Mechanising Set Theory: Cardinal Arithmetic and the Axiom of Choice

Lawrence C. Paulson
Computer Laboratory, University of Cambridge, UK
email: lcp@cl.cam.ac.uk

Krzysztof GraÀbczewski
Nicholas Copernicus University, Toruń, Poland
email: kgrabcze@mat.uni.torun.pl

10 August 1995

1 Introduction

A growing corpus of mathematics has been checked by machine. Researchers have constructed computer proofs of results in logic [23], number theory [22], group theory [25], λ-calculus [9], etc. An especially wide variety of results have been mechanised using the Mizar Proof Checker and published in the Mizar journal [6]. However, the problem of mechanising mathematics is far from solved.

The Boyer/Moore Theorem Prover [2, 3] has yielded the most impressive results [22, 23]. It has been successful because of its exceptionally strong support for recursive deÆnitions and inductive reasoning. But its lack of quantiÆers forces mathematical statements to undergo serious contortions when they are formalised. Most automated reasoning systems are Ærst-order at best, while mathematics makes heavy use of higher-order notations. We have conducted our work in Isabelle [18], which provides for higher-order syntax. Other recent systems that have been used for mechanising mathematics include IMPS [5] and Coq [4].

We describe below machine proofs concerning cardinal arithmetic and the Axiom of Choice (AC). Paulson has mechanised most of the Ærst chapter of Kunen [11] and a paper by Abrial and LafÆtte [1]. GraÀbczewski has mechanised the Ærst two chapters of Rubin and Rubin's famous monograph [21], proving equivalent eight forms of the Well-ordering Theorem and twenty forms of AC. We have conducted these proofs using an implementation of Zermelo-FrÒnkel (ZF) set theory in Isabelle. Compared with other Isabelle/ZF proofs [13, 15, 16] and other automated set theory proofs [20], these are deep, abstract and highly technical results.

We have tried to reproduce the mathematics faithfully. This does not mean slavishly adhering to every detail of the text, but attempting to preserve its spirit. Mathematicians write in a mixture of natural language and symbols; they devise all manner of conventions to express their ideas succinctly. Their proofs make great intuitive leaps, whose detailed justiÆcation requires much additional work. We have been careful to note passages that seem unusually hard to mechanise, and discuss some of them below.

In conducting these proofs, particularly from Rubin and Rubin, we have tried to follow the footsteps of Jutting [10]. During the 1970s, Jutting mechanised a mathematics textbook using the AUTOMATH system [12]. He paid close attention to the text – which described the construction of the real and complex numbers starting from the Peano axioms – and listed any deviations from it. Compared with Jutting, we have worked in a more abstract Æeld, and with source material containing larger gaps. But we have had the advantage of much more powerful hardware and software. We have relied upon Isabelle's reasoning tools to Æll some of the gaps for us.

We have done this work in the spirit of the QED Project [19], which aims ™to build a computer system that effectively represents all important mathematical knowledge and techniques.∫ Our results provide evidence, both positive and negative, regarding the feasibility of QED. On the positive side, we are able to mechanise difÆcult mathematics. On the negative side, the cost of doing so is hard to predict: a short passage can cause immense difÆculties.

2 The Cardinal Proofs: Motivation and Discussion

The original reason for mechanising the theory of cardinals was to generalise Paulson's treatment of recursive data structures in ZF. The original treatment [16] permitted only Ænite branching, as in n-ary trees. Countable branching required deÆning an uncountable ordinal. We are thus led to consider branching of any cardinality.

2.1 InÆnite Branching Trees

Let κ stand for an inÆnite cardinal and κ^+ for its successor cardinal. Branching by an arbitrarily large index set I requires proving the theorem

$$\frac{|I| \leq \kappa \quad \forall_{i \in I}\, \alpha_i < \kappa^+}{\left(\bigcup_{i \in I} \alpha_i\right) < \kappa^+} \tag{1}$$

You need not understand the details of how this is used in order to follow the paper.[1]

Not many set theory texts cover such material well. Elementary texts [8, 24] never get far enough, while advanced texts such as Kunen [11] race through it. But Kunen's rapid treatment is nonetheless clear, and mentions all the essential elements. The desired result (1) follows fairly easily from Kunen's Lemma 10.21 [11, page 30]:

$$\frac{\forall_{\alpha < \kappa}\, |X_\alpha| \leq \kappa}{\left|\bigcup_{\alpha < \kappa} X_\alpha\right| \leq \kappa}$$

This, in turn, relies on the Axiom of Choice and its consequence the Well-ordering Theorem, which are discussed at length below. It also relies on a fundamental result about

[1] To understand those details, refer to Paulson [16, §3.5]. For $i \in I$ let α_i be the least α such that $i \in V[A]_\alpha$. From (1) we can prove

$$\frac{|I| \leq \kappa \quad I \subseteq V[A]_{\kappa^+}}{I \to V[A]_{\kappa^+} \subseteq V[A]_{\kappa^+}}$$

This result allows $V[A]_{\kappa^+}$ to serve as the bounding set for a least Æxedpoint deÆnition [17].

multiplication of inÆnite cardinals:

$$\kappa \otimes \kappa = \kappa.$$

This is Theorem 10.12 of Kunen. (In this paper, we refer only to his Chapter I.) The proof presents a challenging example of formalisation, as we shall see.

We could prove $A \times A \approx A$, for all inÆnite sets A, by appealing to AC in the form of Zorn's Lemma; see Halmos [8, pages 97±8]. Then $\kappa \otimes \kappa = \kappa$ would follow immediately. But we need to prove $\kappa \otimes \kappa = \kappa$ without AC in order to use it in later proofs about equivalences of AC. In fact, the law $A \times A \approx A$ is known to be equivalent to the Axiom of Choice.

Paulson hoped to prove $\kappa \otimes \kappa = \kappa$ directly, but could not Ænd a suitable proof. He therefore decided to mechanise the whole of Kunen's Chapter I, up to that theorem. We suggest this as a principle: theorems do not exist in isolation, but are part of a framework of supporting theorems. It is easier in the long run to build the entire framework, not just the parts thought to be relevant. The latter approach requires frequent, ad-hoc extensions to the framework.

2.2 Overview of Kunen, Chapter I

Kunen's Ærst chapter is entitled, ™Foundations of Set Theory.∫ Kunen remarks on page 1 that the chapter is merely a review for a reader who has already studied based set theory. This explains why the chapter is so succinct, as compared say with Halmos [8].

The Ærst four sections are largely expository. Section 5 introduces a few axioms while §6 describes the operations of Cartesian product, relations, functions, domain and range. Already, §6 goes beyond the large Isabelle/ZF theory described in earlier papers [15, 16]. That theory emphasized computational notions, such as recursive data structures, at the expense of traditional set theory. Now it was time to develop some of the missing material. Paulson introduced some deÆnitions about relations, orderings, well-orderings and order-isomorphisms, and proved the Ærst two lemmas by well-founded induction. The main theorem required a surprising amount of further work; see §3.3 below.

Kunen's §7 covers ordinals. Much of this material had already been formalized in Isabelle/ZF [16, §3.2], but using a different deÆnition of ordinal. A set A is *transitive* if $A \subseteq \mathcal{P}(A)$: every element of A is a subset of A. Kunen deÆnes an ordinal to be a transitive set that is well-ordered by $\in$, while Isabelle/ZF deÆnes an ordinal to be a transitive set of transitive sets. The two deÆnitions are equivalent provided we assume, as we do, the Axiom of Foundation.

Our work required formalizing some material from §7 concerning order types and ordinal addition. We have also formalized ordinal multiplication. But we have ignored what Kunen calls $A^{<\omega}$ because Isabelle/ZF provides $\mathrm{list}(A)$, the set of Ænite lists over A [16, §4.3] for the same purpose.

Kunen's §8 and §13 address the legitimacy of introducing new notations in axiomatic set theory. His discussion is more precise and comprehensive than Paulson's defence of the notation of Isabelle/ZF [15, page 361].

Kunen's §9 concerns classes and recursion. The main theorems of this section, justifying transÆnite induction and recursion over the class of ordinals, were already in the Isabelle/ZF library [16, §3.2,§3.4]. Kunen discusses here (and with some irony in §12) the difficulties of formalizing properties of classes. Variables in ZF range over only sets; classes are essentially predicates, so a theorem about classes must be formalized as a theorem scheme.

Many statements about classes are easily expressed in Isabelle/ZF. An ordinary class is a unary predicate, in Isabelle/ZF an object of type $i \Rightarrow o$, where i is the type of sets and o is the type of truth values. A class relation is a binary predicate and has the Isabelle type $i \Rightarrow (i \Rightarrow o)$. A class function is traditionally represented by its graph, a single-valued class predicate [11, page 25]; it is more easily formalised in Isabelle as a meta-level function, an object of type $i \Rightarrow i$. See Paulson [15, §6] for an example involving the Replacement Axiom.

Because Isabelle/ZF is built upon first-order logic, quantification over variables of types $i \Rightarrow o$, $i \Rightarrow i$, etc., is forbidden. (And it should be; allowing such quantification in uses of the Replacement Axiom would be illegitimate.) However, schematic definitions and theorems may contain free variables of such types. Isabelle/ZF's transfinite recursion operator [16, §3.4] satisfies an equation similar to Kunen's Theorem 9.3, expressed in terms of class functions.

Isabelle/ZF does not overload set operators such as $\cap$, $\cup$, domain and list to apply to classes. Overloading is possible in Isabelle, but is probably not worth the trouble in this case. And the class-oriented definitions might be cumbersome. Serious reasoning about classes might be easier in some other axiomatic framework, where classes formally exist.

Kunen's §10 concerns cardinals. Some of these results presented great difficulties and form one of the main subjects of this paper. But the Schröder-Bernstein Theorem was already formalized in Isabelle/ZF [16, §2.6], and the first few lemmas were straightforward.

An embarrassment was proving that the natural numbers are cardinals. This boils down to showing that if there is a bijection between an m-element set and an n-element set then $m = n$. Proving this obvious fact is most tiresome. Reasoning about bijections is complicated; a helpful simplification (due to M. P. Fourman) is to reason about injections instead. Prove that if there is an injection from an m-element set to an n-element set then $m \leq n$. Applying this implication twice yields the desired result.

Many intuitively obvious facts are hard to justify formally. This came up repeatedly in our proofs, and slowed our progress considerably. It is a fundamental obstacle that will probably not yield to improved reasoning tools.

Kunen proves (Theorem 10.16) that for every ordinal α there is a larger cardinal, κ. Under AC this is an easy consequence of Cantor's Theorem; without AC more work is required. Paulson slightly modified Kunen's construction, letting κ be the union of the order types of all well-orderings of subsets of α, and found a pleasingly short machine proof.

Our main concern, as mentioned above, is Kunen's proof of $\kappa \otimes \kappa = \kappa$. We shall examine the machine proof in great detail. The other theorems of Kunen's §10 concern such matters as cardinal exponentiation and cofinality. We have not mechanised these, but the only obstacle to doing so is time.

The rest of Kunen's Chapter I is mainly discussion.

3 Foundations of Cardinal Arithmetic

Let us examine the cardinal proofs in detail. We begin by reviewing the necessary definitions and theorems. Then we look at the corresponding Isabelle/ZF theories leading up to the main result, $\kappa \otimes \kappa = \kappa$. Throughout we shall concentrate on unusual aspects of the formalization, since much of it is routine.

3.1 Well-orderings

A relation $<$ is *well-founded* over a set A if it admits no inÆnite decreasing chains

$$\cdots < x_n < \cdots < x_2 < x_1$$

within A. If furthermore $\langle A, < \rangle$ is a linear ordering then we say that $<$ *well-orders* A.

A function f is an *order-isomorphism* (or just an *isomorphism*) between two ordered sets $\langle A, < \rangle$ and $\langle A', <' \rangle$ if f is a bijection between A and A' that preserves the orderings in both directions: $x < y$ if and only if $f(x) <' f(y)$ for all $x, y \in A$.

Write $\langle A, < \rangle \cong \langle A', <' \rangle$ if there exists an order-isomorphism between $\langle A, < \rangle$ and $\langle A', <' \rangle$.

If $\langle A, < \rangle$ is an ordered set and $x \in A$ then $\mathrm{pred}(A, x, <) \stackrel{\mathrm{def}}{=} \{y \in A \mid y < x\}$ is called the (proper) *initial segment* determined by x. We also speak of A itself as an initial segment of $\langle A, < \rangle$.

Kunen develops the theory of relations in his §6 and proves three fundamental properties of well-orderings:

- There can be no isomorphism between a well-ordered set and a proper initial segment of itself. A useful corollary is that if two initial segments are isomorphic to each other, then they are equal.
- There can be at most one isomorphism between two well-ordered sets. This result sounds important, but we have never used it.[2]
- Any two well-orderings are either isomorphic to each other, or else one of them is isomorphic to a proper initial segment of the other.

Kunen's proof of the last property consists of a single sentence:

> Let $f =$
>
> $$\{\langle v, w \rangle \mid v \in A \wedge w \in B \wedge \langle \mathrm{pred}(A, v, <_A) \rangle \cong \langle \mathrm{pred}(B, w, <_B) \rangle\};$$
>
> note that f is an isomorphism from some initial segment of A onto some initial segment of B, and that these initial segments cannot both be proper.

This gives the central idea concisely; Suppes [24, pages 233±4] gives a much longer proof that is arguably less clear. However, the assertions Kunen makes are not trivial and Paulson needed two days and a half to mechanise the proof.

[2] Kunen gives straightforward inductive proofs of these Ærst two properties. But Halmos [8, page 72] gives an argument that proves both with a single induction.

3.2 Order Types

The ordinals may be viewed as representatives of the well-ordered sets. Every ordinal is well-ordered by the membership relation $\in$. What is more important, every well-ordered set is isomorphic to a unique ordinal, called its *order type* and written $\mathrm{type}(A, <)$. Kunen [11, page 17] proves this by a direct construction. But to mechanise the result in Isabelle/ZF, it is easier to use well-founded recursion [16, §3.4]. If $\langle A, < \rangle$ is a well-ordering, deÆne a function f on A by the recursion

$$f(x) = \{f(y) \mid y < x\}$$

for all $x \in A$. Then

$$\mathrm{type}(A, <) \stackrel{\text{def}}{=} \{f(x) \mid x \in A\}.$$

It is straightforward to show that f is an isomorphism between $\langle A, < \rangle$ and $\mathrm{type}(A, <)$, which is indeed an ordinal.

Our work has required proving many properties of order types, such as methods for calculating them in particular cases. Our source material contains few such proofs; we have spent much time re-discovering them.

3.3 Combining Well-orderings

Let $A + B \stackrel{\text{def}}{=} (\{0\} \times A) \cup (\{1\} \times B)$ stand for the disjoint sum of A and B, which is formalised in Isabelle/ZF [16, §4.1]. Let $\langle A, <_A \rangle$ and $\langle B, <_B \rangle$ be well-ordered sets. The order types of certain well-orderings of $A + B$ and $A \times B$ are of key importance.

The sum $A + B$ is well-ordered by a relation $<$ that combines $<_A$ and $<_B$, putting the elements of A before those of B. It satisÆes the following rules:

$$\frac{a' <_A a}{\mathrm{Inl}(a') < \mathrm{Inl}(a)} \qquad \frac{b' <_B b}{\mathrm{Inr}(b') < \mathrm{Inr}(b)} \qquad \frac{a \in A \quad b \in B}{\mathrm{Inl}(a) < \mathrm{Inr}(b)}$$

The product $A \times B$ is well-ordered by a relation $<$ that combines $<_A$ and $<_B$, lexicographically:

$$\frac{a' <_A a \quad b', b \in B}{\langle a', b' \rangle < \langle a, b \rangle} \qquad \frac{a \in A \quad b' <_B b}{\langle a, b' \rangle < \langle a, b \rangle}$$

The well-orderings of $A + B$ and $A \times B$ are traditionally used to deÆne the ordinal sum and product. We do not require ordinal arithmetic until we come to the proofs from Rubin and Rubin. But we require the well-orderings themselves in order to prove $\kappa \otimes \kappa = \kappa$. That proof requires yet another well-ordering construction: *inverse image*.

If $\langle B, <_B \rangle$ is an ordered set and f is a function from A to B then deÆne $<_A$ by

$$x <_A y \leftrightarrow f(x) <_B f(y).$$

Clearly $<_A$ is well-founded if $<_B$ is. If f is injective and $<_B$ is a well-ordering then $<_A$ is also a well-ordering. If f is bijective then obviously f is an isomorphism between the orders $\langle A, <_A \rangle$ and $\langle B, <_B \rangle$; it follows that their order types are equal.

Sum, product and inverse image are useful building blocks for well-orderings; this follows Paulson's earlier work [14] within Constructive Type Theory.

```
Cardinal = OrderType + Fixedpt + Nat + Sum +
consts
  Least            :: "(i=>o) => i"    (binder "LEAST " 10)
  eqpoll, lepoll,
          lesspoll :: "[i,i] => o"     (infixl 50)
  cardinal         :: "i=>i"           ("|_|")
  Finite, Card     :: "i=>o"

defs
  Least_def     "Least(P) == THE i. Ord(i) & P(i) &
                                (ALL j. j<i --> ƒP(j))"
  eqpoll_def    "A eqpoll B == EX f. f: bij(A,B)"
  lepoll_def    "A lepoll B == EX f. f: inj(A,B)"
  lesspoll_def  "A lesspoll B == A lepoll B & ƒ(A eqpoll B)"
  Finite_def    "Finite(A) == EX n:nat. A eqpoll n"
  cardinal_def  "|A| == LEAST i. i eqpoll A"
  Card_def      "Card(i) == (i = |i|)"
end
```

Figure 1: Isabelle/ZF Theory DeÆning the Cardinal Numbers

3.4 Cardinal Numbers

Figure 1 presents the Isabelle/ZF deÆnitions of cardinal numbers, following Kunen's §10. The Isabelle theory Æle extends some Isabelle theories (`OrderType` and others) with constants, which stand for operators or predicates. The constants are deÆned essentially as follows:

- The least ordinal α such that $P(\alpha)$ is deÆned by a unique description [15, pages 366±7] and may be written `LEAST` α . $P(\alpha)$.
- Two sets A and B are *equipollent* if there exists a bijection between them. Write $A \approx B$ or, in Isabelle, A `eqpoll` B.
- B *dominates* A if there exists an injection from A into B. Write $A \precsim B$ or A `lepoll` B.
- B *strictly dominates* A if $A \precsim B$ and $A \not\approx B$. Write $A \prec B$ or A `lesspoll` B.
- A set is *Ænite* if it is equipollent to a natural number.
- The *cardinality* of A, written $|A|$, is the least ordinal equipollent to A. Without AC, no such ordinal has to exist; we might then regard $|A|$ as undeÆned. But everything is deÆned in Isabelle/ZF. An ™undeÆned∫ cardinality equals 0; this conveniently ensures that $|A|$ is always an ordinal.
- A set i is a *cardinal* if $i = |i|$; write $\mathrm{Card}(i)$.

Reasoning from these deÆnitions is entirely straightforward except for the ™obvious∫ facts about Ænite cardinals mentioned above.

3.5 Cardinal Arithmetic

Let κ, λ, μ range over Ænite or inÆnite cardinals. Cardinal sum and product are deÆned in terms of disjoint sum and Cartesian product:

$$\kappa \oplus \lambda \stackrel{\text{def}}{=} |\kappa + \lambda|$$
$$\kappa \otimes \lambda \stackrel{\text{def}}{=} |\kappa \times \lambda|$$

These satisfy the familiar commutative, associative and distributive laws. The proofs are uninteresting but non-trivial, especially as we work without AC. We do so in order to use the results in proving various forms of AC to be equivalent (see below); but frequently this forces us to construct well-orderings explicitly.

4 Proving $\kappa \otimes \kappa = \kappa$

We begin with an extended discussion of Kunen's proof and then examine its formalisation.

4.1 Kunen's Proof

Kunen calls this result Theorem 10.12. His proof is admirably concise.

> **Theorem.** If κ is an inÆnite cardinal then $\kappa \otimes \kappa = \kappa$.
>
> **Proof.** By transÆnite induction on κ. Assume this holds for smaller cardinals. Then for $\alpha < \kappa$, $|\alpha \times \alpha| = |\alpha| \otimes |\alpha| < \kappa$ (applying Lemma 10.10 when α is Ænite)[3]. DeÆne a well-ordering $\lhd$ 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
>
> $$|\mathrm{succ}(\max(\alpha, \beta)) \times \mathrm{succ}(\max(\alpha, \beta))| < \kappa$$
>
> predecessors in $\lhd$, so $\mathrm{type}(\kappa \times \kappa, \lhd) \le \kappa$, whence $|\kappa \times \kappa| \le \kappa$. Since clearly $|\kappa \times \kappa| \ge \kappa$, $|\kappa \times \kappa| = \kappa$.

The key to the proof is the ordering $\lhd$, whose structure may be likened to that of a square onion. Let α and β be ordinals such that $\beta \le \alpha < \kappa$. The predecessors of $\langle \alpha, \beta \rangle$ include all pairs of the form $\langle \alpha, \beta' \rangle$ for $\beta' < \beta$, and all pairs of the form $\langle \alpha', \alpha \rangle$ for $\alpha' < \alpha$; these pairs constitute the α^{th} layer of the onion. The other predecessors of $\langle \alpha, \beta \rangle$ are pairs of the form $\langle \gamma, \delta \rangle$ such that $\gamma, \delta < \alpha$; these pairs constitute the inner layers of the onion. (See Figure 2.)

The set of all $\lhd$-predecessors of $\langle \alpha, \beta \rangle$ is a subset of $\mathrm{succ}(\alpha) \times \mathrm{succ}(\alpha)$, which gives an upper bound on its cardinality. Kunen expresses this upper bound in terms of $\max(\alpha, \beta)$ to avoid having to assume $\beta \le \alpha$.

[3] Lemma 10.10 says that multiplication of Ænite cardinals agrees with integer multiplication.

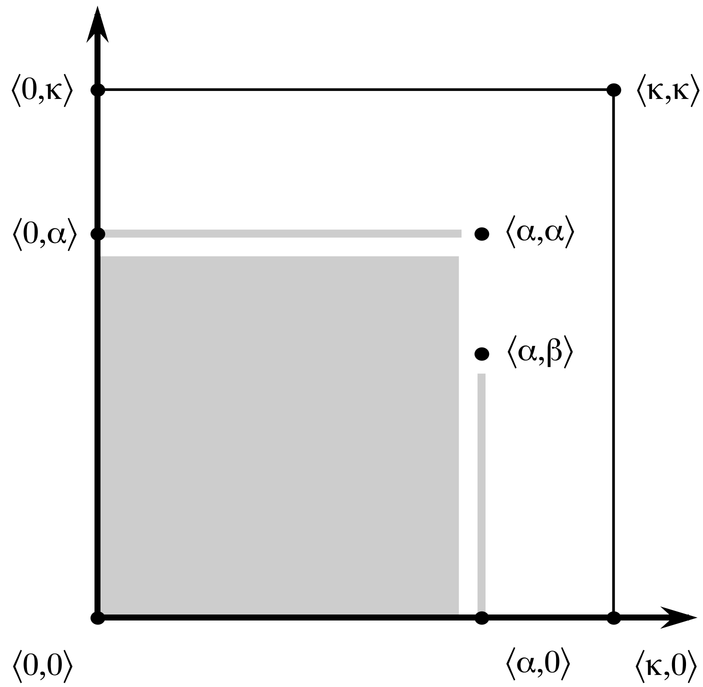

Figure 2: Predecessors of $\langle \alpha, \beta \rangle$, with $\beta \leq \alpha$

To simplify the formal proofs, Paulson used the more generous upper bound

$$|\mathrm{succ}(\mathrm{succ}(\max(\alpha, \beta))) \times \mathrm{succ}(\mathrm{succ}(\max(\alpha, \beta)))| \; .$$

This is still a cardinal below κ. As Kunen notes, there are two cases. If α or β is inÆnite then $\mathrm{succ}(\mathrm{succ}(\max(\alpha, \beta))) < \kappa$ because $\max(\alpha, \beta) < \kappa$ and because inÆnite cardinals are closed under successor; therefore, the inductive hypothesis realizes our claim. If α and β are both Ænite, then so is $\mathrm{succ}(\mathrm{succ}(\max(\alpha, \beta)))$, while κ is inÆnite by assumption.

To complete the proof, we must examine the second half of Kunen's sentence: ™so $\mathrm{type}(\kappa \times \kappa, \lhd) \leq \kappa$, whence $|\kappa \times \kappa| \leq \kappa$.∫ Recall from §3.2 that there is an isomorphism

$$f : \kappa \times \kappa \to \mathrm{type}(\kappa \times \kappa, \lhd)$$

such that

$$f(\alpha, \beta) = \{ f(\gamma, \delta) \mid \langle \gamma, \delta \rangle \lhd \langle \alpha, \beta \rangle \}.$$

Thus, $f(\alpha, \beta)$ is an ordinal with the same cardinality as the set of predecessors of $\langle \alpha, \beta \rangle$. This implies $f(\alpha, \beta) < \kappa$ for all $\alpha, \beta < \kappa$, and therefore $\mathrm{type}(\kappa \times \kappa, \lhd) \leq \kappa$. Because f is a bijection between $\kappa \times \kappa$ and $\mathrm{type}(\kappa \times \kappa, \lhd)$, we obtain $|\kappa \times \kappa| \leq \kappa$. The opposite inequality is trivial.

4.2 Mechanising the Proof

Proving $\kappa \otimes \kappa = \kappa$ requires formalising the relation $\lhd$. Kunen's deÆnition looks complicated, but we can get the same effect using our well-ordering constructors (recall §3.3).

```
CardinalArith = Cardinal + OrderArith + Arith + Finite +
consts
  InfCard       :: "i=>o"
  "|*|"         :: "[i,i]=>i"       (infixl 70)
  "|+|"         :: "[i,i]=>i"       (infixl 65)
  csquare_rel   :: "i=>i"

defs
  InfCard_def  "InfCard(i) == Card(i) & nat le i"
  cadd_def     "i |+| j == |i+j|"
  cmult_def    "i |*| j == |i*j|"

  csquare_rel_def
  "csquare_rel(K) ==
   rvimage(K*K,
           lam <x,y>:K*K. <x Un y, x, y>,
           rmult(K,Memrel(K), K*K, rmult(K,Memrel(K),K,Memrel(K))))"
end
```

Figure 3: Isabelle/ZF Theory File for Cardinal Arithmetic

Note that $\lhd$ is an inverse image of the lexicographic well-ordering of $\kappa \times \kappa \times \kappa$, under the function $g : \kappa \times \kappa \to \kappa \times \kappa \times \kappa$ deÆned by

$$g(\alpha, \beta) = \langle \max(\alpha, \beta), \alpha, \beta \rangle;$$

this function is trivially injective.

Figure 3 presents part of the Isabelle theory Æle for cardinal arithmetic. It deÆnes $\lhd$ as the constant `csquare_rel`. Here is a summary of the operators appearing in its deÆnition:

- `rvimage`$(A, f, <)$ is the inverse image ordering on A derived from $<$ by f.
- `lam <x,y>:K*K. <x Un y, x, y>` is the function called g above. The pattern-matching in the abstraction expands internally to the constant `split`, which takes apart ordered pairs [15, page 367]. Finally `Un` denotes union; note that $\max(\alpha, \beta) = \alpha \cup \beta$ for ordinals α and β.
- `rmult`$(A, <_A, B, <_B)$ constructs the lexicographic ordering on $A \times B$ from the orderings $<_A$ and $<_B$.
- `Memrel`(κ) is the membership relation on κ. This is the primitive well-ordering for ordinals.

Proving that `csquare_rel` is a well-ordering is easy, thanks to lemmas about `rvimage` and `rmult`. A single command proves that our map is injective.

Figure 4 presents the nine theorems that make up the Isabelle/ZF proof of $\kappa \otimes \kappa = \kappa$. The theorems are stated literally in Isabelle notation. There is not enough space to present the proofs, which comprise over sixty Isabelle tactic commands; see Paulson [15, §8] for demonstrations of Isabelle/ZF tactics. The nine proofs require a total of 43 seconds to run.[4]

[4] All Isabelle timings are on a Sun SPARCstation ELC.

```
1  Ord(K) ==>
   (lam z:K*K. SPLIT(%x y. <x Un y, <x, y>>, z)) : inj(K*K, K*K*K)

2  Ord(K) ==> well_ord(K*K, csquare_rel(K))

3  [| x<K;  y<K;  z<K;  <<x,y>, <z,z>> : csquare_rel(K) |] ==>
   x le z & y le z

4  z<K ==> pred(K*K, <z,z>, csquare_rel(K)) <= succ(z)*succ(z)

5  [| x<z;  y<z;  z<K |] ==> <<x,y>, <z,z>> : csquare_rel(K)

6  [| InfCard(K);  x<K;  y<K;  z=succ(x Un y) |] ==>
   ordermap(K*K, csquare_rel(K)) ` <x,y>  <
   ordermap(K*K, csquare_rel(K)) ` <z,z>

7  [| InfCard(K);  x<K;  y<K;  z=succ(x Un y) |] ==>
   |ordermap(K*K, csquare_rel(K)) ` <x,y>| le |succ(z)| |*| |succ(z)|

8  [| InfCard(K);  ALL y:K. InfCard(y) --> y |*| y = y |]  ==>
   ordertype(K*K, csquare_rel(K)) le K

9  InfCard(K) ==> K |*| K = K
```

Figure 4: Theorems for the Proof of $\kappa \otimes \kappa = \kappa$

The Ærst few theorems concern elementary properties of `csquare rel`(κ). We Ænd that it is a well-ordering of κ (theorems 1, 2) and that the initial segment below ξ, for $\xi < \kappa$, is a subset of $\mathrm{succ}(\xi) \times \mathrm{succ}(\xi)$ (theorems 3, 4). The next three theorems (5, 6, 7) form part of the proof that κ is the order type of `csquare_rel`(κ). The isomorphism called f in §4.1 is written in Isabelle/ZF as

```
ordermap(K*K, csquare_rel(K)).
```

If $\alpha, \beta < \kappa$ then, setting $\xi = \mathrm{succ}(\mathrm{succ}(\max(\alpha, \beta)))$, we obtain $f(\alpha, \beta) \precsim f(\xi, \xi)$ and thus, via theorem 4, we have $|f(\alpha, \beta)| \leq |\xi| \otimes |\xi|$.

Theorem 7 corresponds to the Ærst part of Kunen's sentence, ™Each $\langle \alpha, \beta \rangle \in \kappa \times \kappa$ has no more than $|\mathrm{succ}(\max(\alpha, \beta)) \times \mathrm{succ}(\max(\alpha, \beta))|$ predecessors in $\lhd$∫ and it took about a day to prove. Theorem 8 covers the next part of the sentence, ™so $\mathrm{type}(\kappa \times \kappa, \lhd) \leq \kappa$∫ and took another day to prove. This theorem assumes the transÆnite induction hypothesis in order to verify $|\mathrm{succ}(\xi)| \otimes |\mathrm{succ}(\xi)| \leq \kappa$ in the case when ξ is inÆnite, checking the Ænite case separately. At 17 tactic steps, the proof is the most complicated of the nine theorems. The main result, theorem 9, merely sets up the transÆnite induction and appeals to the previous theorems.

Kunen uses without proof the analogous result for addition of inÆnite cardinals, $\kappa \oplus \kappa = \kappa$. We could prove it using an argument like the one above, but with an ordering of $\kappa + \kappa$ instead of $\kappa \times \kappa$. Fortunately there is a much simpler proof, combining the trivial $\kappa \leq \kappa \oplus \kappa$ with the chain of inequalities $\kappa \oplus \kappa = 2 \otimes \kappa \leq \kappa \otimes \kappa = \kappa$. Formalized mathematics requires discovering such simple proofs whenever possible.

The effort required to prove $\kappa \otimes \kappa = \kappa$ includes not only the several days spent formalising the few sentences of Kunen's proof, but also the weeks spent developing a library of results about orders, well-orderings, isomorphisms, order types, cardinal numbers and basic cardinal arithmetic. After proving the theorem, more work was required to complete the theoretical foundation for inÆnite branching trees (recall our original motivation, §2.1). Fortunately, we have been able to re-use the libraries for proofs about AC. This we turn to next.

5 Rubin and Rubin's AC Proofs

Herman and Jean Rubin's book *Equivalents of the Axiom of Choice* [21] is a compendium of hundreds of statements equivalent to the Axiom of Choice. Many of these statements were used originally as formulations of AC; others, of independent interest, were found to be equivalent to AC. Each chapter of the book focusses on a particular framework for formulating AC. Chapter 1 discusses equivalent forms of the Well-Ordering Theorem. Chapter 2 discusses the Axiom of Choice itself. Other chapters cover the Trichotomy Law, cardinality formulations, etc.

Grà bczewski has mechanized the Ærst two chapters, both deÆnitions and proofs. He has additionally proved the equivalence of all the formulations given; the book omits the ™easy∫ proofs and a few of the harder ones. Below we outline the deÆnitions and some of the more interesting proofs.

This is a substantial piece of work. There are 55 deÆnitions, mostly names of the formulations of AC. There are nearly 1900 tactic commands. The full development takes over 44 minutes run.[5]

5.1 The Well-Ordering Theorem

The eight equivalent forms of the Well-Ordering Theorem are the following:

WO_1 Every set can be well-ordered.

WO_2 Every set is equipollent to an ordinal number.

WO_3 Every set is equipollent to a subset of an ordinal number.

$\mathrm{WO}_4(m)$ For every set x there exists an ordinal α and a function f deÆned on α such that $f(\beta) \precsim m$ for every $\beta < \alpha$ and $\bigcup_{\beta<\alpha} f(\beta) = x$.

WO_5 There exists a natural number $m \geq 1$ such that $\mathrm{WO}_4(m)$.

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

WO_7 For every set x, x is Ænite iff for each well-ordering R of x, R^1 also well-orders x.

WO_8 Every set possessing a choice function can be well-ordered.

[5] Such Ægures can be regarded only as a rough guide. Many of the theorems properly belong in the main libraries. Small changes to searching commands can have a drastic effect on the run time. For comparison, the main ZF library (which includes the Kunen, Abrial and LafÆtte proofs) contains 150 deÆnitions and nearly 3300 tactic commands.

```
WO1_def "WO1 == ALL A. EX R. well_ord(A,R)"

WO2_def "WO2 == ALL A. EX a. Ord(a) & A eqpoll a"

WO3_def "WO3 == ALL A. EX a. Ord(a) & (EX b. b <= a & A eqpoll b)"

WO4_def "WO4(m) == ALL A. EX a f. Ord(a) & domain(f)=a &
                   (UN b<a. f`b) = A & (ALL b<a. f`b lepoll m)"

WO5_def "WO5 == EX m:nat. 1 le m & WO4(m)"

WO6_def "WO6 == ALL A. EX m:nat. 1 le m & (EX a f. Ord(a) &
                  domain(f)=a & (UN b<a. f`b) = A &
                  (ALL b<a. f`b lepoll m))"

WO7_def "WO7 == ALL A. Finite(A) <-> (ALL R. well_ord(A,R) -->
                  well_ord(A,converse(R)))"

WO8_def "WO8 == ALL A. (EX f. f : (PROD X:A. X)) -->
                  (EX R. well_ord(A,R))"
```

Figure 5: Isabelle/ZF DeÆnitions of Well-Ordering Principles

Most of Chapter 1 is devoted to proving $\mathrm{WO}_6 \Longrightarrow \mathrm{WO}_1$, which is by far the hardest of the results. GrÀbczewski has proved the equivalence of all the formulations given above by means of the following implications:

$$\mathrm{WO}_1 \Longrightarrow \mathrm{WO}_2 \Longrightarrow \mathrm{WO}_3 \Longrightarrow \mathrm{WO}_1$$
$$\mathrm{WO}_4(m) \Longrightarrow \mathrm{WO}_4(n) \quad \text{if } m \le n$$
$$\mathrm{WO}_4(n) \Longrightarrow \mathrm{WO}_5 \Longrightarrow \mathrm{WO}_6 \Longrightarrow \mathrm{WO}_1 \Longrightarrow \mathrm{WO}_4(1)$$
$$\mathrm{WO}_7 \iff \mathrm{WO}_1$$
$$\mathrm{WO}_8 \iff \mathrm{WO}_1$$

Figure 5 shows how these axioms are formalized in Isabelle.

5.2 The Axiom of Choice

The formulations of the Axiom of Choice are as follows:

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

AC_2 If A is a set of non-empty, pairwise disjoint sets, then there is a set C whose intersection with any member B of A has exactly one element.

AC_3 For every function f there is a function g such that for every x, if $x \in \mathrm{dom}(f)$ and $f(x) \neq 0$, then $g(x) \in f(x)$.

AC_4 For every relation R there is a function $f \subseteq R$ such that $\mathrm{dom}(f) = \mathrm{dom}(R)$.

AC_5 For every function f there is a function g such that $\mathrm{dom}(g) = \mathrm{rng}(f)$ and $f(g(x)) = x$ for every $x \in \mathrm{dom}(g)$.

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

AC_7 The Cartesian product of a set of non-empty sets of the same cardinality is non-empty.

AC_8 If A is a set of pairs of equipollent sets, then there is a function which associates with each pair a bijection mapping one onto the other.

AC_9 If A is a set of sets of the same cardinality, then there is a function which associates with each pair a bijection mapping one onto the other.

$\mathrm{AC}_{10}(n)$ If A is a set of sets of inÆnite sets, then there is a function f such that for each $x \in A$, the set $f(x)$ is a decomposition of x into disjoint sets of size between 2 and n.

AC_{11} There exists a natural number $n \geq 2$ such that $\mathrm{AC}_{10}(n)$.

AC_{12} If A is a set of sets of inÆnite sets, then there is a natural number $n \geq 2$ and a function f such that for each $x \in A$, the set $f(x)$ is a decomposition of x into disjoint sets of size between 2 and n.

$\mathrm{AC}_{13}(m)$ If A is a set of non-empty sets, then there is a function f such that for each $x \in A$, the set $f(x)$ is a non-empty subset of x with $f(x) \precsim m$.

AC_{14} There is a natural number $m \geq 1$ such that $\mathrm{AC}_{13}(m)$.

AC_{15} If A is a set of non-empty sets, then there is a natural number $m \geq 1$ and a function f such that for each $x \in A$, the set $f(x)$ is a non-empty subset of x with $f(x) \precsim m$.

$\mathrm{AC}_{16}(n,k)$ If A is an inÆnite 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.

AC_{17} If A is a set, $B = \mathcal{P}(A) - \{0\}$ and g is a function from $B \to A$ to B, then there is a function $f \in B \to A$ such that $f(g(f)) \in g(f)$.

AC_{18} For every non-empty set A, every family of non-empty sets $\{B_a \mid a \in A\}$ and every family of sets $\{X_{a,b} \mid a \in A,\ b \in B_a\}$, there holds[6]

$$\bigcap_{a \in A} \bigcup_{b \in B_a} X_{a,b} = \bigcup_{f \in \prod_{a \in A} B_a} \bigcap_{a \in A} X_{a,f(a)}.$$

AC_{19} For any non-empty set A, each of whose elements is non-empty,

$$\bigcap_{a \in A} \bigcup_{b \in a} b = \bigcup_{f \in C(A)} \bigcap_{a \in A} f(a),$$

where $C(A)$ is the set of all choice functions on A.

[6] Rubin and Rubin [21, page 9] state this incorrectly. They quantify over B but leave X free in the deÆniens.

GraÀbczewski has mechanised the following proofs in Isabelle:

$$\mathrm{AC}_1 \iff \mathrm{AC}_2 \qquad \mathrm{AC}_4 \iff \mathrm{AC}_5$$
$$\mathrm{AC}_1 \iff \mathrm{AC}_6 \qquad \mathrm{AC}_6 \iff \mathrm{AC}_7$$
$$\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_4 \Longrightarrow \mathrm{AC}_3 \Longrightarrow \mathrm{AC}_1$$
$$\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_8 \Longrightarrow \mathrm{AC}_9 \Longrightarrow \mathrm{AC}_1$$
$$\mathrm{WO}_1 \Longrightarrow \mathrm{AC}_1 \Longrightarrow \mathrm{WO}_2$$
$$\mathrm{WO}_1 \Longrightarrow \mathrm{AC}_{10}(n) \Longrightarrow \mathrm{AC}_{11} \Longrightarrow \mathrm{AC}_{12} \Longrightarrow \mathrm{AC}_{15} \Longrightarrow \mathrm{WO}_6$$
$$\mathrm{AC}_{10}(n) \Longrightarrow \mathrm{AC}_{13}(n-1) \qquad \mathrm{AC}_{13}(n) \Longrightarrow \mathrm{AC}_{14} \Longrightarrow \mathrm{AC}_{15}$$
$$\mathrm{AC}_{11} \Longrightarrow \mathrm{AC}_{14}$$
$$\mathrm{AC}_{13}(m) \Longrightarrow \mathrm{AC}_{13}(n) \quad \text{if } m \leq n$$
$$\mathrm{AC}_1 \iff \mathrm{AC}_{13}(1) \qquad \mathrm{AC}_1 \iff \mathrm{AC}_{17}$$
$$\mathrm{WO}_2 \Longrightarrow \mathrm{AC}_{16}(n,k) \Longrightarrow \mathrm{WO}_4(n-k)$$
$$\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_{18} \Longrightarrow \mathrm{AC}_{19} \Longrightarrow \mathrm{AC}_1$$

Chains such as $\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_4 \Longrightarrow \mathrm{AC}_3 \Longrightarrow \mathrm{AC}_1$ require fewer proofs than proving equivalence for every pair of deÆnitions. We have occasionally deviated from Rubin and Rubin in order to form such chains. We have proved $\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_4$ to avoid having to prove $\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_3$ and $\mathrm{AC}_3 \Longrightarrow \mathrm{AC}_4$. Similarly we have proved $\mathrm{AC}_8 \Longrightarrow \mathrm{AC}_9$ instead of $\mathrm{AC}_8 \Longrightarrow \mathrm{AC}_1$ and $\mathrm{AC}_1 \Longrightarrow \mathrm{AC}_9$. Our new proofs are based on ideas from the text.

Creating one giant chain would minimize the number of proofs, but not necessarily the amount of effort required. In any event, we wished to avoid major deviations from Rubin and Rubin.

5.3 DifÆculties with the DeÆnitions

Although the idea of this study was to reproduce the original proofs faithfully, we sometimes changed basic deÆnitions in order to simplify the Isabelle proofs.

A fundamental concept is that of a *well-ordering*. The Rubins state that a set A is well-ordered by a relation R if A is partially ordered by R, and every non-empty subset of A has an R-Ærst element; they deÆne a partial ordering to be transitive, antisymmetric and reØexive. Isabelle/ZF deÆnes a well-ordering to be a total ordering that is well-founded, and hence irreØexive. Fortunately there was no need to deÆne well-ordering once again. ReØexivity does not play a major role in the Rubins' proofs, which remain valid under the Isabelle deÆnitions. Thus, we may take advantage of the many theorems about well-ordered sets previously proved in Isabelle/ZF.

Another difference is the deÆnition of ordinal numbers. Rubin and Rubin use essentially the same deÆnition as Kunen does; recall §2.2. We tackle this problem by proving that their deÆnition follows from the Isabelle/ZF one.

The Rubins use $A \prec B$ without deÆning it. Fortunately, its deÆnition is standard; see §3.4 for its Isabelle formalization.

Some proofs rely on the notion of an *initial ordinal*. However, an initial ordinal is precisely a cardinal number, as previously formalized in Isabelle. After proving the appropriate equivalence we decided to use cardinals.

5.4 General Comments on the Proofs

We are aiming to reproduce the spirit, not the letter, of the original material. For instance, we have changed ™$P(m) \implies P(m-1)$ for all $m \geq 1$∫ to ™$P(\mathrm{succ}(m)) \implies P(m)$ for all m.∫ Such changes streamline the formalisation without affecting the ideas.

Most of the implications concerning the Well-Ordering Theorem are easy to prove using Isabelle. Rubin and Rubin describe some of them as ™clear.∫ They do not prove the implication $\mathrm{WO}_1 \implies \mathrm{WO}_2$, but cite an external source instead. This implication is trivial with the help of Isabelle's theory of order types (recall §3.2).

It is easy to see that WO_7 is equivalent to the statement

> If x is inÆnite, then there exists a relation R such that R well-orders x but R^{-1} does not.

The Rubins observe (page 5) that this is equivalent to the Well-Ordering Theorem because every transÆnite ordinal is well-ordered by $<$ (the membership relation) and not by $>$ (its converse). To turn this observation into a proof, we need to extend it to every well-ordered set. It is enough to prove that if a set x is well-ordered by a relation R and its converse, then its order type (determined by R) is well-ordered by $>$; this is contradiction if x is inÆnite. Again we exploit Isabelle order types and ordinal isomorphisms.

Rubin and Rubin's proof of $\mathrm{AC}_7 \implies \mathrm{AC}_6$ (page 12) fails in the case of the empty family of sets. The proof of $\mathrm{AC}_{19} \implies \mathrm{AC}_1$ (page 18) fails for a similar reason. When building a mechanised proof we are obliged to treat degenerate cases, however trivial they are.

The proof of $\mathrm{AC}_9 \implies \mathrm{AC}_1$ (page 14) has a small omission. We start with a set s of non-empty sets, and deÆne $y \stackrel{\mathrm{def}}{=} (\cup s)^\omega$. It can be proved that for each $x \in s$, $x \times y \approx y$. Then Rubin and Rubin claim ™it is easy to see that for each $x \in s$, $x \times y \approx (x \times y) \cup \{0\}$.∫ But if $s = \{\{b\}\}$ then x and y are unit sets ($\{b\}$ and $\{b\}^\omega$, respectively) and the claim fails. In order to mechanise this proof we have used $x \times y \times \omega$ instead of $x \times y$. This seems simpler than handling the degenerate case separately.

On page 14, Rubin and Rubin set out to prove that AC_{10} to AC_{15} are equivalent to the Axiom of Choice. They describe a number of implications as ™clear.[7]∫ Then they list some implications that they are going to prove. It appears that they intend to establish two chains

$$\begin{gathered}\mathrm{WO}_1 \implies \mathrm{AC}_{10}(n) \implies \mathrm{AC}_{11} \implies \mathrm{AC}_{12} \implies \mathrm{AC}_{15} \implies \mathrm{WO}_6 \\ \mathrm{AC}_{13}(n) \implies \mathrm{AC}_{14} \implies \mathrm{AC}_{15}\,.\end{gathered}$$

Because of other results, it only remains to show that AC implies $\mathrm{AC}_{13}(n)$. We could prove

$$\mathrm{AC}_1 \implies \mathrm{AC}_{13}(1) \qquad \mathrm{AC}_{13}(m) \implies \mathrm{AC}_{13}(n) \quad \text{if } m \leq n$$

or, more directly, $\mathrm{AC}_{10}(n) \implies \mathrm{AC}_{13}(n-1)$. In this welter of results, Rubin and Rubin have stated and we have mechanised more proofs than are strictly required.

[7] At least one of these, $\mathrm{WO}_1 \implies \mathrm{AC}_{10}(n)$, is non-trivial. We have to partition the inÆnite set x into a set of disjoint 2-element sets, for all $x \in A$. Our proof uses the equation $\kappa = \kappa \oplus \kappa$ to establish a bijection h between the disjoint sum $|x| + |x|$ and x. The partition contains $\{h(\mathrm{Inl}(\alpha)), h(\mathrm{Inr}(\alpha))\}$ for all $\alpha < |x|$.

Another noteworthy proof (page 15) concerns the implication $\mathrm{WO}_2 \implies \mathrm{AC}_{16}$. Rubin and Rubin devote just over half a page to it, but mechanising it took a long time. Near the beginning of the proof they note that if s is an inÆnite set equipollent to a cardinal number ω_α then for all $k > 1$ the set of all k-element subsets of s is also equipollent to ω_α. Demonstrating this is non-trivial, requiring among other things the theorem $\kappa \otimes \kappa = \kappa$ discussed above in this paper.

The next and key step is a recursive construction of a set $t = \bigcup_{\gamma<\omega_\alpha} T_\gamma$ satisfying AC_{16}. Now T_γ is an increasing family of sets of n-element subsets of s. At every stage we add at most one subset. The authors claim that at any stage $\gamma < \omega_\alpha$ we can choose $n-k$ distinct elements of the set $s - (\bigcup T_\gamma \cup k_\gamma)$ where k_γ is a k-element subset of s. They may regard this claim as obvious but we found it decidedly not so.

The difÆculty of this proof lies in the complexity of the recursive deÆnition of T_γ which furthermore contains a typographical error.[8] Formalising the deÆnition was simple, but proving that it satisÆed the desired property required handling theorems with many syntactically complex premises. We changed the deÆnition several times so as to simplify these proofs.

5.5 The Axiom of Dependent Choice

At the end of Chapter 2, Rubin and Rubin present two formulations of another axiom, Dependent Choice:

$\mathrm{DC}(\alpha)$: If R is a relation between subsets and elements of a set X such that $y \prec \alpha \to \exists_{u\in X}\, y\, R\, u$ for all $y \subseteq X$ then there is a function $f \in \alpha \to X$ such that $f``\beta\, R\, f(\beta)$ for every $\beta < \alpha$.

DC: If R is a non-empty relation such that $\mathrm{rng}(R) \subseteq \mathrm{dom}(R)$ then there is a function f with domain ω such that $f(n)\, R\, f(n+1)$ for every $n < \omega$.

They then comment ™It is easy to see that $\mathrm{DC} \iff \mathrm{DC}(\omega)$.∫ But the only proof we could Ænd is complicated; mechanising it required over 200 commands. That is four times the number required for the two theorems proved explicitly.

Consider the proof of $\mathrm{DC} \to \mathrm{DC}(\omega)$. Let $R \subseteq \mathcal{P}(X) \times X$ satisfy the hypothesis of $\mathrm{DC}(\omega)$. Construct a set X' and a relation R' by[9]

$$X' = \bigcup_{n\in\omega} \{f \in n \to X \mid \forall_{k\in n}\; f``k\, R\, f(k)\}$$

$$f\, R\, g \iff \mathrm{dom}(g) = \mathrm{dom}(f) + 1 \text{ and } g \restriction \mathrm{dom}(f) = f\,. \qquad (f, g \in X')$$

It is easy to see that these satisfy the hypotheses of DC, which thus yields a function $f' \in \omega \to X'$ such that $f'(n)\, R'\, f'(n{+}1)$ for $n \in \omega$. The desired function $f \in \omega \to X$ is now deÆned by

$$f(n) = f'(n+1)(n).$$

A similar construction yields the converse.

The Rubins then prove, Theorem 2.20, that the Axiom of Choice (in fact, WO_1) implies $\mathrm{DC}(\alpha)$ for every ordinal α. While mechanising this theorem we noticed that

[8] At the beginning of the Æfth line from the bottom on page 15, $y \in N$ occurs instead of $y \in T_\gamma$.

[9] Here $g \restriction \mathrm{dom}(f)$ means g restricted to the domain of f.

it is incorrect: the quantiÆcation should be restricted to cardinals. If α is not a cardinal then $\mathrm{DC}(\alpha)$ fails.

Here is a short proof of $\neg\mathrm{DC}(\omega+1)$. Let $X = \omega$ and deÆne R by

$$y\,R\,u \iff y \subseteq X, y \prec \omega+1 \text{ and } u \text{ is the least element of } X - y.$$

Assume $\mathrm{DC}(\omega+1)$. Then there is a function $f \in \omega+1 \to \omega$ such that $f``n\,R\,f(n)$ for every $n \in \omega$; this implies $f(n) = n$. Thence $f``\omega = \omega$, so there is no u such that $f``\omega\,R\,u$ as there is no $u \in \omega - \omega = \emptyset$. So $\mathrm{DC}(\omega+1)$ yields a contradiction.

6 Conclusions

We have mechanised parts of two advanced textbooks: most of Chapter I of Kunen [11] and the Ærst two chapters of Rubin and Rubin [21]. Some of this material is fairly recent; the Rubins cite papers from the 1960s. In doing our proofs, we noted a number of difÆculties.

On the whole, we have succeeded in reproducing the material faithfully. Isabelle's higher-order syntax makes it easy to express set-theoretic formulÒ. But Rubin and Rubin frequently use English phrases that translate to complex formulÒ. It is essential to ensure that the formulÒ are not only correct, but as simple as possible.

Standard mathematical concepts have conØicting deÆnitions. Sometimes these definitions are strictly equivalent, as in initial ordinals versus cardinals. Sometimes they are equivalent under certain assumptions: our deÆnition of ordinal relies on the Axiom of Foundation. Sometimes they differ only in inessential details, as in whether a well-ordering is required to be reØexive. No details are inessential in formal proof, and we can forsee that incompatible deÆnitions will become a serious problem as larger and larger bodies of mathematics are formalised.

Comparing the sizes of the formal and informal texts, Jutting [10, page 46] found that the ratio was contant. This may hold on average for a large piece of text, such as a chapter, but it does not hold on a line by line basis. Sometimes the text makes an intuitive observation that requires a huge effort to formalize. And sometimes it presents a detailed calculation that our tools can perform automatically. If we are going to perform such proofs on a large scale, we shall have to discover ways of predicting their size and cost.

Although set theory is formally untyped, mathematicians use different letters to range over natural numbers, cardinals, ordinals, relations and functions. There are obvious inclusions among these types: inÆnite cardinals are cardinals are ordinals, and all objects are sets. Isabelle's type system is of no help here. Other provers, such as IMPS [5] with its subtypes, might handle this aspect better. The proof of $\mathrm{WO}_6 \implies \mathrm{WO}_1$ revealed another limitation of Isabelle: its inability to allow deÆnitions and proofs to occur within the context of a lengthy inductive argument.

We know of no obstacle to proving deeper and deeper results in set theory. But we can forsee complications. For example, constructibility or forcing arguments may require formalising too much meta-theory. Other Æelds of mathematics, such as group theory, pose their own problems. We do not have a convenient way to mechanise deÆnitions and proofs involving algebraic structure.

Acknowledgements. The research was funded by the EPSRC GR/H40570 ™Combining HOL and Isabelle∫ and by the ESPRIT Basic Research Action 6453 ™Types.∫ GrÀbczewski's visit was made possible by the TEMPUS Project JEP 3340 ™Computer Aided Education.∫

References

[1] J. R. Abrial and G. LafÆtte. Towards the mechanization of the proofs of some classical theorems of set theory. preprint, February 1993.

[2] Robert S. Boyer and J Strother Moore. *A Computational Logic*. Academic Press, 1979.

[3] Robert S. Boyer and J Strother Moore. *A Computational Logic Handbook*. Academic Press, 1988.

[4] Gilles Dowek et al. The Coq proof assistant user's guide. Technical Report 154, INRIA-Rocquencourt, 1993.

[5] William M. Farmer, Joshua D. Guttman, and F. Javier Thayer. IMPS: An interactive mathematical proof system. *Journal of Automated Reasoning*, 11(2):213±248, 1993.

[6] *Formalized Mathematics*. Published by Fondation Philippe le Hodey, Av. F. Roosevelt 134 (Bte 7), 1050 Brussels, Belgium.

[7] Martin Gardner. *The Unexpected Hanging and Other Mathematical Diversions*. University of Chicago Press, 1991.

[8] Paul R. Halmos. *Naive Set Theory*. Van Nostrand, 1960.

[9] Gérard Huet. Residual theory in λ-calculus: A formal development. *Journal of Functional Programming*, 4(3):371±394, 1994.

[10] L.S. van Benthem Jutting. *Checking Landau's ™Grundlagen∫ in the AUTOMATH System*. PhD thesis, Eindhoven University of Technology, 1977.

[11] Kenneth Kunen. *Set Theory: An Introduction to Independence Proofs*. North-Holland, 1980.

[12] R. P. Nederpelt, J. H. Geuvers, and R. C. de Vrijer, editors. *Selected Papers on Automath*. North-Holland, 1994.

[13] Philippe Noël. Experimenting with Isabelle in ZF set theory. *Journal of Automated Reasoning*, 10(1):15±58, 1993.

[14] Lawrence C. Paulson. Constructing recursion operators in intuitionistic type theory. *Journal of Symbolic Computation*, 2:325±355, 1986.

[15] Lawrence C. Paulson. Set theory for veriÆcation: I. From foundations to functions. *Journal of Automated Reasoning*, 11(3):353±389, 1993.

[16] Lawrence C. Paulson. Set theory for veriÆcation: II. Induction and recursion. Technical Report 312, Computer Laboratory, University of Cambridge, 1993. To appear in Journal of Automated Reasoning.

[17] Lawrence C. Paulson. A Æxedpoint approach to implementing (co)inductive deÆnitions. In Alan Bundy, editor, *12th International Conference on Automated Deduction*, pages 148±161. Springer, 1994. LNAI 814.

[18] Lawrence C. Paulson. *Isabelle: A Generic Theorem Prover*. Springer, 1994. LNCS 828.

[19] The QED manifesto. On the World Wide Web at URL http://www.mcs.anl.gov/home/lusk/qed/manifesto.html, 1995.

[20] Art Quaife. Automated deduction in von Neumann-Bernays-Gödel set theory. *Journal of Automated Reasoning*, 8(1):91±147, 1992.

[21] Herman Rubin and Jean E. Rubin. *Equivalents of the Axiom of Choice, II*. North-Holland, 1985.

[22] David M. Russinoff. A mechanical proof of quadratic reciprocity. *Journal of Automated Reasoning*, 8(1):3±22, 1992.

[23] N. Shankar. *Metamathematics, Machines, and Gödel's Proof*. Cambridge University Press, 1994.

[24] Patrick Suppes. *Axiomatic Set Theory*. Dover, 1972.

[25] Yuan Yu. Computer proofs in group theory. *Journal of Automated Reasoning*, 6(3):251±286, 1990.