Mechanizing Set Theory:

Cardinal Arithmetic and the Axiom of Choice

Krzysztof Grąbczewski, Copernicus University, Torun, Poland

Lawrence C Paulson, Computer Laboratory, Cambridge University, UK

Funding: EPSRC grant GR/H40570; TEMPUS Project JEP 3340; ESPRIT Project 6453

The Generic Proof Assistant *Isabelle*

many logics ⋆ higher-order syntax ⋆ unification

- *Expressions* are typed λ-terms
- *Schematic rules* are generalized Horn clauses (like λProlog's)
- *Resolution* applies rules for proof checking
- *Tactic language* allows user-defined automation
- *Generic packages* include simplifier, tableau prover, ...

Some Isabelle Logics

- FOL, Constructive Type Theory, modal logics, linear logic, . . .
- ZF set theory
  - Built upon FOL
  - Lamport's Temporal Logic of Actions (*Sara Kalvala*)
  - Milner & Tofte's co-induction example (*Jacob Frost*)
- HOL
  - I/O Automata (*Nipkow & Slind*)
  - hardware examples (*Sara Kalvala*)
  - semantic equivalence (*Lötzbeyer & Sandner*)

The Cardinal Proofs

- *Aim*: justify recursive definitions like $D = 1 + D + (\omega \to D)$
- *Basis*: theories of relations, functions, recursion, ordinals, ...
- *Method*: mechanize most of Kunen, *Set Theory*, Chapter I.
  - orders
  - order-isomorphisms
  - order types
  - ordinal arithmetic
  - cardinality
  - infinite cardinals
  - AC

Kunen's Proof of $\kappa \otimes \kappa = \kappa$

"By transfinite induction on κ. Then for $\alpha < \kappa$, $|\alpha \times \alpha| = |\alpha| \otimes |\alpha| < \kappa$.

Define a wellordering $\lhd$ on $\kappa \times \kappa$ by $\langle\alpha, \beta\rangle \lhd \langle\gamma, \delta\rangle$ iff

$$\max(\alpha, \beta) < \max(\gamma, \delta) \vee [\max(\alpha, \beta) = \max(\gamma, \delta) \wedge$$
$$\langle\alpha, \beta\rangle \text{ precedes } \langle\gamma, \delta\rangle \text{ lexicographically}].$$

Each $\langle\alpha, \beta\rangle \in \kappa \times \kappa$ has no more than

$$|(\max(\alpha, \beta)) + 1 \times (\max(\alpha, \beta)) + 1| < \kappa$$

predecessors in $\lhd$, so $\mathrm{type}(\kappa \times \kappa, \lhd) \leq \kappa$, whence $|\kappa \times \kappa| \leq \kappa$. Since clearly $|\kappa \times \kappa| \geq \kappa$, $|\kappa \times \kappa| = \kappa$." □

Formulations of the Well-Ordering Theorem

WO_1: Every set can be well-ordered.

WO_2: Every set is equipollent to an ordinal number.

$\vdots$

WO_6: For every set x, there exists $m \geq 1$, an ordinal α, and a function f defined on α such that $f(\beta) \preceq m$ for every $\beta < \alpha$ and $\bigcup_{\beta<\alpha} f(\beta) = x$.

WO_7: For every set A, A is finite $\iff$ for each well-ordering R of A, also R^{-1} well-orders A.

From Rubin & Rubin, *Equivalents of the Axiom of Choice*, Chapter 1

Formulations of the Axiom of Choice

AC_1: If A is a set of non-empty sets then there exists f such that $f(B) \in B$ for all $B \in A$.

$\vdots$

AC_6: The product of a set of non-empty sets is non-empty.

$\vdots$

$AC_{16}(n, k)$: If A is an infinite set then there is a set t_n of n-element subsets of A such that each k-element subset of A is a subset of exactly one element of t_n. $(1 < k < n)$

From Rubin & Rubin, *Equivalents of the Axiom of Choice*, Chapter 2

Proof of $WO_6 \Rightarrow WO_1$

Lemma. If WO_6 and $y \times y \subseteq y$ then y can be well-ordered.

Proof: by induction using Lemma (ii) below. □

Theorem. If WO_6 then every set x can be well-ordered.

Proof: Define y such that $x \subseteq y$ and $y \times y \subseteq y$.

$$y = \bigcup_{n \in \omega} z_n, \quad \text{where} \begin{cases} z_0 = x \\ z_{n+1} = z_n \cup (z_n \times z_n) \end{cases}$$

Hence x is a subset of a well-ordered set. □

Lemma for $WO_6 \Rightarrow WO_1$

Let $N_y = \left\{m : \exists_{f,\alpha}\, \mathrm{dom}(f) = \alpha, \bigcup_{\beta<\alpha} f(\beta) = y, \forall_{\beta<\alpha}\, f(\beta) \preceq m\right\}$

Lemma (ii): If $m \in N_y$ and $m > 1$ then $m - 1 \in N_y$.

Proof: Assume $y \times y \subseteq y$ and $m \in N(y)$. Then f and α exist. Put

$$u_{\beta\gamma\delta} \stackrel{\mathrm{def}}{=} [f(\beta) \times f(\gamma)] \cap f(\delta) \qquad (\beta, \gamma, \delta < \alpha)$$

Clearly $u_{\beta\gamma\delta} \preceq m$, $\mathrm{dom}(u_{\beta\gamma\delta}) \preceq m$, $\mathrm{rng}(u_{\beta\gamma\delta}) \preceq m$.

Case 1: $\forall_{\beta<\alpha}.\ f(\beta) \neq 0 \rightarrow \exists_{\gamma,\delta<\alpha}.\ \mathrm{dom}(u_{\beta\gamma\delta}) \neq 0 \land \mathrm{dom}(u_{\beta\gamma\delta}) \prec m$

Case 2: $\exists_{\beta<\alpha}.\ f(\beta) \neq 0 \land \forall_{\gamma,\delta<\alpha}.\ \mathrm{dom}(u_{\beta\gamma\delta}) \neq 0 \rightarrow \mathrm{dom}(u_{\beta\gamma\delta}) \approx m$

Complex reasoning reduces m (and doubles α) in both cases. $\square$

Observations

- Mechanisation of parts of two advanced texts
  - Kunen, *Set Theory*, most of Chapter I (*Paulson*)
  - Rubin & Rubin, *Equivalents of AC*, Chapters 1–2 (*Grąbczewski*)
- Obstacles to faithful mechanisation
  - unevenly-sized gaps in human proofs (intuitive leaps)
  - different definitions of standard concepts
- Features for future systems?
  - type inclusions, e.g. *naturals* $\subseteq$ *cardinals* $\subseteq$ *ordinals* $\subseteq$ *sets*
  - inheritance of structure (for algebra)