Formalising Contemporary Mathematics in Simple Type Theory

Lawrence C Paulson FRS
Computer Laboratory

The Topos Institute Colloquium, 1 July 2021

Supported by the ERC Advanced Grant ALEXANDRIA (742178).
“No matter how much wishful thinking we do, the theory of types is here to stay. There is no other way to make sense of the foundations of mathematics. Russell (with the help of Ramsey) had the right idea, and Curry and Quine are very lucky that their unmotivated formalistic systems are not inconsistent.”

–Dana Scott (1969)
From simple type theory to proof assistants for higher-order logic

- Russell (1910), Ramsey (1926), etc.
- Church’s typed λ-calculus (1940) formalisation
- base types including the Booleans, and function types
- sets and specifications (e.g. \( \mathbb{N} \)) coded as predicates (and sometimes as types)
- Wenzel (1997): axiomatic type classes
Advantages over dependent types

- Simpler syntax, semantics, and therefore implementations
- ... which therefore can give us more automation
- Fewer surprises with hidden arguments, type checking
- HOL is self-contained: inductive definitions, recursion, etc are reducible to the base logic
- Extensional equality for sets and functions
But is formalised maths possible?

Whitehead and Russell needed 362 pages to prove $1+1=2$!

Gödel proved that all reasonable formal systems must be incomplete!

Church proved that first-order logic is undecidable!

We have better formal systems than theirs.

But mathematicians also work from axioms!

We want to assist people, not to replace them.
Mathematics in Isabelle/HOL

- Jordan curve theorem
- Central limit theorem
- Residue theorem
- Prime number theorem
- Gödel’s incompleteness theorems
- Algebraic closure of a field
- Verification of the Kepler conjecture*

- Matrix theory, e.g. Perron–Frobenius
- Analytic number theory, eg Hermite–Lindemann
- Nonstandard analysis
- Homology theory
- Topology
- Complex roots via Sturm sequences
- Measure, integration and probability theory
- Complex roots via Sturm sequences
**Distinctive features of Isabelle/HOL**

- Simple types with axiomatic type classes
- Powerful automation: proofs and counterexamples
- Structured proof language
- Interactive development environment (PIDE)
- User-definable mathematical notation
- “Literate” proof documents can be generated in LaTeX
- An archive of over 600 proof developments; 385 authors and nearly 3 million lines of code
Can we do *set theory* in higher-order logic?

- HOL is actually weaker than *Zermelo* set theory
- ... but we can simply add a type of ZF sets with the usual axioms.
- [our framework presupposes the *axiom of choice*]
- ... and develop cardinals, ordinal arithmetic, order types and the rest.
Partition notation: $\alpha \longrightarrow (\beta, \gamma)^n$

$[A]^n$ denotes the set of unordered $n$-element sets of elements of $A$

if $[\alpha]^n$ is partitioned (“coloured”) into two parts (0, 1) then there’s either

- a subset $B \subseteq \alpha$ of order type $\beta$ whose $n$-sets are all coloured by 0
- a subset $C \subseteq \alpha$ of order type $\gamma$ whose $n$-sets are all coloured by 1

Infinite Ramsey theorem: $\omega \longrightarrow (\omega, \omega)^n$
Erdős’ problem (for 2-element sets)

\[ \alpha \rightarrow (\alpha, 2) \text{ is trivial} \quad \alpha \rightarrow (|\alpha| + 1, \omega) \text{ fails for } \alpha > \omega \]

So which countable ordinals \( \alpha \) satisfy \( \alpha \rightarrow (\alpha, 3) \)?

It turns out that \( \alpha \) must be a power of \( \omega \)

In 1987, Erdős offered a $1000 prize for a full solution
Material formalised for this project

\[ \omega^2 \longrightarrow (\omega^2, m) \quad \text{(Specker)} \]

\[ \omega^{1+\alpha n} \longrightarrow (\omega^{1+\alpha}, 2^n) \quad \text{(Erdős and Milner)} \]

\[ \omega^\omega \longrightarrow (\omega^\omega, m) \quad \text{(Milner, Larson)} \]

Plus background theories: Cantor normal form for ordinals; facts about order types; the Nash-Williams partition theorem

Project done with Mirna Džamonja and Angeliki Koutsoukou-Argyraki
Paul Erdős and E. C. Milner, 1972

\[ \omega^{1+\alpha n} \longrightarrow (\omega^{1+\alpha}, 2^n) \] for \( \alpha \) an ordinal and \( n \) a natural number

“We have known this result since 1959”
(it’s in Milner’s 1962 PhD thesis)

It’s a five-page paper that needed a full-page correction in 1974.
We now conclude the proof of the theorem.
Since $\beta$ is denumerable and nonzero, there is a sequence $(\gamma_n : n < \omega)$ which repeats each element of $B$ infinitely often, i.e. such that

\[(11) \quad |\{n : \gamma_n = \nu\}| = \aleph_0 \quad (\nu \in B).\]

Since $\text{tp } S = \alpha \beta$, we may write $S = S^{(0)} = \bigcup (\nu \in B) A^{(0)}_\nu (\cdot) \cdot$.

Let $n < \omega$ and suppose we have already chosen elements $x_i \in S (i < n)$ and a subset

\[(12) \quad S^{(n)} = \bigcup (\nu \in B) A^{(n)}_\nu (\cdot) \cdot \]

of $S$ of order type $\alpha \beta$. Since $\alpha$ is right-SI, $A^{(n)}_\nu$ contains a final section $A'$ such that

\[A^{(n)}_\nu \cap \{x_0, \ldots, x_{n-1}\} \subseteq A'.\]

By (10), there are $x_n \in A'$, a strictly increasing map

\[g_n : B \rightarrow B\]

and sets $A^{(n+1)}_\nu (\nu \in B)$ such that

\[g_n (\gamma_i) = \gamma_i \quad (i \leq n),\]

\[(13) \quad A^{(n+1)}_\nu \subseteq K_1(x_n) \cap A^{(n)}_\nu (\nu \in B).\]

From the definition of $A'$, it follows that

\[x_n \in A^{(n)}_\nu \subseteq S^{(n)} \quad (\nu \in B),\]

and

\[x_i < x_n \quad \text{if } i < n \quad \text{and} \quad x_i \in A^{(n)}_\nu.\]

$S^{(n+1)}$ is defined by equation (12) with $n$ replaced by $n+1$. It follows by induction that there are $x_n$, $A^{(n)}_\nu (\nu \in B)$, $S^{(n)}$ and $g_n$ such that (12)–(16) hold for $n < \omega$.

Let $Z = \{x_n : n < \omega\}$. If $m < n < \omega$, then by (15), (14), and (12) we have that
Key steps of Erdős and Milner’s proof

- Every ordinal is a “strong type” *(about 200 lines of machine proof)*
- A “remark” about indecomposable ordinals *(72 lines)*
- A key lemma: \( \alpha \beta \rightarrow (\min(\gamma, \omega \beta), 2k) \) if \( \alpha \rightarrow (\gamma, k) \) for \( k \geq 2 \) *(about 960 lines)*
- The main theorem \( \omega^{1+\alpha n} \rightarrow (\omega^{1+\alpha}, 2^n) \) by induction on \( n \) *(about 30 lines)*
- Larson’s corollary: \( \omega^{nk} \rightarrow (\omega^n, k) \) *(about 35 lines)*
Every ordinal is a “strong type”

We will say that $\beta$ is a strong type if, whenever $\text{tp } B = \beta$ and $D \subseteq B$, then there are $n < \omega$ and sets $D_1, \ldots, D_n \subseteq D$ such that

$$\text{tp } D_i \text{ is } \beta \text{ for all } i \leq n$$

**proposition** strong_ordertype_eq:

- **assumes** $D$: "$D \subseteq \text{elts } \beta$" and "Ord $\beta$"
- **obtains** $L$ where
  - $\bigcup (\text{List.set } L) = D$ "$\forall X. X \in \text{List.set } L \implies \text{indecomposable (tp } X)$" and
  - $\forall M. \exists M \subseteq D; \forall X. X \in \text{List.set } L \implies \text{tp } (M \cap X) \geq \text{tp } X \implies \text{tp } M = \text{tp } D$"

**proof** -

- **define** $\varphi$ where "$\varphi \equiv \text{inv_into } D (\text{ordermap } D \text{ VWF})$"
- **then have** $\text{bij}_\varphi$: "$\text{bij_betw } \varphi (\text{elts (tp } D)) D$"
  - **using** $\text{D bij_betw_inv into down ordermap bij by blast}$
- **have** $\varphi_{\text{cancel_left}}$: "$\forall d. d \in D \implies \varphi (\text{ordermap } D \text{ VWF } d) = d$"
  - **by** (metis D $\varphi$ $\text{def bij_betw_inv into left down ordermap bij small_iff_range total_on}$)
- **have** $\varphi_{\text{cancel_right}}$: "$\forall \gamma. \gamma \in \text{elts (tp } D) \implies \text{ordermap } D \text{ VWF } (\varphi \gamma) = \gamma$"
  - **by** (metis $\varphi$ $\text{def f inv_into f ordermap_surj subsetD}$)
- **have** "small $D" \ "D \subseteq \text{ON}""
  - **using** $\text{assms down elts_subset ON [of } \beta \text{] by auto}$
- **then have** $\varphi_{\text{less_iff}}$: "$\forall \gamma \delta. \exists \gamma \in \text{elts (tp } D); \delta \in \text{elts (tp } D) \implies \varphi \gamma < \varphi \delta \iff \gamma < \delta$"
  - **using** $\text{ordermap_mono_less [of } \_ \_ \text{ VWF } D \text{ bij_betw_apply [OF bij}_\varphi \text{] VWF_iff_Ord_less } \varphi \_ \_ \text{ case)}$
    - **by** (metis ON $\text{imp Ord Ord_linear2 less_V_def order.asym}$)
A remark about indecomposable ordinals

If \( x \in A \) and \( A_1 \subseteq A \), with type \( A \), \( A_1 = \alpha \), then there is \( A_2 \subseteq A_1 \) such that \( \{x\} < A_2 \).
$\alpha \beta \rightarrow (\min(\gamma, \omega \beta), 2k)$ if $\alpha \rightarrow (\gamma, k)$

- Assume there is no $X \in [\alpha \beta]^{2k}$ such that $[X]^2$ is 1-coloured
- Assume there is no $C \subseteq \alpha \beta$ of order type $\gamma$ such that $[C]^2$ is 0-coloured
- Then show there is a $Z \subseteq \alpha \beta$ of order type $\omega \beta$ such that $[Z]^2$ is 0-coloured
  
  this will require generating an $\omega$-chain of sets of type $\beta$
\[
\alpha \beta \rightarrow (\min(\gamma, \omega \beta), 2k)
\]
if \[
\alpha \rightarrow (\gamma, k)
\]
Equation (8) with its one-line proof

(8) If $A \subseteq S$, then there is $X \in [A]$. This follows from the hypothesis.
Main Theorem

Suppose (2) holds for some integer $h \geq 1$. Applying the above theorem with $k = 2^h$, $\alpha = \omega^{1+\nu h}$, $\beta = \omega^\nu$, $\gamma = \omega^{1+\nu}$, we see that (2) also holds with $h$ replaced by $h + 1$. Since (2) holds trivially for $h = 1$, it follows that (2) holds for all $h < \omega$. 
Jean Larson, 1973

\[ \omega^\omega \rightarrow (\omega^\omega, m) \text{ for } m \text{ a natural number} \]

Proved by CC Chang in a 56-page paper (J. Combinatorial Theory A) and generalised by EC Milner

Simplified by Larson to 17 pages, including a new proof of \( \omega^2 \rightarrow (\omega^2, m) \)
A few key definitions

Work with finite increasing sequences

- \( W(n) = \{(a_0, a_1, \ldots, a_{n-1}) : a_0 < a_1 < \cdots < a_{n-1} < \omega\} \) has order type \( \omega^n \)
- \( W = W(0) \cup W(1) \cup W(2) \cup \cdots \) has order type \( \omega^\omega \)

Given \( f : [W]^2 \to \{0,1\} \) such that there is no \( M \in [W]^m \) s.t. \( [M]^2 \) is 1-coloured

Show there is a \( X \subseteq W \) of order type \( \omega^\omega \) such that \( [X]^2 \) is 0-coloured
Interaction schemes

For $x, y \in W$, write $x = a_1 \ast a_2 \ast \cdots \ast a_k (a_{k+1})$ and $y = b_1 \ast b_2 \ast \cdots \ast b_k$

put $c = (|a_1|, |a_1| + |a_2|, \ldots, |a_1| + |a_2| + \cdots + |a_k| (a_{k+1}))$

define $i(\{x, y\}) = c \ast a_1 \ast d \ast b_1 \ast a_2 \ast b_2 \ast \cdots \ast a_k \ast b_k (a_{k+1})$

(this classifies how consecutive segments in $x, y$ interact)

By Erdős–Milner we can assume $|x| < |y|$
The Nash-Williams partition theorem

A set $A \subseteq W$ is thin if for all $s, t \in A$, the sequence $s$ is not an initial segment of $t$.

Given an infinite set $M \subseteq \omega$, a thin set $A$, a function $h : \{s \in A : s \subseteq M\} \rightarrow \{0,1\}$.

Then there exists an $i \in \{0,1\}$ and an infinite set $N \subseteq M$ so that $h(\{s \in A : s \subseteq N\}) \subseteq \{i\}$. 
The three main lemmas

**Lemma 3.6.** For every function \( g : [W]^2 \to \{0, 1\} \), there exists an infinite set \( N \subseteq \omega \) and a sequence \( \{j_k : k < \omega\} \), so that for any \( k < \omega \) with \( k > 0 \), and any pair \( \{x, y\} \) of form \( k \) with \( (n_k) < i(\{x, y\}) \subseteq N \), \( g(\{x, y\}) = j_k \).

**Lemma 3.7.** For every infinite set \( N \) and every \( m, l < \omega \) with \( l > 0 \), there is an \( m \) element set \( M \), so that for every \( \{x, y\} \subseteq M \), \( \{x, y\} \) has form \( l \) and \( i(\{x, y\}) \subseteq N \).

**Lemma 3.8.** For any infinite set \( N \subseteq \omega \) there is a set \( X \subseteq W \) of type \( \omega^\omega \) so that for any pair \( \{x, y\} \subseteq X \), there is an \( l < \omega \), so that \( \{x, y\} \) is of form \( l \) and if \( l > 0 \), then \( (n_l) < i(\{x, y\}) \subseteq N \).
Now we finish the proof of Theorem 3.1 using these three lemmas. First we apply Lemma 3.6 to $f$ and obtain an infinite set $N$ and a sequence $\{j_k: k < \omega\}$. Then for each $k < \omega$ with $k > 0$, we apply Lemma 3.7 to $k, m$ and $\{n_l: k < l < \omega\}$ and obtain an $m$ element set $M_k$, so that for any $\{x, y\} \subseteq M_k, f(\{x, y\}) = j_k$. Thus we may conclude that for any $k < \omega$ with $k > 0, j_k = 0$. Next we apply Lemma 3.8 to $N$ and obtain a set $X \subseteq \mathcal{W}$ of type $\omega^\omega$, so that for any $\{x, y\} \subseteq X$, there is an $l < \omega$ for which $\{x, y\}$ has form $l$ and if $l > 0$, then $(n_l) < i(\{x, y\}) \subseteq N$. Thus on pairs $\{x, y\} \subseteq X$ which are not of form 0, $f(\{x, y\}) = j_l = 0$ for some $l$. By assumption, for any pair $\{x, y\}$ of form 0, $f(\{x, y\}) = 0$, so $f([X]^2) = \{0\}$, and the theorem follows.
Why are these machine proofs so long?

- The level of detail in published proofs varies immensely
- … plus my lack of expertise in the area
- “Obvious” claims—about order types, cardinality, combinatorial intuitions—don’t have obvious proofs
- And some of the constructions are gruesome
This sort of inductive definition is tricky!

Let $d^1 = (n_1, n_2, ..., n_{k+1}) = (d^1_1, d^1_2, ..., d^1_{k+1})$ and let $a^1_i$ be the sequence of the first $d^1_i$ elements of $N$ greater than $d^1_{k+1}$. Now suppose we have constructed $d^1, a^1_1, ..., d^i, a^i_i$. Let $d^{i+1} = (d^1_{i+1}, ..., d^1_{k+1})$ be the first $k + 1$ elements of $N$ greater than the last element of $a^i_i$, and let $a^{i+1}_1$ be the first $d^{i+1}_1$ elements of $N$ greater than $d^{i+1}_{k+1}$. This defines $d^1, d^2, ..., d^m, a^1_1, a^2_1, ..., a^m_1$. Let the rest of the sequences be defined in the order that follows, so that for any $i$ and $j$, $a^i_j$ is the sequence of the least $(d^i_j - d^i_{j-1})$ elements of $N$ all of which are larger than the largest element of the sequence previously defined:

$$(a^m_1) a^1_2, a^2_2, a^3_2, ..., a^m_2, a^1_3, ..., a^m_3, ..., a^1_k, ..., a^m_k, a^m_{k+1}, a^m_{k+1}, ..., a^1_{k+1}.$$
<table>
<thead>
<tr>
<th>Other formalisations within ALEXANDRIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>✤ Transcendence of Certain Infinite Series (criteria by Hančl and Rucki)</td>
</tr>
<tr>
<td>✤ Irrationality Criteria for Series by Erdős and Straus</td>
</tr>
<tr>
<td>✤ Irrational Rapidly Convergent Series (a theorem by J. Hančl)</td>
</tr>
<tr>
<td>✤ Counting Complex Roots</td>
</tr>
<tr>
<td>✤ Budan–Fourier Theorem and Counting Real Roots</td>
</tr>
<tr>
<td>✤ Localization of a Commutative Ring</td>
</tr>
<tr>
<td>✤ Projective Geometry</td>
</tr>
<tr>
<td>✤ Quantum Computation and Information</td>
</tr>
<tr>
<td>✤ Grothendieck Schemes</td>
</tr>
</tbody>
</table>
Brief remarks on Grothendieck Schemes

- Build-up of mainstream structures in algebraic geometry: presheaves and sheaves of rings, locally ringed spaces, affine schemes.

- The spectrum of a ring is a locally ringed space, hence an affine scheme.

- Any affine scheme is a scheme.

- They said it couldn’t be done in simple type theory.

- But we did it faster and with less manpower than the Lean guys.

- One key technique: a structuring mechanism known as locales.*

- Led by Anthony Bordg
What can mathematicians expect from proof technology in the future?

- Ever-growing libraries of definitions and theorems
- ... with advanced search
- Verification of dull but necessary facts
- ... and exhibiting counterexamples
- Detection of analogous developments, with hints for proof steps
- Warnings of simple omissions, e.g. “doesn’t $S$ need to be compact?”
- A careful and increasingly intelligent assistant