universität München, Munich, Germany, 1993.
Available from
http://www.cs.swan.ac.uk/~csetzer/articles/weor0.pdf.

A. Setzer.
Well-ordering proofs for Martin-Löf type theory.
Annals of Pure and Applied Logic, 92:113 – 159, 1998.
https://doi.org/10.1016/S0168-0072(97)00078-X,
http://www.cs.swan.ac.uk/~csetzer/articles/2papdiss.pdf.

A. Setzer.
Ordinal systems.
In B. Cooper and J. Truss, editors, Sets and Proofs, pages 301 – 331, Cambridge, 1999. Cambridge University Press.
http://www.cs.swan.ac.uk/~csetzer/articles/ordsyscor010124.pdf.

A. Setzer.
Ordinal systems part 2: One inaccessible.
In S. Buss, P. Hajek, and P. Pudlak, editors, Logic Colloquium '98, ASL Lecture Notes in Logic 13, pages 426 – 448, Massachusetts, 2000. Peters Ltd.
https://doi.org/10.1017/9781316756140.030,
http://www.cs.swan.ac.uk/~csetzer/articles/ordsystwo.pdf.

A. Setzer.
Proof theory of Martin-Löf Type Theory – An overview.
Mathematiques et Sciences Humaines, 42 année, n^{o}165:59 – 99, 2004.
http://msh.revues.org/2959,
http://www.cs.swan.ac.uk/~csetzer/articles/overviewProofTheoryTypeTheory2004.pdf.

A. Setzer.
The use of trustworthy principles in a revised Hilbert's program.
In R. Kahle and M. Rathjen, editors, Gentzen's Centenary, pages 45–60. Springer International Publishing, 2015.
http://dx.doi.org/10.1007/978-3-319-10103-3_3,
http://www.cs.swan.ac.uk/~csetzer/articles/setzerGentzenCentenary.pdf.