An Irrational Construction of $\mathbb{R}$ from $\mathbb{Z}$

R.D. Arthan

Lemma 1 Ltd.
2nd Floor, 31A Chain Street,
Reading UK RG1 2HX
rda@lemma-one.com

Abstract. This paper reports on a construction of the real numbers in the ProofPower implementation of the HOL logic. Since the original construction was implemented, some major improvements to the ideas have been discovered. The improvements involve some entertaining mathematics: it turns out that the Dedekind cuts provide many routes one can travel to get from the ring of integers, $\mathbb{Z}$, to the field of real numbers, $\mathbb{R}$. The traditional stop-over on the way is the field of rational numbers, $\mathbb{Q}$. This paper shows that going via certain rings of algebraic numbers can provide a pleasant alternative to the more well-trodden track.

1 Introduction

1.1 Automated Theorem Proving Background

ProofPower is a suite of tools supporting specification and proof in a range of formalisms. At the heart of the tools is the logical kernel for HOL, which is a re-engineering of the kernel of the Classic HOL system[7]. This re-engineering[1] was undertaken by ICL between 1988 and 1992 to meet requirements for a tool to reason about security properties expressed in Z[10]. Since 1993 ProofPower has been applied to research and development in methods for specification and verification of safety-critical systems. In 1994, a method for specifying and verifying Ada code called the Compliance Notation[12, 15] was implemented to form the Compliance Tool component of ProofPower. Research and development into the notation and the tool continues informed by a number of successful applications and case studies and the tool is currently being put to work on significant verification problems in the military avionics domain.

Early versions of the Compliance Tool had only vestigial support for the Ada data types that represent real numbers. However, investigation of actual code in the intended applications domain has shown that real programmers do use reals. During 1999 and 2000 it became clear that proper support for Ada real types was essential. In 2000, the Defence and Evaluation Research Agency, the designers and main users of the Compliance Notation, commissioned Lemma 1 Ltd., who now develop and market ProofPower, to provide this support.

Ada real types in the Compliance Tool use a formalisation of the real numbers in Z, which, in turn, is based on a theory of the real numbers in ProofPower-HOL.

The ProofPower-HOL theory was developed in November 2000 by the present author using some novel methods intended to make use of the fact that ProofPower-HOL already possessed reasonably well-supported theories for both natural number and integer arithmetic.

As is the norm in the HOL community, the theory of the reals in ProofPower-HOL is developed by conservative extension rather than by axiomatisation. Indeed, just to assert the axioms of the reals, characterised say, as a complete ordered field, would be a relatively trivial (albeit error-prone) exercise. The merits of conservative extension over axiomatisation by *fiat* have been widely discussed, see[8] for a survey.

I should remind the reader that HOL is a typed logic with well-defined principles of conservative extension for introducing new types and constants. The defining property for a new constant $c : \tau$ can be an arbitrary satisfiable predicate defined on the type τ, e.g., one might introduce a constant $\mathsf{Sqrt} : \mathbb{N} \to \mathbb{N}$, with defining property: $\forall m \bullet (\mathsf{Sqrt}\ m)^2 \leq m < (\mathsf{Sqrt}\ m + 1)^2$. The HOL logical kernel imposes a proof obligation to ensure that the defining property is indeed satisfiable so that the introduction of the constant is conservative.

The defining property for a new type has a standard form asserting that the new type is in one-to-one correspondence with a non-empty subset of an existing type. Again a proof obligation is imposed to ensure that the subset is non-empty. As an example, one can introduce a type with a given finite number of elements by requiring it to be in one-to-one correspondence with an appropriate interval of natural numbers. This simple subtyping mechanism, combined with the power of the primitive type constructors, allows a wide variety of standard type constructions to be carried out. For example, given an equivalence relation on an existing type τ, the quotient type (with one element for each equivalence class) can be formed as a subtype of the power set type $(\tau)\mathsf{SET}$.

John Harrison[8] has developed a very elegant refinement of the method of fundamental sequences which is well adapted to constructing a theory of reals using the natural numbers as a starting point. The present author would not hesitate to recommend Harrison's approach in a context where a good theory of integers is not to hand. If the integers are available, the approach of the present paper is offered as an alternative which has its attractions. In particular:

- There is no need to work with equivalence classes[1]
- the only subtype[1] that needs to be created is the type, $\mathbb{R}$, of the real numbers themselves;
- the theories of order, addition and multiplication are dealt with in succession, each one building on what has come before and providing reusable theory for use in later work.

[1] While automation can make dealing with equivalence classes and subtypes straightforward, these devices inevitably involve additional proof obligations.

1.2 Mathematical Background

The textbook journey from $\mathbb{Z}$ to $\mathbb{R}$ is the composite of two standard means of transport. First we take the ring $\mathbb{Z}$ and form its field of fractions, $\mathbb{Q}$ and note that the order structure on $\mathbb{Z}$ carries over to $\mathbb{Q}$. However, $\mathbb{Q}$ is incomplete — numbers such as $\sqrt{2}$ and π fail to show up at this stage of the trip. To remedy this, we appeal to something like the Dedekind completion by cuts, or Cantor's method of fundamental sequences (a.k.a. Cauchy sequences) to arrive at our goal $\mathbb{R}$. Excellent surveys of the terrain are given in [5, 8]. In the sequel, we will concentrate on the Dedekind cuts construction. In an elementary treatment, this construction is presented along something like the following lines.

i) The rational numbers $\mathbb{Q}$ are constructed (e.g., as equivalence classes of pairs $(m, n) : \mathbb{Z} \times \mathbb{N}_1$, with (m, n) representing the fraction m/n). The rational numbers are then shown to comprise an ordered field.

ii) A Dedekind *cut* is now defined to be any non-empty set, C, of rational numbers which is, *(a)*, downwards-closed (i.e., if $q \in C$, then any rational number $p < q$ is also in C), *(b)*, unbounded above in itself (i.e., for any $q \in C$, there is a $p \in C$ with $q < p$), and *(c)* bounded above in $\mathbb{Q}$ (i.e., for some $q \in \mathbb{Q}$, every $p \in C$ satisfies $p < q$). $\mathbb{R}$ is defined to be the set of all such cuts.
The rational numbers $\mathbb{Q}$ are identified with a subset of $\mathbb{R}$, the set of *rational cuts*, by associating $q \in \mathbb{Q}$ with the cut compromising all rational numbers less than q.
The set of cuts is shown to be linearly ordered by set-theoretic inclusion and this ordering is shown to agree with the usual ordering on $\mathbb{Q}$ when restricted to rational cuts. This ordering is seen to be complete (i.e., any non-empty subset of $\mathbb{R}$ that is bounded above has a supremum in $\mathbb{R}$). Indeed, the supremum of a bounded set of cuts turns out to be its set-theoretic union.

iii) Addition of cuts is now defined as follows: if C and D are cuts, the sum $C + D$ is defined to be the set of all sums $p + q$ where $p \in C$ and $q \in D$. This is shown to be a cut and so defines a binary operation $\mathbb{R} \to \mathbb{R} \to \mathbb{R}$, which is then shown to be associative and commutative and to have the rational cut corresponding to $0 \in \mathbb{Q}$ as an identity element.

iv) The additive inverse operator is now defined as follows: if C is a cut, $-C$ is defined to be the set of all $q \in \mathbb{Q}$ such that $p + q < 0$ for every $p \in C$. Again, this is shown to be a cut and so to define a unary operator $\mathbb{R} \to \mathbb{R}$, which is an inverse for the addition.

v) Multiplication and its inverse are defined in a similar fashion to addition and additive inverse, but with some complications due to signs. The interactions among the ordering relation, the additive structure and the multiplicative structure are investigated and we conclude that $\mathbb{R}$ is a complete ordered field.

An analysis of what is being assumed and what the arguments actually prove here reveals a number of useful facts:

– Step (ii) applies to any ordered set. This is the Dedekind-MacNeille completion theorem. For more on this, see, for example, [4]. The algebraic structure of $\mathbb{Q}$ is irrelevant here. Indeed, the completion of any countable, unbounded, densely ordered set is known by a theorem of Cantor to have the same order type as $\mathbb{R}$ (see, for example, [11]).

- Step (iii) makes no use of the multiplicative structure of $\mathbb{Q}$ — only its ordering and its additive structure are needed. However, it is not the case that just any ordered commutative group will do[2]. In fact, what is required is that $\mathbb{Q}$ contains arbitrarily small positive elements, or equivalently, it is densely ordered: for any $x < y$, there is a z with $x < z < y$. Density is required in verifying that the rational cut determined by 0 is indeed an identity for addition.
- Step (iv) also makes no use of the multiplicative structure except for the ability (which exists in any group) to "multiply" elements by natural numbers. However density is not sufficient to make the proof go through[3]. It turns out that we require the archimedean property on the additive group $\mathbb{Q}$: for any positive elements, x and y, there is an $n \in \mathbb{N}$ such that $y < nx$. Here nx denotes the n-fold sum $x + x + \ldots + x$.
- Finally, essentially by a theorem of Hölder [9], step (v) is an instance of a general construction that is independent of the details of the additive structure. Hölder's theorem is usually stated as saying that any archimedean ordered group is isomorphic to a subgroup of the real numbers under addition. Consequently, the completion of any ordered group that is both dense and archimedean must be isomorphic to the real numbers, and so must admit a multiplication. Moreover, the method of the proof of Hölder's theorem comes close to providing a definition for the multiplication.

1.3 A New Approach

The observations of the previous section suggest new approaches to constructing the real numbers. The rest of this paper is mainly concerned with presenting one such approach and is organised as follows:

Section 2 discusses the Dedekind-MacNeille completion theorem. This is well-known and so the discussion is very brief.

Section 3 discusses how the additive structure of the real numbers may be derived from the Dedekind-MacNeille completion of any dense, archimedean, ordered group. Again this is very brief — the classical proofs go through without change.

Section 4 is concerned with deriving the multiplicative structure of the real numbers from the additive structure. This seems to be one of those topics that is well-known but rarely written down, so we give a complete, albeit rather condensed, discussion.

Section 5 is the main contribution of this paper. It provides a source of dense, archimedean, ordered groups that are algebraically much simpler than the

[2] E.g., try using $\mathbb{Z}$ in place of $\mathbb{Q}$.

[3] E.g., try using the product group $\mathbb{Z} \times \mathbb{Q}$ with the lexicographic order in place of $\mathbb{Q}$.

rational numbers. The groups considered are the additive groups of the rings $\mathbb{Z}[\alpha]$ where α can be any one of a variety of irrational numbers. For definiteness, we concentrate on the case $\alpha = \sqrt{2}$.

Section 6 offers my confession that the construction outlined in the present paper is not what was actually done in November 2000 for the ProofPower product. The construction used algebraic structures weaker than ordered groups as its basis. The derivation of the additive structure of the reals from these weaker systems has to be more general than the construction described in this paper. In comparison, the approach proposed here provides some considerable economies in the proofs.

Section 7 gives some concluding remarks.

The present paper deliberately concentrates on the mathematics rather than the details of the particular formalisation in ProofPower. This is because some of the mathematics is not very accessible in the literature and some parts of it are believed to be new, whereas how to formalise the mathematics will depend on the system being used and should be fairly clear to a competent user of any adequately expressive system.

Demo versions of the ProofPower treatment of the material outlined in this document are available on the World-Wide Web[4]. The reader is referred to that material for further details of the formalisation.

The construction described in this document may seem at first sight to be rather exotic. However, from several points of view it can be seen as quite natural. One such point of view is this: let us take it as given that we wish to avoid the expense of constructing the rationals and tools to reason about them prior to constructing the reals, since $\mathbb{Q}$ will appear as a subfield of $\mathbb{R}$ in any case. As a substitute for $\mathbb{Q}$, we look for a dense subgroup of $\mathbb{R}$ which is simple enough to be directly amenable to existing tools for reasoning about the integers. A subgroup such as $\mathbb{Z}[\sqrt{2}]$, which is isomorphic as an additive group to the cartesian product $\mathbb{Z} \times \mathbb{Z}$, would do nicely. However we will need an easy way of working with the ordering that $\mathbb{Z}[\sqrt{2}]$ receives as a subgroup of $\mathbb{R}$. As we will see in section 5.2 of this paper, it turns out that there is a very tractable description of this ordering and the properties needed of $\mathbb{Z}[\sqrt{2}]$ are very easy to prove.

2 Dedekind-MacNeille Completion

The Dedekind-MacNeille completion theorem proves to be simplicity itself. In the ProofPower treatment, MacNeille's generalisation of the Dedekind construction to partially ordered sets was not needed, so the theory was developed for linearly ordered sets only.

The result we have to prove is that any unbounded, dense, linearly ordered may be embedded as an unbounded dense subset of a complete ordered set. The actual statement of the theorem gives an explicit witness for the complete

[4] Follow the link from `http://www.lemma-one.com/papers/papers.html`

ordered set. This is very simple first-order set theory and the main proofs were found in the course of one day.

Once one has a suitable densely ordered set, S say, the theory of Dedekind-MacNeille immediately enables one to define the type $\mathbb{R}$. The defining property for the new type is entirely order-theoretic and just states that there $\mathbb{R}$ admits a linear order which is dense and complete and admits an embedding of S as an unbounded, dense subset. On the basis of this type definition, it involves a trivial proof to define the constant $<: \mathbb{R} \to \mathbb{R} \to \mathbb{B}$ that gives the ordering on the real numbers. One can then define the supremum operator[5] $\mathsf{Sup} : (\mathbb{R})\mathsf{SET} \to \mathbb{R}$. $\leq$, $>$ and $\geq$ can also conveniently be defined at this stage.

At this point, one can start to develop useful, reusable, theory about the ordering and the supremum operator. E.g., one can show that for non-empty, bounded above, sets A and B, a sufficient condition for $\mathsf{Sup}(A) \leq \mathsf{Sup}(B)$ is that $A \subseteq B$. This theory is useful both in the rest of the construction and in ordinary use of the theory of reals once the construction is complete.

3 Defining the Additive Structure

Defining the additive structure of the reals given a dense, archimedean, ordered group is essentially what is achieved in steps (iii) and (iv) of the classical Dedekind cuts construction as described in section 1.2 above. The reader is referred to any good calculus textbook for the details, e.g., [14]. However, some descriptions, e.g., that in [5], skate over the role of the archimedean property.

As with the order structure, new constants $+ : \mathbb{R} \to \mathbb{R} \to \mathbb{R}$, $0_{\mathbb{R}} : \mathbb{R}$ and $- : \mathbb{R} \to \mathbb{R}$ are introduced and their elementary properties derived. Particularly useful are theorems about cancellation of like terms on either side of an equality or inequality.

4 Defining the Multiplicative Structure

The author has been unable to find an accessible modern treatment of the derivation of the multiplicative structure in the literature. This is probably because results like Hölder's theorem are generally given in a context where the real numbers are already available.

The arguments needed are, in essence, all given in a paper by Behrend[2]. However, Behrend's arguments are set in a context which is rather different from ours. The ProofPower treatment uses a recasting of the core arguments from Behrend in modern dress. It also delivers theorems which may be of general use in further development of the theory.

So let us assume that R is a non-trivial complete ordered commutative group. We want to show that R can be equipped with a multiplication turning it into

[5] Sup is conceptually a partial function. It is formalised in ProofPower as a total function whose defining property reveals no information about values of the function which are conceptually undefined.

an ordered field. To this end, let us fix some positive element $1_R : R$ which we will make into the multiplicative identity element of the field.

The basic idea is that, if R can be turned into an ordered field, then, for any $x : R$, multiplication by x determines an additive group homomorphism $R \to R$. Moreover, if x is positive, multiplication by x is (strictly) order-preserving (i.e., $xy < xz$ whenever $y < z$). Thus we can hope to derive the multiplicative structure by investigating the order-preserving additive homomorphisms $R \to R$. Let us call these OPAHs.

It is not hard to see that OPAHs are necessarily injective functions[6]. What is true, but somewhat harder to prove is that OPAHs are also surjective. To prove this we first observe that any subgroup of R containing arbitrarily small positive elements is dense in R. Now the image of an OPAH, f, is a subgroup of R and it is not hard to see that it contains arbitrarily small positive elements[7]. Thus the image of f is a dense subgroup of R. So any OPAH, f, is an order-preserving injective function from R to a dense subset of itself; but viewed as a subset of R ordered as a subset of R, the image of f must be complete because R is complete, and f is order-preserving. It is now not hard to see that the image must be equal to R and so f is indeed surjective[8].

A homomorphism $f : R \to R$ is said to be *central* if it commutes with every homomorphism $g : R \to R$, i.e., if $f(g(x)) = g(f(x))$ for every $x \in R$. Central OPAHs (COPAHs) will serve for us as a substitute for the multiplication by natural numbers used in [2] and other treatments such as [9].

What we now want to show is that COPAHs abound. To see this, let $\delta \in R$ be any positive element. Consider the set $A = A_\delta$ of elements, $x \in R$ such that either $x = 0$ or for some COPAH g, we have $g(\delta) = x$ or $g(\delta) = -x$. Then it is not very hard to see that A is a dense subgroup of R. Density is the only tricky part. For density, one verifies that the function $t : R \to R$ defined by $t(x) = x+x$ is a COPAH. Since COPAHs are OPAHs, and OPAHs are surjective, t has an inverse $h : R \to R$, and h is then itself a COPAH with the property that, for any $x \in R$, we have $x = h(x) + h(x)$. I.e., h is "division by 2". It follows that A has no least positive element[9], i.e. A is dense.

In fact, the dense subgroups A_δ defined in the previous paragraph are complete and so $A_\delta = R$ for every positive δ. I.e., for any $x \in R$ with $x \neq 0$, there is a COPAH g, such that either $x = g(\delta)$ or $x = -g(\delta)$. The proof of this requires us to show, in effect, that the (pointwise) supremum of a bounded family of COPAHs is itself a COPAH. We omit the details, just noting that the key is to show that if f and g are two OPAHs, then if $f(x) < g(x)$ for some positive x, then $f(x) < g(x)$ for every positive x. This is proved essentially by the argument

[6] If $f(x) = f(y)$, then $x < y$ and $y < x$ are both impossible, so we must have $x = y$

[7] It contains some positive elements, e.g., $f(1_R)$; if it contained a least positive element, $f(\epsilon)$, say, then by density of R there would be a δ with $0 < \delta < \epsilon$, but then $f(\delta)$ is positive and smaller than $f(\epsilon)$

[8] Consider a least positive element that is not in the image.

[9] If $x = f(\delta)$ were such an element, with f the COPAH that testifies to $x \in A$, then $g = h \circ f$ is also a COPAH and $g(\delta) < f(\delta)$.

of the uniqueness half of the main theorem in [2], using COPAHs rather than multiplication by natural numbers to show that it is not possible for $f(y) \geq g(y)$ for any y.

What we have just proved is that for any positive $\delta \in R$ and any non-zero $x \in R$, there is a COPAH, g, with $g(\delta) = x$ or $g(\delta) = -x$, and this may be shown to be unique. Fixing $\delta = 1_R$, this says that for every positive x, there is a unique $g = g_x$ such that $g(1_R) = x$. We now define multiplication by x by $xy = g_x(y)$. This definition may be extended to cover the case when $x \leq 0$ in the obvious way, and making heavy use of the uniqueness of g_x, one shows that this turns R into ring with unit 1_R. Since COPAHs are bijections, this ring is actually a field and all the properties of an ordered field follow. For the details, we refer to [2] yet again — this part of the argument translates easily into the present context.

In ProofPower this part of the construction was not difficult, but was a little time-consuming. It took perhaps 5 days to discover and formalise the arguments, which provide the consistency proofs for the definitions of the constants $* : \mathbb{R} \to \mathbb{R} \to \mathbb{R}$ and ${}^{-1} : \mathbb{R} \to \mathbb{R}$ giving multiplication and multiplicative inverse for the real numbers.

5 An Alternative to $\mathbb{Q}$

In this section, we construct a dense, archimedean ordered commutative group. Given the arguments of sections 2, 3 and 4 above, this is all that is needed to complete our construction of the reals. The group we use is called $\mathbb{Z}[\sqrt{2}]$. It is introduced in section 5.1 below. In fact, since it involves little extra work, we will show that $\mathbb{Z}[\sqrt{2}]$ is actually an ordered ring.

5.1 Calculating in $\mathbb{Z}[\sqrt{2}]$

Imagine using a square with 1-inch sides to mark off points along the real number line starting at the fixed base point 0. Using a side of the square you can mark off any whole number of inches to the left or the right of the base point. However, you can use the diagonal of the square to mark off distances in either direction too. Pythagoras' theorem says that the diagonal is $\sqrt{2} = \sqrt{1^2 + 1^2}$ inches long. So, the points you can mark off are precisely the real numbers $a + b\sqrt{2}$ where a and b are integers. These are the numbers that make up the ring $\mathbb{Z}[\sqrt{2}]$.

Addition and additive inverse in $\mathbb{Z}[\sqrt{2}]$ is easy to describe purely in terms of integer arithmetic; describing multiplication is not much harder:

$$\begin{aligned}
(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\
-(a + b\sqrt{2}) &= (-a) + (-b)\sqrt{2} \\
(a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2}.
\end{aligned}$$

In the sequel we will often turn facts about the real numbers into definitions. Here, if we consider pairs (a, b) where a and b are integers, we can define addition, negation and multiplication as follows:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$-(a, b) = (-a, -b)$$
$$(a, b)(c, d) = (ac + 2bd, ad + bc).$$

One may then check that the above definitions turn the set, $\mathbb{Z} \times \mathbb{Z}$, of all pairs of integers into a ring with zero element $\mathbf{0} = (0, 0)$ and unit element $\mathbf{1} = (1, 0)$.

The pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ thus give a model, defined solely in terms of integer arithmetic, for the arithmetic of all real numbers of the form $a + b\sqrt{2}$. From now on, we shall refer to this model as $\mathbb{Z}[\sqrt{2}]$. It is here that $\mathbb{Z}[\sqrt{2}]$ has its main advantage over $\mathbb{Q}$: the verifications of the ring laws reduce to equations over the integers that are easily solved by a linear arithmetic decision procedure. Stating and proving the laws took the author less than half an hour in ProofPower.

5.2 The Ordering of $\mathbb{Z}[\sqrt{2}]$

Given members $\mathbf{y} = (c, d)$ and $\mathbf{z} = (e, f)$ of $\mathbb{Z}[\sqrt{2}]$, how do we decide the relative order of the real numbers $y = c + d\sqrt{2}$ and $z = e + f\sqrt{2}$ that $\mathbf{y}$ and $\mathbf{z}$ represent?

To simplify the problem a little, I should explain that it is enough to decide, given any $\mathbf{x} = (a, b)$ in $\mathbb{Z}[\sqrt{2}]$, whether or not $x = a + b\sqrt{2}$ is positive (i.e., greater than 0). For, in $\mathbb{R}$, we know that $y < z$ precisely when $0 < z - y$. In general, to define an ordering on a (commutative) group, G, it is enough to identify a subset P of "positive elements". This subset must be closed under the group operation (addition), must not contain 0, and must be such that, for any non-zero element, g, of G, either g or $-g$ belongs to P. Given such a subset, P, defining $g < h$ to mean $h - g \in P$ gives a linear ordering of the elements of G compatible with the addition in G, in the sense that whenever $g < h$, then, also, $g + k < h + k$ for any k in G.

In the case of $\mathbb{Z}[\sqrt{2}]$, a first attempt at a rule for deciding whether $\mathbf{x} = (a, b)$ is positive would be to consider four cases as follows: *if,* (i)*, a and b are both positive then* $\mathbf{x}$ *certainly represents a positive real number; if,* (ii)*, neither of a and b is positive then* $\mathbf{x}$ *certainly does not represent a positive real number; otherwise, to ensure that* $\mathbf{x}$ *represents a positive real number, we must have either,* (iii)*, that a is negative and b is positive and $a^2 < 2b^2$ or,* (iv) *that a is positive, b is negative and $a^2 > 2b^2$.*

Unfortunately the above rules for identifying the positive numbers is not at all convenient[10]. It involves four cases, and when we try to verify the properties we require of the set of positive elements, the cases multiply and we find ourselves having to do some not very nice algebra in each case. While there are some symmetries between the cases, to show that the set of positive elements is

[10] Nonetheless, proving that $\mathbb{Z}[\sqrt{2}]$ becomes an ordered group under this definition is set as an exercise in the well-known textbook on algebra by Birkhoff and MacLane[13]. They also set the case $\mathbb{Z}[\sqrt{3}]$ as an asterisked, i.e., hard, exercise.

closed under addition requires verification of several different kinds of quadratic diophantine inequality whose proofs require some ingenuity. An alternative method is called for.

There is a recipe that has been known since antiquity for producing good rational approximations to $\sqrt{2}$. Consider the following sequence of rational numbers:

$$
\begin{array}{rcl}
u_1/v_1 & = & 1/1 \\
u_2/v_2 & = & 3/2 \\
u_3/v_3 & = & 7/5 \\
u_4/v_4 & = & 17/12 \\
 & \dots & \\
u_{i+1}/v_{i+1} & = & (u_i + 2v_i)/(u_i + v_i) \\
 & \dots &
\end{array}
$$

An induction on i shows that $u_i^2 - 2v_i^2 = (-1)^i$ for all natural numbers i. E.g., $17^2 - 2 \times 12^2 = 289 - 288 = 1 = (-1)^4$. So, for each i, $(u_i/v_i)^2 = 2 + (-1)^i/v_i^2$. Using the methods of the calculus, it follows that u_i/v_i converges to $\sqrt{2}$ as i tends to infinity. Because of this, $a + b\sqrt{2}$ will be positive precisely when $a + (u_i/v_i)b$ is positive for all sufficiently large i. However, while we are *en route* to $\mathbb{R}$, the methods of the calculus are away in the distance. We need a rule for deciding when $a + (u_i/v_i)b$ is positive without appealing to the calculus or even to the existence of real or rational numbers.

Since the v_i are all positive, $a + (u_i/v_i)b$ will be positive precisely when $w_i = v_i a + u_i b$ is positive. Given integers a, and b, let's look at the sequence of numbers w_i:

$$
\begin{array}{rcl}
w_1 & = & a + b \\
w_2 & = & 2a + 3b \\
w_3 & = & 5a + 7b \\
w_4 & = & 12a + 17b \\
 & \dots &
\end{array}
$$

If we set $w_0 = b$ to help us get started, the w_i follow a very simple rule:

$$
\begin{aligned}
w_0 &= b \\
w_1 &= a + b \\
w_{i+2} &= 2w_{i+1} + w_i
\end{aligned}
$$

We have already observed that $a+b\sqrt{2}$ is positive precisely when w_i is positive for all sufficiently large i. From the above rule for the w_i, this will happen precisely when two consecutive values, w_i and w_{i+1} are positive for some i.

In the light of the above, we can now describe an algorithm, which to the best of my knowledge is new, for testing the sign of an element, $\mathbf{x} = (a, b)$ of $\mathbb{Z}[\sqrt{2}]$. To describe the algorithm, we begin by introducing the "sign-test" functions. These are a family of functions, ST_i, one for each natural number i. Each of the sign-test functions maps $\mathbb{Z}[\sqrt{2}]$ to $\mathbb{Z}$. They are defined by the following recurrence equations which hold for any natural number i and integers a and b:

$$\begin{aligned}\mathsf{ST}_0(a,b) &= b\\ \mathsf{ST}_1(a,b) &= a+b\\ \mathsf{ST}_{i+2}(a,b) &= 2\mathsf{ST}_{i+1}(a,b)+\mathsf{ST}_i(a,b)\end{aligned}$$

It is easy to verify by induction on i that the sign-test functions are all homomorphisms from the additive group of $\mathbb{Z}[\sqrt{2}]$ to the additive group of $\mathbb{Z}$. I.e., for any natural number i and members $\mathbf{x}$ and $\mathbf{y}$ of $\mathbb{Z}[\sqrt{2}]$ the following equation holds:

$$\mathsf{ST}_i(\mathbf{x}+\mathbf{y}) = \mathsf{ST}_i(\mathbf{x})+\mathsf{ST}_i(\mathbf{y})$$

Here the addition on the left-hand side is our newly-defined addition in $\mathbb{Z}[\sqrt{2}]$, while the addition on the right is the usual addition in $\mathbb{Z}$. Note this implies that for any integers n, a and b, we have $\mathsf{ST}_i(na,nb) = n\mathsf{ST}_i(a,b)$ and $\mathsf{ST}_i(-a,-b) = -\mathsf{ST}_i(a,b)$. If $n \in \mathbb{Z}$, and $\mathbf{x} = (a,b) \in \mathbb{Z}[\sqrt{2}]$, we will write $n\mathbf{x}$ for (na,nb). For $n \in \mathbb{N}$, $n\mathbf{x}$ is equal to the iterated addition: $\mathbf{x}+\mathbf{x}+\ldots+\mathbf{x}$, with n appearances of $\mathbf{x}$ (which we take, by convention, to be $\mathbf{0}$ if $n=0$).

The algorithm for testing the sign of $\mathbf{x} = (a,b) \in \mathbb{Z}[\sqrt{2}]$ is as follows: calculate $w_i = \mathsf{ST}_i(\mathbf{x})$ for $i = 0,1,2,\ldots$ in turn until one of the following three outcomes occurs: either, *(i)*, $w_i = w_{i+1} = 0$, in which case, as is easy to see, a and b were both equal to 0 to start with and $\mathbf{x} = \mathbf{0}$; *(ii)*, w_i and w_{i+1} are both positive, in which case, as we have already remarked, $\mathbf{x}$ is positive; or, *(iii)*, w_i and w_{i+1} are both negative, in which case $\mathbf{x}$ is negative (because carrying out the calculation using $-\mathbf{x}$ in place of $\mathbf{x}$ would end up in case *(ii)* and show that $-\mathbf{x}$ is positive).

We must prove that this algorithm terminates:

Theorem 1 *For any integers a and b, if we construct the sequence of numbers defined by the equations, $w_0 = b$, $w_1 = a+b$ and $w_{i+2} = 2w_{i+1}+w_i$, $(i = 0,1,2,\ldots)$, then, for some i, and hence for all sufficiently large i, exactly one of the following three cases will obtain:* (i), $w_i = w_{i+1} = 0$, (ii), $0 < w_i \wedge 0 < w_{i+1}$ *or,* (iii) $w_i < 0 \wedge w_{i+1} < 0$. *I.e., the sign-test algorithm described above always terminates.*

Proof: The absolute values of the integers w_i cannot decrease indefinitely, so there is a k such that $|w_k| \leq |w_{k+1}|$. If $w_{k+1} = 0$, then $w_k = 0$ and the algorithm terminates at or before stage k in case *(i)*. If $w_{k+1} \neq 0$, then because $w_{k+2} = 2w_{k+1}+w_k$ and $|w_k| \leq |w_{k+1}|$, w_{k+2} and w_{k+1} must have the same sign, and the algorithm terminates at or before stage $k+1$ in case *(ii)* or *(iii)* according as w_{k+1} is positive or negative[11]. ■

We may now define the set, $\mathbf{P}$, of positive elements of $\mathbb{Z}[\sqrt{2}]$. $\mathbf{P}$ is the set of all members of $\mathbb{Z}[\sqrt{2}]$ for which the sign-test algorithm returns a positive result.

[11] The same argument will work if we replace the recurrence equation $w_{i+2} = 2w_{i+1} + w_i$, by $w_{i+2} = Aw_{i+1}+Bw_i$, for any integers A and B with $A \geq B > 0$. This can be shown to give routes from $\mathbb{Z}$ to $\mathbb{R}$ via subrings $\mathbb{Z}[\alpha]$ for a variety of real numbers α including all those of the form $\sqrt{m}$ for m any positive integer for which $\sqrt{m} \notin \mathbb{Z}$.

Formally, $\mathbf{P}$ may be defined by either of the following two equations (which are equivalent by our earlier remarks about the sequences w_i):

$$\begin{aligned}\mathbf{P} &= \{\mathbf{x} : \mathbb{Z}[\sqrt{2}] | \exists i : \mathbb{N} \bullet \mathsf{ST}_i(\mathbf{x}) > 0 \wedge \mathsf{ST}_{i+1}(\mathbf{x}) > 0\} \\ &= \{\mathbf{x} : \mathbb{Z}[\sqrt{2}] | \exists i : \mathbb{N} \bullet \forall j \bullet i \leq j \Rightarrow \mathsf{ST}_j(\mathbf{x}) > 0\}\end{aligned}$$

Let us record what we now know about the sign-test algorithm and our observations on ordered groups to give the following theorem:

Theorem 2 *$\mathbb{Z}[\sqrt{2}]$ equipped with the ordering defined by taking $\mathbf{P}$ as the set of positive elements is an ordered commutative group.*

Proof: What we have to prove is that $\mathbf{P}$ is closed under addition, does not contain $\mathbf{0}$, and, for any element $\mathbf{x}$ of $\mathbb{Z}[\sqrt{2}]$, either $\mathbf{x}$ belongs to $\mathbf{P}$ or $-\mathbf{x}$ belongs to $\mathbf{P}$.

Our discussion of the sign-test algorithm has proved everything except that $\mathbf{P}$ is closed under addition. To see this, let $\mathbf{x}$ and $\mathbf{y}$ be any two members of $\mathbf{P}$, so that $\mathsf{ST}_i(\mathbf{x})$ and $\mathsf{ST}_i(\mathbf{y})$ are positive for all sufficiently large i. Now, $\mathsf{ST}_i(\mathbf{x}+\mathbf{y}) = \mathsf{ST}_i(\mathbf{x}) + \mathsf{ST}_i(\mathbf{y})$, and so $\mathsf{ST}_i(\mathbf{x}+\mathbf{y})$ will be positive for all sufficiently large i (just wait until i is large enough so that $\mathsf{ST}_j(\mathbf{x})$ and $\mathsf{ST}_j(\mathbf{y})$ are *both* positive whenever $j \geq i$). This means that $\mathbf{x}+\mathbf{y}$ will also be a member of $\mathbf{P}$, and so $\mathbf{P}$ is indeed closed under addition as needed to complete the proof of the theorem. ■

Therefore, the relation $<$ defined on $\mathbb{Z}[\sqrt{2}]$ by saying that $\mathbf{x} < \mathbf{y}$ holds precisely when $\mathbf{y} - \mathbf{x}$ belongs to $\mathbf{P}$ gives a linear ordering on $\mathbb{Z}[\sqrt{2}]$ which is compatible with addition, in the sense that, if $\mathbf{x} < \mathbf{y}$, then $\mathbf{x}+\mathbf{z} < \mathbf{y}+\mathbf{z}$ for any $\mathbf{z}$ in $\mathbb{Z}[\sqrt{2}]$.

5.3 Properties of the Ordering

In this section, we show that the ordering $<$ on $\mathbb{Z}[\sqrt{2}]$ induced by the set of positive elements $\mathbf{P}$ is archimedean and dense. We also show that $\mathbf{P}$ is compatible with multiplication.

The *archimedean property* states that iterated addition of any positive quantity results in a sequence of quantities that increase without bound:

Theorem 3 *Let $\mathbf{x}$ be any member of $\mathbf{P}$ and $\mathbf{y}$ any member of $\mathbb{Z}[\sqrt{2}]$, then there is a natural number, n, such that $\mathbf{y} < n\mathbf{x}$.*

Proof: By the definition of $\mathbf{P}$, the assumption that $\mathbf{x} \in \mathbf{P}$ means that we can find an i such that two consecutive values, $\mathsf{ST}_i(\mathbf{x})$ and $\mathsf{ST}_{i+1}(\mathbf{x})$, are both positive. Choose a natural number n which is greater than the larger of the absolute values $|\mathsf{ST}_i(\mathbf{y})|$ and $|\mathsf{ST}_{i+1}(\mathbf{y})|$. I claim that n satisfies $\mathbf{y} < n\mathbf{x}$. For $\mathsf{ST}_i(n\mathbf{x} - \mathbf{y}) = n\mathsf{ST}_i(\mathbf{x}) - \mathsf{ST}_i(\mathbf{y}) \geq n - \mathsf{ST}_i(\mathbf{y}) > 0$, since $\mathsf{ST}_i(\mathbf{x}) \geq 1$, and $n > |\mathsf{ST}_i(\mathbf{y})|$ by our choices of i and n, and similarly for $\mathsf{ST}_{i+1}(n\mathbf{x} - \mathbf{y})$. So, $n\mathbf{x} - \mathbf{y}$ is in $\mathbf{P}$, and by definition of $<$, we do have $\mathbf{y} < n\mathbf{x}$, as claimed. ■

Now for *density*: an ordered group is densely ordered if its set of positive elements has no least element. We now show that this is the case for $\mathbb{Z}[\sqrt{2}]$:

Theorem 4 **P** *has no least element.*

Proof: What we have to show is that, if $\mathbf{y}$ is any member of $\mathbf{P}$, then there is a member $\mathbf{x}$ of $\mathbf{P}$ such that $\mathbf{x} < \mathbf{y}$. As $\mathbf{y} \in \mathbf{P}$, then for some i, $\mathsf{ST}_i(\mathbf{y})$ and $\mathsf{ST}_{i+1}(\mathbf{y})$ satisfy $0 < \mathsf{ST}_i(\mathbf{y}) < \mathsf{ST}_{i+1}(\mathbf{y})$. Now consider the recurrence equations that define the ST_j. These equations can be used in the reverse direction to find an $\mathbf{x}$ such that $\mathsf{ST}_i(\mathbf{x}) = 0$ and $\mathsf{ST}_{i+1}(\mathbf{x}) = 1$, whence $\mathsf{ST}_{i+2}(\mathbf{x}) = 2$, $\mathsf{ST}_i(\mathbf{y}-\mathbf{x}) > 0$ and $\mathsf{ST}_{i+1}(\mathbf{y}-\mathbf{x}) > 0$ so that $\mathbf{x}$ is in $\mathbf{P}$ and $\mathbf{x} < \mathbf{y}$ as required. ■

It is natural at this point to ask about the interplay between order and multiplication in $\mathbb{Z}[\sqrt{2}]$. If we plan to follow the approach of section 4 above, we do not actually need to study this part of the scenery in $\mathbb{Z}[\sqrt{2}]$. However, for completeness, we record the following theorem and give a sketch of a proof:

Theorem 5 $\mathbb{Z}[\sqrt{2}]$ *equipped with the ordering defined by taking* **P** *as the set of positive elements is an ordered ring.*

Proof: An ordered ring is an (additive) ordered group together with a multiplication making it into a ring in such a way that *(i)* the unit element $\mathbf{1}$ is positive and *(ii)* multiplication by positive elements is order-preserving — if $\mathbf{0} < \mathbf{x}$, and $\mathbf{y} < \mathbf{z}$, then $\mathbf{xy} < \mathbf{xz}$. Equivalently, $\mathbf{1}$ is positive and the set of positive elements is closed under multiplication.

In our case, it easy to check that $\mathbf{1} \in \mathbf{P}$ directly from the definitions. To check that $\mathbf{P}$ is closed under multiplication, assume $\mathbf{x}$ and $\mathbf{y}$ are members of $\mathbf{P}$. By definition, this means that, if we let $s_i = \mathsf{ST}_i(\mathbf{x})$ and $t_i = \mathsf{ST}_i(\mathbf{y})$, then the s_i and t_i are positive for all sufficiently large i. Let $w_i = \mathsf{ST}_i(\mathbf{xy})$, so that what we have to prove is that the w_i are positive for all sufficiently large i.

I claim that the following equation holds for any natural numbers m and n:

$$w_{m+n+1} = s_{m+1}t_{n+1} + s_m t_n$$

Given the equation above, if s_m and t_n are both positive, then w_{m+n+1} is too. As the s_i and t_i are positive for all sufficiently large i, then so are the w_i as required.

It remains to prove the equation. To do this, one first proves by induction on m that the equation holds for any m when $n = 0$, then, using that to provide the base case, one proves the equation for all m and n by induction on n. The inductions involve a little algebra and some care with the subscripts. ■

5.4 Discussion

The motivation behind the construction in this paper was as follows: given any irrational real number λ, the subgroup $\mathbb{Z} + \lambda\mathbb{Z}$ of $(\mathbb{R}, +)$ generated by 1 and λ is, *(i)*, dense (and so its Dedekind-MacNeille completion will be $\mathbb{R}$) and *(ii)* a free abelian group on the given generators (and so it is algebraically very tractable, in particular, every element has a canonical representation as $a + b\lambda$ for unique integers a and b). In contrast, *(i)*, no finitely generated subgroup of $(\mathbb{Q}, +)$ is dense and, *(ii)*, no dense subgroup of $(\mathbb{Q}, +)$ is free as an abelian group.

The case where λ is a real integral quadratic surd, such as $\sqrt{2}$, looked particularly promising, since in that case $\mathbb{Z} + \lambda\mathbb{Z}$ is actually a subring of $\mathbb{R}$. Of course, to construct $\mathbb{R}$ as the completion of $\mathbb{Z} + \lambda\mathbb{Z}$, we need to understand how the latter group is ordered, but the ordering turns out to be very tractable using the rather simple sign-test algorithm discussed above.

So with $\mathbb{Z}[\sqrt{2}]$, one has simple canonical representations and the minor complication of the sign-test algorithm to decide the ordering. In contrast, to get canonical representations of the elements of $\mathbb{Q}$, one has to appeal to the euclidean algorithm, the theory of which is significantly harder than the theory of the sign-test algorithm presented in this paper. The usual construction of $\mathbb{Q}$ as a set of equivalence classes avoids the need for canonical representations, at the price of proof obligations to justify definitions over the set of equivalence classes.

6 The Actual ProofPower Construction

The actual construction of the real numbers in ProofPower as carried out in November 2000 was significantly harder than the improved approach presented here. Nonetheless, measured in terms of lines of proof scripts, the complexity is about equal with that of Harrison's approach as described in [8].

The reason for the extra complication was simple and pragmatic: I had formulated the proof plan sketched in sections 1.2 and 1.3 above, but the direct approach to specifying the ordering in $\mathbb{Z}[\sqrt{2}]$ looked far from attractive and I had not discovered the easier approach of section 5.2. To leave some room for manoeuvre, I formulated a variant of the construction of the additive structure which requires less algebraic structure than the classical Dedekind construction allows. Under suitable hypotheses, the Dedekind construction can be applied to a monoid[12] rather than a group, and I knew I would be able to construct a suitable monoid. The Dedekind construction turns out to be not much harder than the usual one conceptually, but involves quite a lot more work with supremum arguments.

The monoid used is the multiplicative monoid of dyadic rational numbers. A dyadic rational number is one of the form $m/2^n$ where m and n are integers. Positive dyadic rationals may be identified with the set $\mathbb{N} \times \mathbb{Z}$ under the correspondence $(m, n) \mapsto (2m + 1)/2^n$ and the multiplication operator and ordering relation are not hard to define in terms of this. Verifying the required properties of these is a relatively straightforward but rather lengthy exercise in elementary algebra.

Thus, a combination of luck and design means that the actual construction was "transcendental" rather than just "irrational": the starting point for the Dedekind construction amounted to the monoid of all real numbers $\log(m/2^n)$ with $m > 0$ and n integers and most of these numbers are transcendental.

The theory is formulated so that the actual details of the construction are almost invisible to a user of the theory. What a user sees is a collection of

[12] A monoid is a "group without an inverse function", i.e., a set with an associative binary product with an identity element.

constants giving the field operations and ordering relation on $\mathbb{R}$ with defining properties that give the usual axiomatisation of $\mathbb{R}$ as a complete ordered field.

7 Concluding Remarks

The reader is again referred to [5, 8] for comprehensive surveys of constructions of the real numbers with many additional references. In this paper, there is only space for a few observations about other approaches.

The approach promoted here derives the multiplicative structure of $\mathbb{R}$ from its additive structure. This lets us exploit the delightfully simple additive structure of groups such as $\mathbb{Z}[\sqrt{2}]$ which turn out to have a very tractable order structure as well. However, the ring structure is simple too, and it now seems to the author that deriving the multiplicative structure of the reals in the traditional way from the ring structure of $\mathbb{Z}[\sqrt{2}]$ may well be advantageous.

This paper has concentrated on the Dedekind-MacNeille method of completing a dense ordered algebraic system. However, an approach using Cantor's method of fundamental sequences could also take $\mathbb{Z}[\sqrt{2}]$ as a starting point. This would need multiplicative inverses to be defined by a supremum argument rather than by pointwise operations on the fundamental sequences, but the supremum argument is an easy one.

A construction of the real numbers from the integers bypassing the rationals is given by Faltin et al. in [6]. Their method is to use a binary positional representation in which the digits are allowed to be arbitrary integers. This results in a presentation of the real numbers as a quotient of a certain subring of a ring of formal Laurent series. This gives considerable insight into the way carries propagate in infinite binary arithmetic and can be applied to other constructions (such as the p-adic completions of the integers). However, the method is considerably more complicated from an arithmetic point of view than the more traditional constructions.

In [3], Conway gives a construction which embraces $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ and much more using a uniform representation of numbers as pairs of sets which can be thought of as two-player games. The uniform representation leads to very uniform, if rather recondite, methods of proof. Characterising the real numbers within the Conway numbers is a little tricky but can be done. Unfortunately, in a typed framework such as HOL, identifying a type suitable for carrying out enough of the Conway construction to include $\mathbb{R}$ involves a far from trivial exercise in justifying transfinite inductive definitions.

In conclusion, selecting a method of constructing $\mathbb{R}$ in a mechanised theorem-proving system involves many trade-offs. The choice will be heavily influenced by what theories are already available and what theories are going to be developed in the future. If, for example, you have plans to do a lot of general commutative algebra, then your best route might be to do the general field-of-fractions construction and the standard material on ideals and quotient rings first and use these big guns to attack the specific problems of constructing $\mathbb{Q}$ as a field-of-fractions and then $\mathbb{R}$ via fundamental sequences. If you only have $\mathbb{N}$, and want to get going on analysis quickly, then Harrison's approach is probably the method of choice. If you have good working theories for $\mathbb{N}$ and $\mathbb{Z}$ then the methods of the present paper are offered for your consideration as a quick and simple route from $\mathbb{Z}$ to $\mathbb{R}$.

Acknowledgments

I am grateful to John Harrison for some very helpful correspondence and, in particular, for drawing the work of Behrend to my attention. I am indebted to the referees for all their comments and suggestions; these were most stimulating and have been of great assistance in revising the paper for publication.

References

1. R.D. Arthan. A Report on ICL HOL. In Myla Archer, Jeffrey J. Joyce, Karl N. Levitt, and Philip J. Windley, editors, *Proceedings of the 1991 International Workshop on the HOL Theorem Proving System and its Applications*. IEEE Computer Society Press, 1992.
2. F.A. Behrend. A Contribution to the Theory of Magnitudes and the Foundations of Analysis. *Mathematische Zeitschrift*, 63:345–362, 1956.
3. John H. Conway. *On Numbers and Games*. A.K. Peters Ltd., Second edition, 2001.
4. B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.
5. H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert. *Numbers*. Springer-Verlag, 1990.
6. F. Faltin, N. Metropolis, B. Ross, and G.-C. Rota. The Real Numbers as a Wreath Product. *Advances in Mathematics*, 16, 1975.
7. Michael J.C. Gordon and Tom F. Melham, editors. *Introduction to HOL*. Cambridge University Press, 1993.
8. John Harrison. Theorem Proving with the Real Numbers. Technical report, University of Cambridge Computer Laboratory, 1996.
9. O. Hölder. Die Axiome der Quantität und die Lehre vom Mass. *Ber. Verh. Kon. Sch. Ges. Wiss.*, pages 1–64, 1901.
10. R.B. Jones. Methods and Tools for the Verification of Critical Properties. In R.Shaw, editor, *5th Refinement Workshop*, Workshops in Computing. Springer-Verlag/BCS-FACS, 1992.
11. E. Kamke. *Mengenlehre*. Berlin, 1928. Reprinted by Dover in an English translation by F. Bagemihl as *Theory of Sets*. 1950.
12. D.J. King and R.D. Arthan. Development of Practical Verification Tools. *Ingenuity — the ICL Technical Journal*, 1996.
13. Saunders MacLane and Garrett Birkhoff. *Algebra*. AMS Chelsea Publishing, Third edition, 1999.
14. Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill Book Company, 1974.
15. C. T. Sennett. Demonstrating the Compliance of Ada Programs with Z Specifications. In R.Shaw, editor, *5th Refinement Workshop*, Workshops in Computing. Springer-Verlag/BCS-FACS, 1992.