Constructive Reals in Coq: Axioms and Categoricity

Herman Geuvers and Milad Niqui
{herman,milad}@cs.kun.nl

Department of Computer Science, University of Nijmegen, the Netherlands

Abstract. We describe a construction of the real numbers carried out in the Coq proof assistant. The basis is a set of axioms for the constructive real numbers as used in the FTA (Fundamental Theorem of Algebra) project, carried out at Nijmegen University. The aim of this work is to show that these axioms can be satisfied, by constructing a model for them. Apart from that, we show the robustness of the set of axioms for constructive real numbers, by proving (in Coq) that any two models of it are isomorphic. Finally, we show that our axioms are equivalent to the set of axioms for constructive reals introduced by Bridges in [2].
The construction of the reals is done in the 'classical way': first the rational numbers are built and they are shown to be a (constructive) ordered field and then the constructive real numbers are introduced as the usual Cauchy completion of the rational numbers.

1 Introduction

The FTA project at the University of Nijmegen (see [10]) had as goal to formalize a constructive proof of the Fundamental Theorem of Algebra in the proof assistant Coq [8]. For reasons of modularity, it was decided not to start with a specific construction of the real numbers, but to work axiomatically. So, a list of axioms was defined, which together define the notion of a *real number structure*. To do this, Coq allows a nice modular approach, using *dependent labelled record types*, on which simple inheritance relations can be defined using *coercions*. So, a real number structure is defined as a Cauchy complete Archimedean ordered field, where an ordered field is again defined as a field extended with an ordering satisfying certain properties. Fields are defined in terms of rings, which are defined in terms of groups, etcetera. In this way there is an algebraic hierarchy of structures that extend each other and that inherit operations, relations and properties from each other. For the present exposition we do not describe the full hierarchy, but just the relevant nodes: constructive setoids, rings, fields, ordered fields and real number structures.

The outline of the paper is as follows. After describing the relevant part of the algebraic hierarchy, we give the construction of the rational numbers $\mathbb{Q}$ and show that they form a constructive ordered field. Then we define the reals as Cauchy sequences over $\mathbb{Q}$ and show that they form a real number structure. This roughly follows the standard texts [13, 1]. As a matter of fact, we proceed in a slightly more general fashion by showing that the Cauchy sequences over *any* Archimedean constructive ordered field form a real number structure. The notion of real number structure describes a collection of models and we may wonder whether the axioms characterize the reals completely. This is the case: any two real number structures are isomorphic. This property has been formally stated and proved inside Coq. Finally, we compare our axioms for the reals and prove (within Coq) that they are equivalent to the ones of [2].

The mathematics described in this paper is formalized in Coq. To make the paper of interest to constructive mathematicians in general, we have tried to keep Coq syntax to a minimum. Some features of (the type theory of) Coq that are important to the formalization are: the propositions-as-types interpretation of logic (to formalize logical reasoning), record types and inductive types (to formalize mathematical structures and to have a type of natural numbers), dependent types (to formalize, e.g. the notion of subset) and the Axiom of Choice.

The present work gives a constructive version of what is already in the Coq standard library. This constructive version is required by the FTA project [9]. The Coq standard library contains classical real numbers, see [7]. They are axiomatized, based on a parameter R which is of type `Type` (and hence does not satisfy our axioms), together with relations and operations on R, which satisfy the *classical* axioms of real numbers. Other constructions of the reals in a type theoretic proof assistants are described in [12] (in the system LEGO), in [4] (in the system NuPrl) and [5] (in Coq). In [12] a real number is defined as a collection of arbitrary small nested intervals with rational endpoints. More precisely, a general construction for completing a metric space is given, with the metric space of the rationals as primary example. In [4] the set of rational numbers is defined, and then the type of reals is defined following Bishop's original construction [1], using regular Cauchy sequences. Finally the Cauchy completeness of reals is proved as a theorem in Nuprl. In [5], a construction of the reals in Coq is described, using infinite (lazy) streams. The work is especially of interest, as special care is taken to obtain an *efficient* implementation of the reals, with which one might actually compute. In [6], a (constructive) axiomatization for these reals is given. The axioms are very similar to ours, with the distinguished exception that in [6] special attention is paid to the minimality of the proposed axioms. This has lead to a minimal set of 16 axioms, which is compared to our axioms (Section 2) and Bridges axioms [2]. A good classical construction of the reals can be found in [11], which is especially interesting because much attention is devoted to the optimization of the operations and generating useful decision procedures.

2 Ordered Fields and Real number structures

We now present the definitions, in Coq, of a constructive ordered field and a real number structure. We present them as part of a constructive algebraic hierarchy, of which we present here only the part that is relevant for the purpose of understanding the real number axioms. See [9] for the full details.

Coq Definition 1.
```
Record CSetoid   : Type :=
{ C             :> Set;
  [=]           : C->C->Prop;
  [#]           : C->C->Prop;
  ap_irr        : (x:C)~(x [#] x);
  ap_sym        : (x,y:C)(x [#] y) -> (y [#] x);
  ap_cot        : (x,y:C)(x [#] y) -> (z:C)(x [#] z)\/(z [#] y);
  ap_tight      : (x,y:C)~(x [#] y) <-> (x [=] y)              }.
```

An important remark to make is that the above is *not* syntactically correct Coq code. The symbols `[#]` and `[=]` cannot be used as labels in a record structure. These symbols are only introduced *after* the record definition as syntactic sugared infix notation (via grammar rules). For readability we will throughout this paper use the syntactic sugared symbols already *in* the definition, as infix operations.

The notation `C :> Set` signifies that there is a coercion from constructive setoids to `Set`. This allows, in Coq, to use a term of type `CSetoid` (a constructive setoid) in places where a term of type `Set` (a set) is asked for: the type checker will insert `C`, the projection on the first field of the record.

The definition says that a constructive setoid (a term of type `CSetoid`) is a tuple $\langle C, =, \#, a_1, a_2, a_3, a_4\rangle$, with $C : \mathsf{Set}$, $=$ and $\#$ binary relations over C, a_1 a proof of the irreflexivity of $\#$, a_2 a proof of the symmetry of $\#$, a_3 a proof of the *cotransitivity* of $\#$ and a_4 saying that $\#$ is *tight* with respect to $=$. On real numbers the apartness is basic; a constructive setoid axiomatizes its basic properties, of which the cotransitivity is the most noteworthy. Cotransitivity gives the positive meaning to the apartness.

It is also possible to do without equality altogether and define $=$ as the negation of $\#$. A reason for not doing so is that $=$ is very basic and the universal algebraic laws are all stated in terms of $=$. With respect to functions between constructive setoids, there are now several choices. Given the constructive setoids $S := \langle C, =, \#, a_1, a_2, a_3, a_4\rangle$ and $S' := \langle C', =', \#', a_1', a_2', a_3', a_4'\rangle$, there are the terms of type $C \to C'$, which can be seen as algorithms that take a representation of an element of S and return a representation of an element in S'. Obviously, such an algorithm need not preserve the equality. For a *constructive setoid function*, we want more. First of all that it preserves the equality: we want to consider only those $f : C \to C'$ for which $\forall x, y{:}C.(x = y) \to f(x) =' f(y)$ holds. As we are in a constructive setting, we even want a bit more: we want a *constructive setoid function* to reflect the apartness. This is called *strong extensionality* and it is defined as (for f unary and g binary, respectively)

$$\forall x, y{:}C. f(x) \#' f(y) \to (x \# y)$$
$$\forall x_1, x_2, y_1, y_2{:}C. g(x_1, x_2) \#' g(y_1, y_2) \to (x_1 \# y_1) \vee (x_2 \# y_2)$$

Strong extensionality of a function f says that f cannot distinguish (via $\#'$) two elements that were indistinguishable (via $\#$). Note that strong extensionality of binary functions arises naturally from the notion of binary product on setoids. Strong extensionality of f implies that it preserves the equality, so we don't have to assume that separately. As an example of the power (and usefulness) of the notion, we remark that strong extensionality of multiplication $*$ (see below) implies that $\forall x, y{:}C.(x * y)\#0 \rightarrow (x\#0 \wedge y\#0)$ holds.

Coq Definition 2.

```
Record CRing     : Type :=
{ R              :> CSetoid;
  zero           : R;
  add            : R->R->R;
  add_strext     : (x1,x2,y1,y2:R)((x1 [+] y1) [#] (x2 [+] y2)) ->
                                             (x1 [#] x2)\/(y1 [#] y2);
  add_assoc      : (x,y,z:R)((x [+] (y [+] z)) [=]
                                                   ((x [+] y) [+] z));
  add_unit       : (x:R)((x [+] zero) [=] x);
  add_commut     : (x,y:R)((x [+] y) [=] (y [+] x));

  minus          : R->R;
  minus_strext   : (x,y:R)([--]x [#] [--]y) -> (x [#] y);
  minus_proof    : (x:R)((x [+] [--]x) [=] zero);
  one            : R;
  mult           : R->R->R;
  mult_strext    : (x1,x2,y1,y2:R) ((x1 [*] y1) [#] (x2 [*] y2))->
                                             (x1 [#] x2)\/(y1 [#] y2);
  mult_assoc     : (x,y,z:R)
                        ((x [*] (y [*] z)) [=] ((x [*] y) [*] z));
  mult_unit      : (x:R)((x [*] one) [=] x);
  mult_commut    : (x,y:R)((x [*] y) [=] (y [*] x));
  dist           : (x,y,z:R) ((x [*] (y [+] z)) [=]
                                           ((x [*] y) [+] (x [*] z)));
  non_triv       : (one [#] zero)                                     }.
```

So, a constructive ring consists of a constructive setoid as a carrier, extended with an addition function `add`, with infix notation `[+]`, a unary minus function, `minus`, with prefix notation `[--]` and a multiplication function `mult`, with infix notation `[*]`. The axioms are the usual ones, apart from the fact that we assume all functions to be strongly extensional.

A constructive field is a ring extended with a reciprocal function, which is a *partial function* on the type F. The partiality is expressed by requiring both an $x : F$ and a proof of $x\#0$ as input. In the formalization the reciprocal is defined as a function on the *subsetoid* of non-zeros of F. Given a predicate over a setoid, say `P : S -> Prop`, the 'set' of elements satisfying `P` is defined by the record:

Coq Definition 3.

```
Record subsetoid [S : CSetoid; P : S -> Prop] : Set :=
  { elem  :> S;
    prf   : (P elem)
  }.
```

This subsetoid is then turned into a constructive setoid by inheriting the apartness and equality from those on `S` (i.e. ignoring the proof term).

To define fields we use the subsetoid of non-zeroes of a ring. Given `R : CRing`, we define `(NonZeros R)` as `(subsetoid R [x:F](x [#] zero))`. Constructive fields are then defined by the following record structure.

Coq Definition 4. `Record CField : Type :=`

```
{ F              :> CRing;
  rcpcl          : (NonZeros F) -> (NonZeros F);
  rcpcl_strext   : (x,y:(NonZeros F))
                     ((rcpcl x) [#] (rcpcl y)) -> (x [#] y);
  rcpcl_proof    : (x:(NonZeros F))
                     ((nzinj x) [*] (nzinj (rcpcl x )) [=] one) }.
```

Here, `nzinj : (NonZeros F) -> F` is the function that maps a non-zero (of a ring) to the underlying element. So it is just the projection to the `elem` field for the subsetoid of non-zeros.

Coq Definition 5. `Record COrdField : Type :=`

```
{ OF             :> CField;
  [<]            : OF->OF->Prop;
  less_strext    : (x1,x2,y1,y2:OF) (x1 [<] y1) ->
                               (x2 [<] y2)\/(x1 [#] x2)\/(y1 [#] y2);
  less_trans     : (x,y,z:OF)(x [<] y) -> (y [<] z) -> (x [<] z);
  less_irr       : (x:OF)~(x [<] x);
  less_asym      : (x,y:OF)(x [<] y) -> ~(y [<] x);
  add_resp_less  : (x,y:OF)(x [<] y) ->
                                     (z:OF)((x [+] z) [<] (y [+] z));
  times_resp_pos : (x,y:OF)(zero [<] x) -> (zero [<] y)->
                                (zero [<] (x [*] y));
  less_conf_ap   : (x,y:F)(x [#] y) <-> ((x [<] y)\/(y [<] x))    }.
```

An ordered field is the union of a field with an ordered ring. Apart from the standard requirements for the ordering `[<]`, we require it to be *strongly extensional*, which is asserted by `less_strext`. This is (just like strongly extensional functions) a positive way of saying that the relation cannot distinguish between elements that are indistinguishable. Note that it follows from the strong extensionality that order respects the equality ($x < y \wedge y = z \rightarrow x < z$ etcetera). The final axiom connects apartness with the ordering in the expected way and together with the cotransitivity of the apartness implies the important cotransitivity property of $<$, i.e. the property $x < y \rightarrow x < z \vee z < y$.

A *real number structure* is an ordered field that is *Archimedean* (every real is majorized by some natural number), and Cauchy complete, i.e. every Cauchy sequence has a limit. For the Archimedean property, we define, for `F` an arbitrary field, the function `nreal : nat -> F`, which maps `O` to `zero` and `(S n)` to `((nreal n) [+] one)`. If `F` is ordered, this is an injection. We want to define a Cauchy sequence over the ordered field F as an $s{:}\mathbb{N}{\rightarrow}F$ such that

$$\forall \varepsilon{:}F_{>0}.\exists N{:}\mathbb{N}.\forall m \geq N.(|s_m - s_N| < \varepsilon).$$

However, constructively, the absolute value function is not definable in an arbitrary ordered field, so it has to be replaced with something else. For this purpose the notion `AbsSmall` has been introduced.

Coq Definition 6.
```
AbsSmall [e,x:F]: Prop := ([--]e [<] x) /\ (x [<] e).
```

So `AbsSmall e x` expresses that, for a positive `e`, `x` is small with respect to `e`. Now the Cauchy property can be defined.

Coq Definition 7.
```
Definition cauchy [g:nat->F]: Prop :=
  (e:F)(zero [<] e) ->
    (EX N:nat | (m:nat)(le N m) -> (AbsSmall e ((g m)[-](g N))) ).
```

Note that we do not explicitly require Cauchy sequences to have a modulus of convergence. By the Axiom of Choice, every Cauchy sequence has a modulus of convergence and the Axiom of Choice is provable in our framework. Next, for a real number structure we assume a function `lim` that takes a Cauchy sequence and returns its limit.

Coq Definition 8.
```
Record CReals : Type :=
{IR            :> CField;
lim            : (s:nat->IR)(cauchy s)->IR;
lim_proof      : (s:nat->F)(c:(cauchy s))
                   (e:F)(zero [<] e) ->
                     (EX N:nat | (m:nat)(le n m) ->
                                  (AbsSmall e (s m)[-](lim s c)));
arch_proof     : (x:F)(EX n:nat | (x [<] (nreal n)))              }.
```

2.1 On the choice of primitives: $\frac{1}{k}$ versus ε

The notion of Cauchy sequence (and similarly the notion of limit) is defined above via the 'ε-definition':

$$\forall \varepsilon{:}F_{>0}.\exists N{:}\mathbb{N}.\forall m \geq N.(|s_m - s_N| < \varepsilon).$$

Let us call such a sequence s an ε-Cauchy sequence. An alternative is the '$\frac{1}{k}$-definition':

$$\forall k{:}\mathbb{N}.\exists N{:}\mathbb{N}.\forall m \geq N.(|s_m - s_N| < \frac{1}{k+1})$$

and we will call this a $\frac{1}{k}$-Cauchy sequence. Any ε-Cauchy sequence is a $\frac{1}{k}$-Cauchy sequence. For the reverse implication we need the Archimedean property. (To find an $N \in \mathbb{N}$ such that $\forall m \geq N.|s_m - s_N| < \varepsilon$, we have to find $k, N \in \mathbb{N}$ such that $\forall m \geq N.|s_m - s_N| < \frac{1}{k}$ and $\frac{1}{k} < \varepsilon$. The inequality $\frac{1}{k} < \varepsilon$ is solved by applying the Archimedean property to $\frac{1}{\varepsilon} < k$.)

Similarly one can define the notion of limit via the ε-definition (the ε-limit) or via the $\frac{1}{k}$-definition (the $\frac{1}{k}$-limit). If s has an ε-limit, then s has a $\frac{1}{k}$-limit and the reverse holds by the Archimedean property.

So, in an Archimedean ordered field, the two notions are equivalent. In a non-Archimedean field (e.g. a non-standard model of the reals) they are not equivalent and one may wonder what the 'best' definition of Cauchy sequence is (and of limit). We feel that the question isn't very relevant, because for the analysis of non-standard reals, sequences of length ω are just too short. We have a slight preference for the ε-definitions for the following reasons.

(1) If one defines Cauchy-completeness as 'all $\frac{1}{k}$-Cauchy sequences have a $\frac{1}{k}$-limit', then $1, \frac{1}{2}, \frac{1}{3}, \ldots$ has a limit, which seems unnatural in non-standard reals (all infinitesimals are limit of this sequence). Also, limits are not unique anymore: if a and b are $\frac{1}{k}$-limit of s, then $\forall k.|a-b| < \frac{1}{k+1}$, but to conclude $a = b$ from this we need the Archimedean property.

(2) For constructing the reals out of the rationals, we consider Cauchy-sequences of rationals. The construction can be made more modular by considering Cauchy sequences over an arbitrary ordered field (even a non-Archimedean one). It turns out that $\frac{1}{k}$-Cauchy sequences over an ordered field do not necessarily form a field, whereas ε-Cauchy sequences do. See the discussion in Section 4 (after Definition 4.8) for details.

As a final remark we want to point out that there is yet another (useful) definition of Cauchy completeness as 'all $\frac{1}{k}$-Cauchy sequences have an ε-limit'. Then the Archimedean property follows from Cauchy completeness: let $x > 0$ and to find an $n \in \mathbb{N}$ with $n > x$ consider the $\frac{1}{k}$-Cauchy sequence $1, \frac{1}{2}, \frac{1}{3}, \ldots$. This sequence has an ε-limit, and if we take ε to be $\frac{1}{x}$, we find an $N \in \mathbb{N}$ for which

$$\forall m \geq N. |\frac{1}{m+1} - \frac{1}{N+1}| < \frac{1}{x}.$$

Taking m to be $N+1$, we conclude that $x < (N+1)(N+2)$ and we are done.

3 Rational numbers

The job is to construct a real number structure, that is, a term of type `CReals`. It will be constructed from Cauchy sequences of rational numbers, so we need to have a construction of rational numbers in Coq. In the Coq standard library the rational numbers are not developed. So we have to construct them. Arithmetic is developed quite considerably in Coq: natural numbers are defined as an inductive type nat with constructors zero and successor, and relations and operations on them are all defined using induction or recursion. The inductive natural numbers are very useful for proving theorems about, but for actual computation this unary representation is very inefficient. For this reason, the integers are defined as the disjoint union of the one element type and two copies of the type of binary sequences (one denoting the positive numbers and one denoting the negative numbers). This yields a relatively fast (standard binary) implementation of the integers.

We represent an element of $\mathbb{Q}$ as a pair $\langle p, n \rangle$ of an integer and a natural number, denoting the rational $\frac{p}{n+1}$. This method is rather useful as it avoids carrying around the proof obligation corresponding to a non zero denominator.

In Coq, this is encoded using the `Record` constructor. We define the equality on $\mathbb{Q}$ in such a way that it corresponds to the intended interpretation of the pair $\langle p,n\rangle$: $\langle p,n\rangle =_{\mathbb{Q}} \langle q,m\rangle$ is defined as $p(m+1) = q(n+1)$. This means that we identify the two rationals $\frac{1}{2}$ and $\frac{2}{4}$. So unlike the case of natural numbers and integers, we deal with an inductive type for which the useful equality is not Leibniz equality. This is only because our way of representing rational numbers has redundancy in contrast to the definition of natural numbers and integers. Whenever we want to prove an equality on $\mathbb{Q}$, it boils down to proving an equality between integers, which we can verify using the arithmetics developed in the `ZArith` library. We define the *apartness* relation on $\mathbb{Q}$ to be the negation of the equality and we prove the required properties for it. The constants zero and one and the addition operation are defined in the expected way: $\langle p,n\rangle+\langle q,m\rangle :=$ $\langle p(m+1)+q(n+1), nm+n+m\rangle$. Similarly, the unary minus and the multiplication function are defined in the expected way. Then we prove that these operations are strongly extensional and satisfy the ring properties.

Defining the reciprocal is a bit more complicated, since we have to give a partial function taking nonzero elements of $\mathbb{Q}$ to nonzero elements of $\mathbb{Q}$. The idea is that, as $\langle p,n\rangle$ represents the rational $\frac{p}{n+1}$, the inverse of $\langle p,n\rangle$ should be $\langle n+1, p-1\rangle$. But $p-1$ should be a natural, so we have to take $\langle -(n+1), -(p-1)\rangle$ if $p < 0$. (The case $p = 0$ does not occur, as we only consider the non-zeros of $\mathbb{Q}$.) So, the inverse on $\mathbb{Q}_{\#0}$ is defined as follows.

$$\frac{1}{\langle p,n\rangle} := \begin{cases} \langle n+1, p-1\rangle & \text{if } p > 0 \\ \langle -(n+1), -(p-1)\rangle & \text{if } p < 0 \end{cases}$$

We prove that the inverse is strongly extensional and satisfies the field axiom. We have equipped our model of rational numbers with all the constructive field operations. In Coq terms, we have given a term of type `CField`. Now we define an order relation on $\mathbb{Q}$ in the natural way, using the order on $\mathbb{Z}$:

$$\langle p,n\rangle <_{\mathbb{Q}} \langle q,m\rangle := p*(m+1) <_Z q*(n+1).$$

We prove that $<_{\mathbb{Q}}$ is strongly extensional, and that it satisfies the order axioms. It is also easy to prove that $\mathbb{Q}$ is Archimedean. So we wrap up what we did in this section, in the following theorem:

Theorem 3.1. *$\mathbb{Q}$ together with the operations and relations defined above forms an Archimedean constructive ordered field.*

The rational numbers are the 'simplest' example of a constructive ordered field: every constructive ordered field contains a copy of the rational numbers. An important property of rational numbers is that equality is decidable (which is, for example, not the case for the set of Cauchy sequences over $\mathbb{Q}$). Decidability of equality allows to define the maximum function. In general, this is not possible for constructive ordered fields. However it is possible for real number structures, see [10].

4 Real numbers

Now we need to construct a real number structure out of the set of Cauchy sequences over the rationals. Unless stated otherwise, we will always talk about ε-Cauchy sequences (see Section 2.1). For reasons of readability, we will not use Coq notation, but ordinary mathematical notation. So, for example, we write $\mathbb{N}$ for the type of naturals (and $\mathbb{Q}$ for the type of rationals as we already did in the previous section). Instead of working with the concrete rationals $\mathbb{Q}$, we prove a general result about Archimedean constructive ordered fields.

Notation. Let F be a constructive ordered field. We denote the set of Cauchy sequences over F by $\mathrm{CauchySeq}_F$.

Theorem 4.1. *Let F be a constructive ordered field. If F is Archimedean then $CauchySeq_F$ is a real number structure.*

The largest part of the formalization consists of the proof of this theorem. Instantiating it with the term obtained in Theorem 3.1, we get a concrete term of the type 'real number structure', and our implementation is finished. We divide the proof of Theorem 4.1 into two separate parts, especially to highlight the use of the Archimedean property. We prove the following two results.

Theorem 4.2. *Let F be a constructive ordered field. Then $CauchySeq_F$ is also a constructive ordered field.*

Theorem 4.3. *Let F be a constructive ordered field. If F is Archimedean then $CauchySeq_F$ is Archimedean and Cauchy complete.*

For the proof of Theorem 4.2, we systematically define the constructive ordered field operations and relations on $\mathrm{CauchySeq}_F$. We introduce the following shorthands, corresponding to Coq Definition 6.

Notation. For x and ε elements of a constructive ordered field F, we denote $\mathrm{AbsSmall}(\varepsilon, x) := -\varepsilon < x \wedge x < \varepsilon$, and $\mathrm{AbsBig}(\varepsilon, x) := 0 < \varepsilon \wedge (x < -\varepsilon \vee \varepsilon < x)$.

The familiar real number properties that are stated using the absolute value function can all be stated in terms of these two predicates. We now define the relations on Cauchy sequences.

Definition 4.4 (order). *Let $g, h : \mathrm{CauchySeq}_F$, we define $g < h$ as*

$$\exists \varepsilon{:}F_{>0}.\exists N{:}\mathbb{N}.\forall m \geq N.(\varepsilon < h_m - g_m).$$

An alternative definition of the ordering (that goes along naturally with the alternative definition of Cauchy sequence, as discussed in Section 2.1) can be given using $\frac{1}{k}$ instead of ε as follows: $g < h$ if $\exists k \in \mathbb{N}.\exists N{:}\mathbb{N}.\forall m \geq N.(\frac{1}{k+1} < h_m - g_m)$. If F is Archimedean, the $\frac{1}{k}$-order and the ε-order are the same, but in general only the first implies the second and not the other way around. If F is non-Archimedean, then in $\mathrm{CauchySeq}_F$ with the $\frac{1}{k}$-order, some distinct elements become identified, which may be undesirable.

Definition 4.5. *We define apartness # and equality = on Cauchy sequences in terms of order as follows.* $f\#g := f < g \vee g < f$, $f = g := \neg(f\#g)$.

We prove that # satisfies the axioms of apartness. Then we define some equivalent definitions for apartness and equality, that are useful in practice. We mention two of them.

Lemma 4.6. *Let* $f, g : \mathrm{CauchySeq}_F$. $f\#g$ *is equivalent to*

$$\exists\varepsilon{:}F_{>0}.\exists N{:}\mathbb{N}.\forall m \geq N.\mathrm{AbsBig}(\varepsilon, f_m - g_m).$$

$f = g$ *is equivalent to*

$$\forall\varepsilon{:}F_{>0}.\exists N{:}\mathbb{N}.\forall m \geq N.\mathrm{AbsSmall}(\varepsilon, f_m - g_m).$$

The following lemma states another important property of Cauchy sequences that is used several times in our proofs. It gives us an upper-bound for a Cauchy sequence.

Lemma 4.7. *Let* $s : \mathrm{CauchySeq}_F$. *Then* $\exists K{:}F_{\#0}.\forall m{:}\mathbb{N}.\mathrm{AbsSmall}(K, s_m)$.

To turn the Cauchy sequences into a ring, we define zero and one as the sequences which are constant zero, respectively one. Similarly we define addition, minus and multiplication on Cauchy sequences via the pointwise addition, minus and multiplication. We prove that these operations are strongly extensional. In the case of multiplication, the proof of strong extensionality uses Lemma 4.7. Finally, we prove that we have constructed a constructive ring.

Now we have to define the reciprocal. Let s be a Cauchy sequence and suppose $s\#0$. By Lemma 4.6, this means that, from a certain N onwards we know that we are a positive distance from zero. So, determine ε and N such that

$$\forall m \geq N.\mathrm{AbsBig}(\varepsilon, s_m).$$

So for $m \geq N$, the elements s_m are all $\#0$. Now we take the reciprocals of these elements to get the reciprocal of the Cauchy sequence x:

Definition 4.8 (Reciprocal). *Let the non-zero Cauchy sequence* s *be given and let* N *be such that for* $m \geq N$, $s_m\#0$. *Define the sequence* s^{-1} *as follows.*

$$s_m^{-1} = \begin{cases} 0 & \text{if } m < N \\ \frac{1}{s_m} & \text{if } m \geq N \end{cases}$$

This definition uses the Axiom of Choice to assign an N to each s. We prove that the above sequence is a Cauchy sequence and is apart from zero. Then we show that the operation $(\_)^{-1}$ is strongly extensional and satisfies the field axiom for reciprocal.

Remark 4.9 ($\frac{1}{k}$-Cauchy sequences versus ε-Cauchy sequences). If we use $\frac{1}{k}$-Cauchy sequences, the reciprocal can not be defined without assuming the Archimedean property.

(1) If we use the ε-order (and hence the ε-apartness and ε-equality of Definitions 4.4, 4.5), one needs the Archimedean property to show that s^{-1} is a $\frac{1}{k}$-Cauchy sequence: we need to find $N \in \mathbb{N}$ such that $\forall m \geq N |\frac{1}{s_m} - \frac{1}{s_N}| < \frac{1}{k+1}$. This is equivalent to finding N such that $\forall m \geq N |\frac{s_m - s_N}{s_m s_N}| < \frac{1}{k+1}$. If we have a lower bound $\frac{1}{K_0} \in \mathbb{N}$ on $|s_m s_{N_0}|$ (for all m from a certain N_0 onward), this N can be computed from the fact that s is a $\frac{1}{k}$-Cauchy sequence. The existence of the lower bound $\frac{1}{K_0}$ is equivalent to the Archimedean property.

(2) If we use the $\frac{1}{k}$-order (see the remark just after Definition 4.4) and also $\frac{1}{k}$-apartness and $\frac{1}{k}$-equality, then s^{-1} is a $\frac{1}{k}$-Cauchy sequence indeed. (The lower bound $\frac{1}{K_0}$ that was required above, is now derived from the fact that $s\#0$, which now yields: $\exists K \exists N \forall m \geq N |s_m| > \frac{1}{K}$.) But now we can not prove that $s^{-1}\#0$, for $s\#0$, because the reciprocal of an 'infinite element' is just 0 under the $\frac{1}{k}$-equality. (We need the Archimedean property.)

Finally we prove that the order as defined in Definition 4.4 satisfies the required axioms and then we have proved Theorem 4.2.

In order to prove Theorem 4.3, we assume that F is Archimedean and let s:CauchySeq$_F$. We use Lemma 4.7 to obtain a bound K:F for s. The Archimedean property for F gives us an n:$\mathbb{N}$ such that $K < n$ in F. It is now easy to prove that the constant sequence $\lambda x{:}\mathbb{N}.n$ bounds s in CauchySeq$_F$.

To prove completeness, we use a kind of diagonalization argument. Note, however, that if $s^1, s^2, \ldots$ are Cauchy sequences, then $\lambda i{:}\mathbb{N}.s^i_i$ may not be the right choice for the limit of $\{s^i\}_{i=0}^{\infty}$ (it may not even be a Cauchy sequence). Instead we have to take $\lambda i{:}\mathbb{N}.s^i_{\tau(i)}$, where $\tau(i)$ is a number N (depending on the sequence s^i) such that s^i is *sufficiently close* to its limit from N onwards. To formalize the notion of 'sufficiently close', we use $\frac{1}{i+1}$ as a bound.

Definition 4.10. *Given a sequence of Cauchy sequences $\{s^i\}_{i=0}^{\infty}$, we define a function $\tau : \mathbb{N} \to \mathbb{N}$ satisfying*

$$\forall m > \tau(i).\text{AbsSmall}(\frac{1}{i+1}, s^i_m - s^i_{\tau(i)}).$$

The map $\tau(i)$ is defined using the Cauchy property for the sequence s^i, which gives us (for $\varepsilon = \frac{1}{i+1}$) an N such that the above holds. Due to the fact that Cauchy sequences are not represented using a *modulus of convergence*, but via an existential quantifier, we need the Axiom of Choice to define τ.

Definition 4.11. *Given the sequence of Cauchy sequences $\{s^i\}_{i=0}^{\infty}$, we define the limit sequence l by*

$$l := \lambda n.s^n_{\tau(n)}$$

To prove that l has the Cauchy property we need the Archimedean property: l is 'convergent with respect to $\frac{1}{k}$' by construction, but it needs to be 'convergent with respect to ε'. The proof that l is the limit of $\{s^i\}_{i=0}^{\infty}$ similarly uses the Archimedean property and moreover the fact that the canonical embedding of F into CauchySeq_F is dense.

This finishes the proof of Theorem 4.3 and hence the proof of Theorem 4.1. We already have a proof that $\mathbb{Q}$ is Archimedean and by applying Theorem 4.1 to this result we have proved the following theorem.

Theorem 4.12. $\text{CauchySeq}_{\mathbb{Q}}$, *the set of Cauchy sequences of rational numbers, together with the relations and operations defined on Cauchy sequences as in 4.4-4.11, is a constructive real number structure.*

5 Homomorphisms and isomorphisms

In the end of Section 3 we mentioned that every constructive ordered field F contains a 'copy' of $\mathbb{Q}$. In this and the following Section, we will extend this to real number structures: every real number structure contains a 'copy' of $\text{CauchySeq}_{\mathbb{Q}}$. The result is even stronger: every real number structure is essentially $\text{CauchySeq}_{\mathbb{Q}}$. More precisely, we prove that every two real number structures are isomorphic (and hence isomorphic to $\text{CauchySeq}_{\mathbb{Q}}$). To do this we define the notion of a morphism between two real number structures.

Definition 5.1. *Let R_1 and R_2 be two real number structures. We say that $\varphi : R_1 \longrightarrow R_2$ is a* homomorphism from R_1 to R_2, *if it has the following properties.*

1. *(strongly extensional)* $\forall x, y : R_1.\ \varphi(x) \# \varphi(y) \to x \# y$.
2. *(order preserving)* $\forall x, y : R_1.\ x < y \to \varphi(x) < \varphi(y)$.
3. *(addition preserving)* $\forall x, y : R_1.\ \varphi(x + y) = \varphi(x) + \varphi(y)$.
4. *(multiplication preserving)* $\forall x, y : R_1.\ \varphi(x * y) = \varphi(x) * \varphi(y)$.

The equality used in this definition is the setoid equality. (In the definition, the relations and operations are taken from the appropriate real number structures, R_1, resp. R_2, which is left implicit.) Note that a homomorphism between real number structures is just a homomorphism between the underlying ordered rings. The preservation of reciprocals $(\varphi(\frac{1_{R_1}}{x}) = \frac{1_{R_2}}{\varphi(x)})$ and limits $(\varphi(\lim\{g_i\}_{i=0}^{\infty}) = \lim\{\varphi(g_i)\}_{i=0}^{\infty})$ comes as a consequence. To state the latter we first have to show that φ maps Cauchy sequences over R_1 to Cauchy sequences over R_2. In the following, let φ be a homomorphism from R_1 to R_2.

Proposition 5.2.
1. *(order reflecting)* $\forall x, y : R_1.\ \varphi(x) < \varphi(y) \to x < y$.
2. *(apartness preserving)*$\forall x, y : R_1.\ x \# y \to \varphi(x) \# \varphi(y)$.
3. *(zero preserving)* $\forall x : R_1.\ \varphi(0_{R_1}) = 0_{R_2}$.
4. *(minus preserving)* $\forall x : R_1.\ \varphi(-x) = -\varphi(x)$.
5. *(unit preserving)* $\forall x : R_1.\ \varphi(1_{R_1}) = 1_{R_2}$.
6. *(reciprocal preserving)* $\forall x : R_1.x \# 0_{R_1} \to (\varphi(x) \# 0_{R_2} \wedge \varphi(\frac{1_{R_1}}{x}) = \frac{1_{R_2}}{\varphi(x)})$.
7. *(Cauchy preserving) If $\{g_i\}_{i=0}^{\infty}$ is Cauchy, then $\{\varphi(g_i)\}_{i=0}^{\infty}$ is Cauchy.*

Proof (of 7). This follows from the following property of φ:

$$\forall \varepsilon{:}R_2.\varepsilon > 0 \to \exists \delta{:}R_1.\delta > 0 \wedge \varphi(\delta) < \varepsilon \tag{1}$$

(which again is a direct consequence of the Archimedean property for R_2). To find, for a given $\varepsilon > 0$, the $N \in \mathbb{N}$ such that $\forall m \geq N |\varphi(g_m) - \varphi(g_N)| < \varepsilon$, we take the $\delta{:}R_1$ that results from (1) and then we take $N \in \mathbb{N}$ (using the Cauchy property of $\{g_i\}_{i=0}^{\infty}$) to be such that $\forall m \geq N |g_m - g_N| < \delta$. Then $\forall m \geq N |\varphi(g_m) - \varphi(g_N)| < \varphi(\delta) < \varepsilon$. (N.B. With $\frac{1}{k}$-Cauchy sequences, we wouldn't need the Archimedean property in this proof, because the '$\frac{1}{k}$-analogue' of (1) is immediate) □

Lemma 5.3. *The homomorphism $\varphi : R_1 \longrightarrow R_2$ preserves limits, that is* $\forall g{:}\text{CauchySeq}_{R_1}.\varphi(\lim\{g_i\}_{i=0}^{\infty}) = \lim\{\varphi(g_i)\}_{i=0}^{\infty}$.

An isomorphism is defined as a pair of homomorphisms $\langle \varphi, \psi \rangle$ that are inverses to each other, i.e. $\forall x{:}R_2.\varphi(\psi(x)) =_{R_2} x$ and $\forall x{:}R_1.\psi(\varphi(x)) =_{R_1} x$. Note that to define a composition of homomorphisms, we do not just compose the maps but we also 'compose' the two homomorphism-proofs into a proof that the composed map is a homomorphism.

We now construct an isomorphism between any two real number structures. (An alternative is to show that any real number structure is isomorphic to $\text{CauchySeq}_{\mathbb{Q}}$, which amounts to the same technical work.) The basic idea is to define a map which is the 'identity' on rational numbers and then to extend this map in the canonical way to Cauchy sequences We first define for any real number structure R, the canonical injection $\mathbb{Q}2R$ of $\mathbb{Q}$ into R. (This injection is defined by first defining the injection nring of natural numbers into R and the injection zring of integers into R. Then $\mathbb{Q}2R$ is the map that takes the term $\langle p, q \rangle : \mathbb{Q}$ to $\frac{\text{zring } p}{\text{nring}(q+1)}$.) The map $\mathbb{Q}2R$ is strongly extensional and preserves addition, multiplication, negation, order, AbsSmall and the Cauchy property. Moreover, the image of $\mathbb{Q}$ under $\mathbb{Q}2R$ is dense in R.

If no confusion arises, we omit the injection nring and $\mathbb{Q}2R$ that map $\mathbb{N}$, respectively $\mathbb{Q}$ into R.

Theorem 5.4. *For any $x : R$, we can construct a sequence $q_0, q_1, \ldots$ of elements of $\mathbb{Q}$ such that $x = \lim\{q_i\}_{i=0}^{\infty}$. In other words, every real number is the limit of a Cauchy sequence of (images of) rational numbers.*

Proof. We construct (using Axiom of Choice), two Cauchy sequences of rationals $q_0, q_1, \ldots$ and $r_0, r_1, \ldots$ which both converge to x. Using the Archimedean property of R for x and $-x$, we obtain two natural numbers N_1 and N_2 such that $-N_2 < x < N_1$. Define q_0 as N_2 and r_0 as N_1 (both seen as elements of $\mathbb{Q}$). So $q_0 < x < r_0$. Now assume that we have constructed q_n and r_n. To get q_{n+1} and r_{n+1} we use an interval trisection argument (which is the constructive counterpart of interval bisection in classical analysis). Since $\frac{2q_n+r_n}{3} < \frac{q_n+2r_n}{3}$, we have (using cotransitivity of $<$) *either* $\mathbb{Q}2R(\frac{2q_n+r_n}{3}) < x$ *or* $x < \mathbb{Q}2R(\frac{q_n+2r_n}{3})$. In the first case we set $q_{n+1} := \frac{2q_n+r_n}{3}$, $r_{n+1} = r_n$ and in the second case we set $q_{n+1} := q_n$, $r_{n+1} := \frac{q_n+2r_n}{3}$. We prove following facts about q_i and r_i:

1. $\forall n{:}\mathbb{N}(r_n - q_n = (r_0 - q_0)(\frac{2}{3})^n)$,
2. $\forall m, n{:}\mathbb{N}(m \leq n \to q_m \leq q_n \wedge r_n \leq r_m)$,

Hence $\{q_i\}_{i=0}^{\infty}$ and $\{r_i\}_{i=0}^{\infty}$ are Cauchy sequences in $\mathbb{Q}$ and the injections of these sequences in R are Cauchy sequences in R. We also prove the following facts.

$$\forall n{:}\mathbb{N}(q_n < x < r_n),$$
$$\forall n{:}\mathbb{N}(\text{AbsSmall}((r_0 - q_0)(\frac{2}{3})^n, x - q_n)).$$

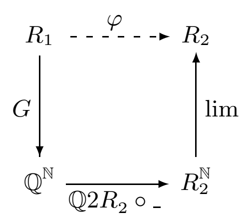
And it follows (using the Archimedean property) that x is the limit of $\{q_i\}_{i=0}^{\infty}$ □

Definition 5.5. *For $x : R$, we define $G(x)$ as the following Cauchy sequence over $\mathbb{Q}$.*

$$G(x) := \lambda n.q_n,$$

where $\{q_i\}_{i=0}^{\infty}$ is the sequence constructed from x in the proof of Theorem 5.4.

We are now ready to construct an isomorphism $\langle \varphi, \psi \rangle$ between two real number structures R_1 and R_2. For clarity, we present a sequence $\{x_i\}_{i=0}^{\infty}$ as $\lambda n{:}\mathbb{N}.x_n$. We define $\varphi : R_1 \to R_2$ by composing the maps G, $\mathbb{Q}2R_2$ and lim as indicated in the following diagram. So, $\varphi(x)$ is the map $\lim(\lambda n{:}\mathbb{N}.\mathbb{Q}2R_2(G(x)_n))$ (for $x : R_1$). Similarly we define $\psi : R_2 \to R_1$.



We have the following properties of lim and G.

- lim and G preserve $<$, $+$ and $*$.
- lim and G reflect $<$.

Using these properties we prove the following for φ and ψ.

Proposition 5.6. *1. φ and ψ are inverses to each other.*
2. φ and ψ are strongly extensional and they preserve order, addition and multiplication.

Then, by Lemma 5.3, φ and ψ are homomorphisms, and since they are inverses to each other, they form an isomorphism from R_1 to R_2.

Theorem 5.7. *All real number structures are isomorphic.*

6 Cauchy completion versus order completion

Classically, Dedekind cuts are an alternative way of constructing the reals out of the rationals. In this approach, the emphasis lies on the order completion of the rationals. However, the classical least upper bound principle, does not hold constructively: for a subset of $\mathbb{Q}$ to have a least upper bound, it is not enough to be bounded. But the principle can be modified, using a constructive version of boundedness. This approach is taken in the axiomatization of the reals in [2]: the axioms for the reals are the same as ours except for the Cauchy completeness, which is replaced by a constructive version of the least upper bound principle. We will show that the two axiomatizations are equivalent. To introduce the axiom of [2], we need some notations and definitions. First note that in type theory, a subset is formalized via a predicate over a 'carrier type'. As we will not be using type theoretic notation, we just write $x \in S$ if we want to denote that x is in the subset S, leaving the carrier type and the precise encoding of subsets in type theory implicit.

Definition 6.1. *Let F be an Archimedean constructive ordered field. Let $S \subseteq F$, nonempty. An element $b : F$ is the* least upper bound of S*, if the following hold.*

- *b is an* upper bound of S*, that is, $\forall s \in S. s \leq b$*
- *for each $b' < b$ there exists $s : S$ such that $s > b'$,*

where $\leq$ is defined by $x \leq y := \forall z(x > z \rightarrow y > z)$ (which is equivalent to $\neg(y < x)$).

We will write $x \geq S$ if x is an *upper-bound* of the set S. It is easily shown that a least upper bound is unique, if it exists. The classical axiom says that all nonempty bounded subsets have a least upper-bound; constructively speaking, only the *weakly located subsets* do. The following definition is implicit in [2].

Definition 6.2. *A subset S of F is* weakly located *if (1) it is inhabited, (2) it has an upper bound and (3) for all $x, y : F$ with $x < y$, either $y \geq S$ or $\exists s \in S(s > x)$.*

The following axiom replaces the Cauchy completeness axiom. We show that the axiom holds for all real number structures as defined in Section 2.

Least Upper Bound Principle. Every weakly located subset has a least upper bound.

The argument in the proof of the next theorem is used in [3] to justify the least upper bound principle.

Theorem 6.3. *Let F be a real number structure, then F satisfies the least upper bound principle.*

Proof. Assume S is a weakly located subset of F. Let $s \in S$ and $b \geq S$. We construct a least upper bound for S by repeating the interval trisection argument that we also used to prove Theorem 5.4. So, we define Cauchy sequences $\{l_i\}_{i=0}^{\infty}$ and $\{r_i\}_{i=0}^{\infty}$ such that $\forall i(l_i < r_i)$, $\{l_i\}_{i=0}^{\infty}$ and $\{r_i\}_{i=0}^{\infty}$ have the same limit and $\forall i(r_i \geq S \wedge \exists s' \in S(s > l_i))$.

We start by taking $l_0 := s-1$ and $r_0 := b+1$. Now, given that we have l_n, r_n satisfying the requirements, we consider $x = \frac{2l_n+r_n}{3}$ and $y = \frac{l_n+2r_n}{3}$. Then $x < y$ so by the weakly-locatedness of S we can distinguish cases:

- if $y \geq S$, take $l_{n+1} := l_n$ and $r_{n+1} := y$.
- if there is an $s' \in S$ such that $s' > x$, take $l_{n+1} := x$ and $r_{n+1} := r_n$.

It is easy to show that $\{l_i\}_{i=0}^{\infty}$ and $\{r_i\}_{i=0}^{\infty}$ are Cauchy sequences that satisfy the requirements above. Their limit is the least upper-bound of S. □

The proof above is formalized in Coq. (It is very similar to the formalized proof of Theorem 5.4.) As one might expect, the converse of this theorem also holds: if a constructive ordered field satisfies the least upper bound principle, then it is Cauchy complete. A proof of this fact is given in [2]. So the two axiomatizations are equivalent. We have also formalized this proof inside Coq. In other words we have formally proved the following statement.

Theorem 6.4. *Let F be an Archimedean constructive ordered field that satisfies the least upper bound principle. Then every Cauchy sequence in F has a limit.*

Taking the least upper bound principle as an axiom originates from the construction of reals as subsets of $\mathbb{Q}$. This construction is given (constructively) in [13]. There, a Dedekind cut is defined as a nonempty bounded *located* (a modification of 6.2 phrased for sets of rational numbers) subset of $\mathbb{Q}$. This yields the canonical order completion of rational numbers. We want to emphasize that we *have not* constructed a model of the Dedekind real numbers as special subsets of $\mathbb{Q}$ in Coq. Such a formalization requires a step by step construction of the operations and relations on located subsets of $\mathbb{Q}$, similar to what we have done for Cauchy sequences over $\mathbb{Q}$. Having proved all the required properties, Theorem 6.4 then yields a concrete term of type `CReals` out of the Dedekind real numbers.

7 Conclusion

The above results have all been formalized in Coq; the source files are available as part of the FTA project in [10]. Of course, the source files contain a lot of collateral lemmata which we haven't mentioned here. Most of them are not interesting from a mathematical point of view, and deal with microscopic details needed for the proofs. For the results in Section 3 we have mainly used the standard libraries `Arith` and `ZArith` of Coq. When doing arithmetic on integers we have used the tactic `Ring` of Coq. For the remaining results, the tactics `Algebra` and `Rational` of the FTA project have been thoroughly used. The whole formalization uses the syntactic definitions and symbols introduced by the algebraic hierarchy of the FTA project [9]

As for the implementation, we have mentioned the main points in this paper, and this may be useful for possible implementations of constructive real numbers in other proof assistants. As we have already pointed out in the introduction, there are more constructions of the reals in type theory ([4, 12, 5]), implemented in various proof assistants with different aims. The added value of the present work is that we work from a set of axioms. We use our construction to show that the axioms can be satisfied (there is a model for them) and that the axiomatization is categorical (any two models are isomorphic). This shows that Coq can serve very well as a logical framework in which both axiomatic and model-theoretic reasoning can be formalized.

Acknowledgements We want to thank Venanzio Capretta, Freek Wiedijk and Jan Zwanenburg for the many fruitful discussions and their useful Coq suggestions. We thank Bas Spitters for the useful discussions on constructive analysis. We thank the referees for their insightful comments and useful suggestions.

References

[1] E. Bishop and D. Bridges. *Constructive Analysis.* Number 279 in Grundlehren der mathematischen Wissenschaften. Springer, Berlin, 1985.

[2] D. Bridges. Constructive mathematics: a foundation for computable analysis. *Theoretical Computer Science*, 219:95–109, 1999.

[3] D. Bridges and S. Reeves. Constructive mathematics in theory and programming practice. *Philosophia Mathematica*, 7, 1999.

[4] J. Chirimar and D. Howe. Implementing constructive real analysis. In J.P. Myers and M.J. O'Donnel, editors, *Constructivity in Computer Science*, number 613 in LNCS, pages 165–178, 1992.

[5] A. Ciaffaglione and P. Di Gianantonio. A coinductive approach to real numbers. In Th. Coquand, P. Dybjer, B. Nordström, and J. Smith, editors, *Types 1999 Workshop, Lökeberg, Sweden*, number 1956 in LNCS, pages 114–130, 2000.

[6] A. Ciaffaglione and P. Di Gianantonio. A tour with constructive real numbers. In *Types 2000 Workshop, Durham, UK*, 2001. This Volume.

[7] D. Delahaye and M. Mayero. Field: une procédure de décision pour les nombres réels en Coq. In *Proceedings of JFLA'2001.* INRIA, 2001.

[8] B. Barras et al. *The Coq Proof Assistant Reference Manual, Version 7.1.* INRIA, http://coq.inria.fr/doc/main.html, sep 2001.

[9] H. Geuvers, R. Pollack, F. Wiedijk, and J. Zwanenburg. The algebraic hierarchy of the FTA project. In *Calculemus 2001 Proc.*, pages 13–27, Siena, Italy, 2001.

[10] H. Geuvers, F. Wiedijk, J. Zwanenburg, R. Pollack, M. Niqui, and H. Barendregt. FTA project. http://www.cs.kun.nl/gi/projects/fta/, nov 2000.

[11] J. Harrison. *Theorem Proving with the Real Numbers.* Distinguished dissertations. Springer, London, 1998.

[12] C. Jones. Completing the rationals and metric spaces in LEGO. In G. Huet and G. Plotkin, editors, *Logical Environments*, pages 297–316. CUP, 1993.

[13] A. Troelstra and D. van Dalen. *Constructivism in Mathematics, vol I*, volume 121 of *Studies in Logic and The Foundation of Math.* North Holland, 1988. 342 pp.