Formalizing a Discrete Model of the Continuum in Coq from a Discrete Geometry Perspective

Nicolas Magaud[1], Agathe Chollet[2], and Laurent Fuchs[3]

[1] LSIIT UMR 7005 CNRS - Université de Strasbourg
Bld Sébastien Brant BP 10413 67412 Illkirch Cedex, France
magaud@unistra.fr,
[2] Laboratoire MIA - Université de La Rochelle,
Avenue Michel Crépeau 17042 La Rochelle Cedex, France
achollet01@univ-lr.fr,
[3] Laboratoire XLIM-SIC UMR 6172 CNRS - Université de Poitiers
Bat. SP2MI Bld Marie et Pierre Curie
BP 30179 86962 Futuroscope Chasseneuil Cedex, France
Laurent.Fuchs@sic.univ-poitiers.fr.

Abstract. This work presents a formalization of the discrete model of the continuum introduced by Harthong and Reeb [10], the Harthong-Reeb line. This model was at the origin of important developments in the Discrete Geometry field [21]. The presented formalization is based on the work presented in [4] where it was shown that the Harthong-Reeb line satisfies the axioms for constructive real numbers introduced by Bridges [3]. A formalization of a first attempt for a model of the Hartong-Reeb line based on the work of Laugwitz and Schmieden [12] is also presented and analyzed. We hope that this work could help reasoning and implementation of numeric computations in geometric systems.

1 Introduction

Dealing with geometric problems (geometric constraints solving, geometric modeling) people are, finally, faced to computations that involve computer representation of real numbers. Due to their important impact, the studies about real numbers in computer science are numerous and our purpose is not to surpass them but to reactivate an efficient point of view that has been forgot for a while [21].

This point of view was built in the eighties by J. Harthong and G. Reeb and consists in a model of the continuum based over the integers that is the Harthong-Reeb line. This model was at the origin of important developments in the Discrete Geometry field [21]. And, at that time, the constructive content of this model was neglected even if it was explicitly noted in Diener and Reeb's book [7].

In previous works [4] it was shown that the Harthong-Reeb line satisfies the axioms for constructive real numbers introduced by Bridges [3]. However, the Harthong-Reeb line construction is based on a nonstandard arithmetic of the integer that was not explicitly built. To be short, starting with the naive integer sequence (the one that you can enumerate; $1, 2, \ldots$), G. Reeb argues that it must exists an integer ω that is greater than all naive integers. Using the compacity theorem[4] the from model theory [11], the existence of this nonstandard integer ω is sufficient to deduce that it exists a nonstandard model of the integer arithmetic with such nonstandard integer ω and then this model can be used to build the Harthong-Reeb line.

Nevertheless, this nonstandard model of integer arithmetic is not built and, in order to be put on computers, the Harthong-Reeb line needs a constructive nonstandard model of integer arithmetic. A first attempt of such construction, based on the Ω-numbers of Laugwitz and Schmieden [13], was made by some of the authors with others in [5].

This work presents a first formalization of the Harthong-Reeb line using the Coq proof assistant. It can be seen as a light counterpart of the seminal works about the formalization of exact arithmetic [20, 9]. Our motivations to do this work reside into the difficulties that we faced when showing that the Harthong-Reeb line satisfies the axioms proposed by Bridges [3]. Unless proofs have been read carefully we have no way to be sure that they were entirely correct. This confidence problem of proofs is mainly due to the unusual mathematics that we deal with. The handled arithmetic is in a nonstandard framework and the axioms are in a constructive framework. So, it was not clear that handwritten proofs didn't contain subtle mistakes or imprecisions. Moreover, the formalization has entailed a better understanding of how concepts and proofs are related to one with others.

From a more practical point of view, the Harthong-Reeb line provides a rich theoretical framework that allows to analyze a wide range of geometrical objects. So, our formalization can also be thought as a model for geometric computations. One main advantage of such model is that computation algorithms and reasoning about these algorithms (e.g. to prove that they are correct) can be done in the same framework. And we hope that this will help to the development of geometric systems where computations are made using the Harthong-Reeb line. This goal can be reasonably reached because the Coq proof assistant [6, 1] implements a higher constructive logic and is also a programming language equipped with inductive definitions and recursive functions. Therefore, it is the perfect tool to carry out a constructive formalization.

This paper is organized as follows. In section 2, we formally describe in the Coq a nonstandard model of arithmetic and build the Harthong-Reeb line $\mathcal{HR}_\omega$ on top of it. In Section 3, we prove $\mathcal{HR}_\omega$ verifies Bridges' Axioms which capture what a constructive real line is. In Section 4, we study how to formalize and prove correct the least upper bound property. In Section 5, we investigate the limitations of the Ω-numbers of Laugwitz and Schmieden when it comes to being an adequate model of the nonstandard arithmetic we consider. Finally, in Section 6, we discuss our results as well as alternative approaches to our formalization.

[4] Roughly speaking it says that if for a theory with infinitely many axioms, each finite subset of axioms has a model then the theory has a model.

2 A Parametric module to describe the Harthong-Reeb line

In this section the parametric module that formalize the Harthong-Reeb line is described. The ground idea of the Harthong-Reeb line is to introduce a non trivial rescaling on the usual set of integers in order to get a discrete form of the continuum. To do so a nonstandard arithmetic is used. This is described in the next subsection.

2.1 Nonstandard Model of Arithmetic

We first have to specify the axiomatic numbers we shall use in this work as well as their functions and their properties. We do that using a module type in Coq. This can be viewed as an interface which, on the one hand, is the first step in our construction of the Harthong-Reeb line and on the other hand, can be implemented by a concrete datatype, operations and proofs of the axioms (as we do in section 5). This module type contains the declaration of the basic objects of the theory:

```
Parameter A:Type.

Parameter a0 a1 : A.
Parameter plusA multA divA modA : A -> A -> A.
Parameter oppA absA : A -> A.

Parameter leA ltA : A -> A -> Prop.

Parameter w:A.
Parameter lim:A->Prop.
```

Notations can be introduced to ease reading and writing of specifications. This also allows to stay close to the way mathematicians would write.

```
Notation "x + y " := (plusA  x y).
Notation "x * y " := (multA  x y).
Notation "x / y " := (divA  x y).

Notation "0" := (a0).
Notation "1" := (a1).
Notation "- x" := (oppA x).
Notation "| x |" := (absA x) (at level 60).
Notation "x ?<= y" := (leA x y) (at level 50).
Notation "x ?< y" := (ltA x y) (at level 50).
```

Then all the basic properties of A are expressed as axioms.

```
Parameter plus_neutral : forall x,0 + x = x.
Parameter plus_comm : forall x y,  x + y =  y + x.
Parameter plus_assoc : forall x y z,  x + (y + z) = (x + y) + z.
Parameter plus_opp : forall x, x + (- x) = 0.

Parameter abs_pos : forall x, 0?<=|x|.
Parameter abs_pos_val : forall x, 0?<=x -> |x|=x.
Parameter abs_neg_val : forall x, x?<=0 -> |x|=-x.
[...]
```

Overall, we assume that A with the operations $+,\times,\ldots$ is equipped with a ring structure. This will allow to prove basic algebraic equations automatically and also to perform some otherwise tedious simplications of expressions.

In addition, we assume that the order relations $? <=$ and $? <$ enjoy their usual properties such as transitivity, regularity w.r.t operations such as addition, etc. We also assume these relations are decidable by adding the following axiom which states that forall $x : A$, either $x? < 0$ or $x = 0$ or $0? < x$.

```
Axiom A0_dec : forall x, {x ?<0}+{x=0}+{0 ?< x}.
```

Even if axiomatic theories of nonstandard analysis, such as IST [18], are available, we present here, in the spirit of some works of Nelson or Lutz [19, 15], a weaker axiomatic which is well suited for our purpose.

First we introduce a new predicate lim over integer numbers: $lim(x)$ "means" that the integer x is limited.

```
Parameter lim : A -> Prop.
Parameter w : A.
```

This predicate is external to the classical integer theory and its meaning directly derives from the following axioms ANS1, ANS2, ANS3, ANS4 (and ANS5 which will be introduced later):

ANS1. *The number* 1 *is limited.*

```
Parameter ANS1 : lim 1.
```

ANS2. *The sum and the product of two limited numbers are limited.*

```
Parameter ANS2a : forall x y, lim x -> lim y -> lim (x + y).
Parameter ANS2b : forall x y, lim x -> lim y -> lim (x * y).
```

ANS3. *Non-limited integer numbers exist.*

```
Parameter ANS3 : ~ lim w.
```

We simply assert that w is not limited (in Coq, ~ stands for logic negation).
ANS4. *For all* $(x, y) \in A^2$ *such that* x *is limited and* $|y| \leq |x|$*, the number* y *is limited.*

```
Parameter ANS4 :
  forall x, (exists y, lim y /\ | x | ?<= | y |)-> lim x.
```

For reading conveniences, we introduce the following notations [4]:

- $\forall^{lim} x\ F(x)$ is an abbreviation for $\forall x\ (lim(x) \Rightarrow F(x))$ and can be read as "for all limited x, $F(x)$ stands".
- $\exists^{lim} x\ F(x)$ is an abbreviation for $\exists x\ (lim(x) \wedge F(x))$ and can be read as "exists a limited x such that $F(x)$".

We say that a formula or a proposition P is *external* when the predicate `lim` occurs in P and *internal* otherwise. This distinction is necessary to know when properties known for standard properties can be extended to the nonstandard ones. In fact, when a property P is internal, i.e. when it does not use the predicate `lim`, the extension of P to infinitely large numbers is immediate. This is given by the following *Overspill principle*. But for external properties, we cannot proceed in the same way. We need to introduce a new extension principle as an axiom (called $ANS5$ in this paper). This principle states that the formula which contains these external properties can be extended to infinitely large numbers, but that we do not know whether these infinitely large numbers verify this property.

Proposition 1. ***(Overspill principle)*** *Let $\mathcal{P}(x)$ be an internal formula such that $\mathcal{P}(n)$ is true for all $n \in A_{lim}, n \geq 0$. Then, there exists an infinitely large $\nu \in A, \nu \geq 0$ such that $\mathcal{P}(m)$ is true for all integers m such that $0 \leq m \leq \nu$.*

```
Parameter overspill_principle : forall P:A -> Prop,
 (forall n:A, lim n /\ 0?<=n -> P n) ->
  (exists v:A, ~lim v /\ 0?<=v /\ (forall m:A, 0?<=m /\ m ?<=v -> P m)).
```

Proof. The class $C = \{x \in A, x \geq 0\ ;\ \forall y \in [0, x]\ \mathcal{P}(y)\}$ is an internal set (i.e. a classical set) containing $A_{lim} = \{x \in A, x \geq 0, lim(x)\}$. Since A_{lim} is an external set, the inclusion $A_{lim} \subset C$ is strict and leads to the result. $\square$

In the same way, the application of an inductive reasoning on an external formula could be illegitimate. For example, number 0 is limited, $x + 1$ is limited for all limited x. Nevertheless not all integers are limited. To improve the power of our nonstandard tool, we have to add a special induction that fits with external formulae. In the following principle which is our last axiom, $\mathcal{P}$ denotes an internal or external formula:

ANS5. ***(External inductive defining principle):*** *We suppose that*

1. *there is $x_0 \in A^p$ such that $\mathcal{P}((x_0))$;*
2. *for all $n \in A_{lim} = \{x \in A, x \geq 0, lim(x)\}$ and all sequence $(x_k)_{0 \leq k \leq n}$ in $\mathbb{Z}^p$ such that $\mathcal{P}((x_k)_{0 \leq k \leq n})$ there is $x_{n+1} \in A^p$ such that $\mathcal{P}((x_k)_{0 \leq k \leq n+1})$.*

Therefore, there exists an internal sequence $(x_k)_{k\in A,k\geq 0}$ *in* $\mathbb{Z}^p$ *such that, for all* $n \in A_{lim}$*, we have* $\mathcal{P}((x_k)_{0\leq k\leq n})$.
This principle means that the sequence of values x_k for k limited can be prolonged in an infinite sequence $(x_k)_{k\in A,k\geq 0}$ defined for all integers. Saying that this sequence is internal means that it has all the properties of the classical sequences in usual number theory. Particularly, if $\mathcal{Q}(x)$ is an internal formula, then the class $\{k \in A, k \geq 0 \; ; \; \mathcal{Q}(x_k)\}$ is an internal part of $\{k \in A, k \geq 0\}$.

In Coq, we choose a slighly different and more convenient definition of $ANS5$:

```
Parameter ANS5 :
forall P :A -> Prop,
(forall u : forall n:A, lim n /\ 0 ?<= n -> A,
  P (u 0 H0) ->
  (forall n:A, forall Hn : lim n /\ 0 ?<= n,
     (forall k:A, forall Hk:0 ?<= k /\ k ?<= n,
      forall Hn1 : lim (n+1)/\0?<=(n+1),
        P (u k (ANS4_special n k Hn Hk)) -> P(u (plusA n 1) Hn1))) ->
    (* {u:A->A | ... } *)
    sigT(fun v => forall n:A, forall Hn:lim n /\ 0?<= n,
          forall k:A, forall Hk:0 ?<= k /\ k ?<= n,
            P (v k) /\ v k = u k (ANS4_special n k Hn Hk))).
```

2.2 The system $\mathcal{HR}_\omega$.

Let us now give the definition of the system $\mathcal{HR}_\omega$. Introduced by M. Diener [8], this system is the formal version of the so-called Harthong-Reeb line. In the next section we prove that this system can be viewed as a model of the real line which is partly constructive. In some sense, $\mathcal{HR}_\omega$ is equivalent to $\mathbb{R}$ (see [4] for details).

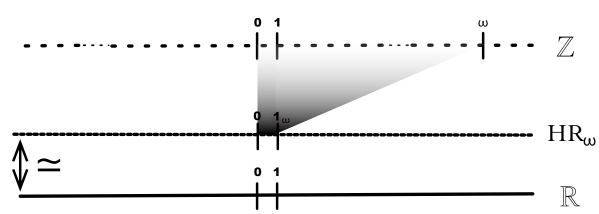

Fig. 1. An intuitive representation of $\mathcal{HR}_\omega$.

Accordingly to axiom ANS3, the construction starts by considering an infinitely large (non-limited) positive (i.e. ≥ 0) integer $\omega \in A$. Our purpose is to define a new numerical system such that all the elements are integers and, in which ω is the new unit. Let us introduce the underlying set of this system.

Definition 1. *The set $\mathcal{HR}_\omega$ of the admissible integers considering the scale ω is defined by:* $\mathcal{HR}_\omega = \{x \in A\ ;\ \exists^{lim} n \in A, n \geq 0\ |x| < n\omega\}$.

This definition can be easily translated in Coq:

```
Definition P :=
  fun (x:A)=> exists n:A, (lim n /\ 0 ?< n /\  (|x| ?<= n*w)).
Definition HRw := {x:A | P x}.
```

Note that {`x:A|P x`}, which is a convenient notation for (`sig` P), allows to describe sets comprenhensively. Here it corresponds to the set of elements of A which verify P. This corresponds to an inductive definition in Coq. It comes together with two projections: `proj1_sig`, which returns `a` and `proj2_sig` which returns a proof `H` of `P a`.

The set $\mathcal{HR}_\omega$ is an external set. Moreover, it is an additive sub-group of A. We provide $\mathcal{HR}_\omega$ with the operations $+_\omega$ and $*_\omega$, the ω-scale equality, the ω-scale inequality relations (noted $=_\omega$ and $\neq_\omega$) and the order relation $>_\omega$:

Definition 2. *Let X and Y be any elements of $\mathcal{HR}_\omega$.*

- *X and Y are* equal *at the scale ω and we write $X =_\omega Y$ when* $\forall^{lim} n \in \mathbb{N} \quad n|X - Y| \leq \omega$.
- *Y is* strictly greater *than X at the scale ω and we write $Y >_\omega X$ when* $\exists^{lim} n \in \mathbb{N} \quad n\,(Y - X) \geq \omega$.
- *X is* different *from Y at the scale ω and we write $X \neq_\omega Y$ when* $(X >_\omega Y$ *or* $Y >_\omega X)$
- *The* sum *of X and Y at the scale ω is $X +_\omega Y := X + Y$ (like the usual sum). For this operation, the* neutral element *is $0_\omega = 0$ and the* opposite *of each element $Z \in \mathcal{HR}_\omega$ is $-_\omega Z := -Z$.*
- *The* product *of X and Y at the scale ω is $X \times_\omega Y := \lfloor \frac{X.Y}{\omega} \rfloor$ (different from the usual one). The* neutral element *is $1_\omega := \omega$, and the* inverse *of each element $Z \in \mathcal{HR}_\omega$ such that $Z \neq_\omega 0_\omega$ is $Z^{(-1)_\omega} := \left\lfloor \frac{\omega^2}{Z} \right\rfloor$.*

Algebraic operations are defined on the integers of the set A onto with $\mathcal{HR}_\omega$ is built. Therefore we must ensure the result still belongs to $\mathcal{HR}_\omega$. For the sum, it consists in proving the following lemma:

```
Lemma Pplus: forall x y:A, P x -> P y -> P ( x + y).
```

Then, the addition in $\mathcal{HR}_\omega$ can be defined as follows:

```
Definition HRwplus (x y: HRw) : HRw :=
match x with exist xx Hxx =>
match y with exist yy Hyy =>
exist P (xx + yy) (Pplus xx yy Hxx Hyy)
end end.
```

All lemmas and formal definitions of the objects of Definition 2 are summarized in Fig. 2.

```
Lemma Pplus : forall x y, P x -> P y -> P (x + y).

Definition HRwplus (x y: HRw) : HRw :=
 match x with exist xx Hxx => match y with exist yy Hyy =>
  exist P (xx + yy) (Pplus xx yy Hxx Hyy)
end end.

Lemma Popp : forall x, P x -> P (- x).

Definition HRwopp (x: HRw) : HRw :=
 match x with exist xx Hxx => exist P (- xx) (Popp xx Hxx) end.

Definition HRwminus (x y : HRw) : HRw := HRwplus x (HRwopp y).

Lemma Pmult : forall x y, P x -> P y -> P (( x * y) / w).

Definition HRwmult (x y: HRw) : HRw :=
 match x with exist xx Hxx => match y with exist yy Hyy =>
  exist P ((xx * yy) / w) (Pmult xx yy Hxx Hyy)
end end.

Definition HRwequal (x y : HRw) : Prop :=
 match x with exist xx Hxx => match y with exist yy Hyy =>
  (forall n, lim n ->0 ?< n -> ( (n*|xx + (- yy)|) ?<= w))
end end.

Definition HRwgt (y x : HRw) : Prop :=
 match y with exist yy Hyy => match x with exist xx Hxx =>
  (exists n, lim n /\ 0 ?< n /\ (w ?<= (n*(yy+ (-xx)))))
end end.

Definition HRwge (a b : HRw) : Prop :=
 (proj1_sig b) ?<= (proj1_sig a) \/ HRwequal a b.

Definition HRwdiff (x y : HRw) : Prop := HRwgt x y \/ HRwgt y x.

Lemma Pdiv : forall x ,  HRwdiff x HRw0 -> P ((w * w ) /(proj1_sig x)).

Definition HRwinv (x : HRw) (H: HRwdiff x HRw0) : HRw :=
 exist P ((w * w ) / (proj1_sig x)) (Pdiv x H).
```

Fig. 2. Definitions of $\mathcal{HR}_\omega$ operations in Coq

3 Bridges' Axioms

In the 90' Brigdes proposed in [3] an axiomatic definition of what is a constructive real line. It is derived in three groups about algebraic structure (R1), ordered set (R2) and the last group (R3) deals with special properties (see follow the details). A field which satisfies these axioms is called an Bridges-Heyting ordered field. In [4], the proof of that *the Harthong-Reeb line with associated operations and relations is a Bridges-Heyting ordered field* is given. The particularity is that this theorem is proved only using intuitionnistic logic. Let us just make some remarks about these axioms.

3.1 R1. About algebrica structure

$\forall x, y, z \in \mathcal{HR}_\omega$,

1. $x +_\omega y =_\omega y +_\omega x$
2. $(x +_\omega y) +_\omega z =_\omega x +_\omega (y +_\omega z)$
3. $0_\omega +_\omega x =_\omega x$
4. $x +_\omega (-_\omega x) =_\omega 0_\omega$
5. $x \times_\omega y =_\omega y \times_\omega x$
6. $(x \times_\omega y) \times_\omega z =_\omega x \times_\omega (y \times_\omega z)$
7. $1_\omega \times_\omega x =_\omega x$
8. $x \times_\omega x^{(-1)_\omega} =_\omega 1_\omega$ if $x \neq_\omega 0_\omega$
9. $x \times_\omega (y +_\omega z) =_\omega x \times_\omega y +_\omega x \times_\omega z$

This first group presents the attended properties about the two operations $+_\omega$ and $\times_\omega$. There is not any major difficulties to prove that $\mathcal{HR}_\omega$ verifies these axioms.

All the axioms of this group can be formally proven using the definitions of the operations involved. These properties are expressed using Leibnitz equality of Coq. They proceed by case analysis on the elements of $\mathcal{HR}_\omega$, destructuring them into an element x of A and a proof H that $P(x)$ holds. We present the proof of the first one (commutativity of addition). Proving the terms `HRwplus` x y and `HRwplus` y x are equal in $\mathcal{HR}_\omega$ consists in not only proving the witnesses (in A) are equal but also proving the proofs of the properties $P(x+y)$ and $P(y+x)$ are equal. As what matters is only that P holds for the considered element, we use the principle of *proof irrelevance* to show all proofs of the same property (e.g. $P(x)$) are equal. This principle is expressed with the following axiom in Coq:

```
Axiom proof_irr :forall A:Prop, forall p p':A, p=p'.
```

This well-known principle is consistent with Coq's logic and therefore we can safely add it to our formal description.

3.2 R2. Basic properties of $>_\omega$

$\forall x, y, z \in \mathcal{HR}_\omega$,

1. $\neg\,(x >_\omega y \wedge y >_\omega x)$
2. $(x >_\omega y) \Rightarrow \forall z\ (x >_\omega z\ or\ z >_\omega y)$
3. $\neg(x \neq_\omega y) \Rightarrow x =_\omega y$
4. $(x >_\omega y) \Rightarrow \forall z\ (x +_\omega z >_\omega y +_\omega z)$

5. $(x >_\omega 0_\omega \wedge y >_\omega 0_\omega) \Rightarrow x \times_\omega y >_\omega 0_\omega$

All these properties can be proven in a very straightforward manner in Coq, following the informal proofs of [4]. This definition of inequality is quite more complex than the classical definition of inequality. It is explain by that the decidability is not necessarily request. Because of the definition of inequality on the Harthong-Reeb line, these axioms are easily provable. The proof often derived from the properties of order on A. In fact we just need to assume that the basic inequality on A is decidable. This hypothesis is not a problem for an axiomatic definition of nonstandard arithmetic but, in practice there is some problem, for example in the Laugwitz-Schmieden model, the inequality is not decidable (see section 5). But, we try to obtain this quality with an other model derived from the Type Theory of Martin-Lof [16, 17].

Links between orders in $\mathcal{HR}_\omega$ and orders in A . There exists different correlations between orders in $\mathcal{HR}_\omega$ and in our non standard integers set A. We recall that, in $\mathcal{HR}_\omega$ the strictly great relation and the great or equal relation are defined from the less or equal relation on A ($y >_\omega x \equiv \exists^{\lim} n \in A \quad n\,(y-x) \geq \omega$ and $y \geqslant_\omega x \equiv \forall^{\lim} n \in A \quad n\,(y-x) \leqslant \omega$). We have the following correspondences for all $a, b \in \mathcal{HR}_\omega$:

1. $a \geqslant b$ implies $a \geqslant_\omega b$
2. $a >_\omega b$ implies $a > b$

These properties are key properties of our development and were easily established in Coq.

3.3 R3: Special Properties of $>_\omega$

The two last properties to prove to fulfil the requirements of Bridges' axiom system are the following ones:

1. **Property of Archimedes**: For each $X \in \mathcal{HR}_\omega$ there exists a constructive $n \in A$ such that $X < n$.
2. **The constructive least-upper-bound principle**

Archimedes property can be easily formalized in Coq:

```
Lemma Archimedes : forall X:HRw, exists n:HRw, n >=w X.
```

Proof. Its proof is immediate because the elements x of $\mathcal{HR}_\omega$ are such that there exists a limited $k \in \mathbb{N}$, $|x| < k\omega$. So the property can be proved using the integer $k\omega$ as a witness for n.

On the contrary, the proof of the least-upper bound principle is fairly technical and intricate. Therefore it deserves a whole section by itself.

4 Least upper bound

A subset S of $\mathcal{HR}_\omega$ is the collection of elements of $\mathcal{HR}_\omega$ which satisfies a given property defined in the system. This property may be internal or external. Such a subset S is *bounded above relative to the relation* $\geq_\omega$ if there is $b \in \mathcal{HR}_\omega$ such that $b \geq_\omega s$ for all $s \in S$; the element b is called an *upper bound* of S. A *least upper bound* for S is an element $b \in \mathcal{HR}_\omega$ such that

- $\forall s \in S \quad b \geq_\omega s$ (b is an upper bound of S);
- $\forall b' \ (b >_\omega b') \Rightarrow (\exists s \in S \quad s >_\omega b')$.

A least upper bound is unique: if b and c are two least upper bounds of S, then we have $\neg(b >_\omega c)$ and $\neg(c >_\omega b)$; thus, according to the properties[5] of the relations $>_\omega$, $\geq_\omega$ and $= \omega$, we get $c \geq_\omega b$ and $b \geq_\omega c$ and then $b =_\omega c$.

The constructive least-upper-bound principle: Let S be a nonempty subset of $\mathcal{HR}_\omega$ that is bounded above relative to the relation $\geq_\omega$, such that for all $\alpha, \beta \in \mathcal{HR}_\omega$ with $\beta >_\omega \alpha$, either β is an upper bound of S or else there exists $s \in S$ with $s >_\omega \alpha$; then S has a least upper bound.

The subset property is defined as a property, i.e. $S\ x$ means x belongs to the set S.

Proof. To formalize and prove this property correct in Coq we follow the proof proposed in [4], which itself uses the heuristic motivation given by Bridges in [2].

4 sequences $(s_n, b_n, \alpha_n, \beta_n)$ These four sequences are defined in a mutually recursive way :

```
Definition def_s_b_alpha_beta :
    forall n:A, forall Hn:(lim n /\ 0 ?<= n),
{sn:HRw & {bn:HRw & {alphan:HRw &{betan : HRw &
   S sn /\
   upper_bound S bn /\
   bn +w (-w sn) =w ((power two_third n Hn)*w (b0 +w (-w s0))) /\
   HRwgt betan alphan /\
   alphan=(two_third *w sn) +w (one_third *w bn) /\
   betan=(one_third *w sn) +w (two_third *w bn)}}}}.
```

Computing the next terms s_n and b_n of the sequences depends on the four preceding terms $(s_{n-1}, b_{n-1}, \alpha_{n-1}, \beta_{n-1})$ and also requires a proof of the property $\beta_{n-1} >_\omega \alpha_{n-1}$. Thus we must keep track of this property in Coq during the computations of $(s_n, b_n, \alpha_n, \beta_n)$. Therefore, we choose to specify the function as precisely as possible when defining it, hence the numerous postconditions characterizing the output $(s_n, b_n, \alpha_n, \beta_n)$ of the function.

Initially, we have $(s_0, b_0, \alpha_0, \beta_0)$ with an arbitrary element s_0 of S, b_0 an upper bound of S, $\alpha_0 = \frac{2}{3}s_0 + \frac{1}{3}b_0$ and $\beta_0 = \frac{1}{3}s_0 + \frac{2}{3}b_0$.

[5] These properties are not completely trivial in intuitionistic logic.

This requires to assume in Coq that we can always choose an arbitrary element s of S. This corresponds to a form of choice which can be expressed as follows:

```
Axiom choice : forall X:subset, (non_empty X) -> {x:HRw|X x}.
```

Given a non-empty subset X of elements of $\mathcal{HR}_\omega$, there exists an element x of $\mathcal{HR}_\omega$ for which (Px) holds.

Suppose for a given n, we have $((s_n, b_n, \alpha_n, \beta_n))$ with $alpha_n <_\omega beta_n$. Two different cases can happen :

- **First case** β_n is an upper bound of S. Then $s_{n+1} = s_n$ and $b_{n+1} = \beta_n$.
- **Second case** there exists s such that $(S\ s)$ and that $\alpha_n <_\omega s$. Then $s_{n+1} = s$ and $b_{n+1} = b_n + s - \alpha_n$.

In both cases, $\alpha_{n+1} = \frac{2}{3}s_{n+1} + \frac{1}{3}b_{n+1}$ and $\beta_{n+1} = \frac{1}{3}s_{n+1} + \frac{2}{3}b_{n+1}$.

Key properties Several key properties of the elements of the sequences are already expressed in the type of `def_b_alpha_beta`. They hold by construction (i.e. they are established using induction at the same time the actual sequences are computed). All s_n belongs to S, all b_n are upper bounds of S, therefore for any k and n, we have $b_k >_\omega s_n$. We also have the property that b_n and s_n are connected by the relation

$$b_n -_\omega s_n =_w (2/3)^n \times (b0 -_\omega s0).$$

In addition to all the properties specified in the type of `def_b_alpha_beta`, we also need to establish that the sequence (s_n) is increasing. Although this is immediate from its mathematical definition, it still has to be formalized in Coq. At the time of writing the paper, this is still a work in progress and no formal proof has been achieved yet.

Thanks to axiom ANS5, the sequences can be extended to all integers, including non-limited ones. In addition, the overspill principle allows to show the existence of ν such that

$$\min_{0 \leq k \leq \nu} b_k \geq s_\nu \geq \ldots \geq s_1 \geq s_0.$$

Details are available in the proof scripts.

A least upper bound of S : $b := \min_{0 \leq k \leq \nu} b_k$
We simply follow the reasoning steps of the proof presented in [4] to prove:

- on the one hand, that b is an upper bound of S,
- on the other hand, that b is actually a least upper bound, i.e. that for all $b' <_\omega b$, there exists $s \in S$ such that $s >_\omega b'$.

5 The Ω-numbers of Laugwitz and Schmieden

The Ω-numbers of Laugwitz and Schmieden permits the extension of a classical numerical system to a nonstandard one. Here is presented the extension of natural numbers, it can be viewed as a model of the axiomatic definition of the nonstandard arithmetic presented in part 3. In theirs papers [12–14], Laugwitz and Schmieden extend the rational numbers and show that their system is equivalent to classical real numbers (without limit consideration). In this section, we will not describe the whole theory but only introduce the basic notions that are essential to understand the Harthong-Reeb line. For more details about our approach please refer to [5].

To extend a theory of integer numbers, Laugwitz and Schmieden introduce a new symbol, Ω to the classical ones $(0, 3, 9, +, /, ...)$. The only thing that we know about it is that Ω verifies the following property named the *Basic Definition* and called (BD) :

Definition 3. *Let $S(n)$ be a statement in $\mathbb{N}$ depending of $n \in \mathbb{N}$. If $S(n)$ is true for almost $n \in \mathbb{N}$, then $S(\Omega)$ is true.*

We consider the expression "*almost* $n \in \mathbb{N}$" means "for all $n \in \mathbb{N}$ from some level N", i.e. "$(\exists N \in \mathbb{N})$ such that $(\forall n \in \mathbb{N})$ with $n > N$". Since Ω can be substituted to any natural number, it denotes an Ω-number which is the first example of Ω-integer. Hence, each element a of this theory will be declined as a sequence $(a_n)_{n\in\mathbb{N}}$.

Ω-numbers are defined in Coq as sequences indexed by natural numbers (`nat`), whose values are relative integers (`Z`). The function `Z_of_nat` simply injects natural numbers into $\mathbb{Z}$.

```
Definition A := nat->Z.

Definition a0 : A := fun (n:nat) => 0%Z.
Definition a1: A := fun (n:nat) => 1%Z.

Definition w :A := fun (n:nat) => (Z_of_nat n).
```

To compare such Ω-numbers, we put the following equivalence relation:

Definition 4. *Let $a = (a_n)_{n\in\mathbb{N}}$ and $b = (b_n)_{n\in\mathbb{N}}$ be two Ω-numbers, a and b are equal if it exists $N \in \mathbb{N}$ such that for all $n > N$, $a_n = b_n$.*

This is captured by the definition `ext_almost_everywhere`. The axiom `ext` which expresses the extentionality principle for functions is used to directly prove that 2 Ω-numbers are equal.

```
Definition ext_almost_everywhere (u v:A) :=
 exists N:nat, forall n:nat, n>N -> u n=v n.

Axiom ext : forall u v:A, (forall n:nat, (u n)=(v n)) -> u = v.
```

We can distinguish two classes of elements in this nonstandard theory:

- the class of *limited* elements: they are the elements $\alpha = (\alpha_n)_{n\in\mathbb{N}}$ which verify $\exists p \in \mathbb{Z}$ such that $\exists N \in \mathbb{N},\ \forall n > N, \alpha_n < p$ (example: $(2)_{n\in\mathbb{N}}$).
- the class of elements: *infinitely large numbers*, which are the sequences $\alpha = (\alpha_n)_{n\in\mathbb{N}}$ such that $lim_{n\to+\infty}\alpha_n = +\infty$

Immediately, we can verify that Ω is infinitely large, i.e. greater than every element of $\mathbb{N}$. Indeed, for $p \in \mathbb{N}$, we apply (BD) to the statement $p < n$ which is true for almost $n \in \mathbb{N}$; thus $p < \Omega$ for each $p \in \mathbb{N}$. And Ω is the sequence $(n)_{n\in\mathbb{N}}$.

The definition of the operations and relations between $\mathbb{Z}_\Omega$, the set of Ω-numbers are the following:

Definition 5. *Let $a = (a_n)_{n\in\mathbb{N}}$ and $b = (b_n)_{n\in\mathbb{N}}$ two Ω-numbers,*

– $a + b =_{def} (a_n + b_n)_{n\in\mathbb{N}}$ *and* $-a =_{def} (-a_n)$ *and* $a \times b =_{def} (a_n \times b_n)_{n\in\mathbb{N}}$;

```
Definition plusA (u v:A) := fun (n:nat) => Zplus (u n) (v n).
Definition multA (u v:A) := fun (n:nat) => Zmult (u n) (v n).
Definition oppA (u:A) := fun (n:nat) => Zopp (u n).
```

– $a > b =_{def} [(\exists N \forall n > N)\ a_n > b_n]$ *and* $a \geqslant b =_{def} [(\exists N \forall n > N)\ a_n \geqslant b_n]$*;*

```
Definition leA (u v:A) :=
   exists N:nat, forall n:nat, n>N -> Zle (u n) (v n).

Definition ltA (u v:A) :=
   exists N:nat, forall n:nat, n>N -> Zlt (u n) (v n).
```

– $|a| =_{def} (|a_n|)$.

```
Definition absA (u:A) := fun (n:nat) => Zabs (u n).
```

Specificity of the theory Regarding the order relation, the usual properties true on $\mathbb{Z}$ are not always verified on $\mathbb{Z}_\Omega$. For instance

$$(\forall a, b \in \mathbb{Z}_\Omega) \quad (a \geqslant b) \vee (b \geqslant a) \tag{1}$$

is not valid as we can see for the particular Ω-integers $a = ((-1)^n)_{n\in\mathbb{N}}$ and $b = ((-1)^{n+1})_{n\in\mathbb{N}}$. Nevertheless, given two arbitrary Ω-integers $a = (a_n)$ and $b = (b_n)$, we have

$$(\forall n \in \mathbb{N}) \quad (a_n \geqslant b_n) \vee (b_n \geqslant a_n). \tag{2}$$

Using (BD), we obtain $(a_\Omega \geqslant b_\Omega) \vee (b_\Omega \geqslant a_\Omega)$ and thus (1) since $a_\Omega = a$ and $b_\Omega = b$. Hence, there is a contradiction. To avoid it, we might admit that the application of (BD) leads to a notion of truth weaker than the usual notion.

This shows that the Ω-numbers can not be a model of the theory presented in Section 2. The main issue is the decidability property `AO_dec` of the order relation which is obviously not provable in this setting.

Nonstandard axioms We define what two predicates `std` and `lim`: (`std` n) states that an Ω-number n is standard and (`lim` n) that n is limited.

```
Definition std (u:A) :=
 exists N:nat, forall n m, n>N -> m>N -> (u n)=(u m).

Definition lim (a:A) :=
 exists p, std p /\ leA a0 p /\ ltA (absA a) p.
```

From these definitions, we can derive proofs of the axioms $ANS1$ to $ANS4$ presented in Section 2. It remains an open question to know whether $ANS5$ could be proved formally in Coq for Ω-numbers.

6 Discussion

In this paper, we have presented a work in progress which consists in formalizing mathematical results obtained in the field of discrete geometry. We focused on the paper of Chollet et al. [4] in which it has been proved that the Harthong-Reeb line satisfies the Bridges' axioms of constructive reals [3].

The results obtained so far show that it is tractable to transform the mathematical handwritten proof of [4] into a formal one in Coq. It was useful in the sense that it makes the proof more precise and also ensures that there were no hidden mistakes. So, this dramatically increases the confidence into the proofs. In particular for the Least Upper Bound axiom where subtle notions are used. Another obtained byproduct is that properties needed to complete the proofs are well identified and, hence, we also know the one that are useless.

The formalization of an actual model of the abstract integers presented in section 2 has also been investigated. The Ω-numbers model developed in [5] based on the work of Laugwitz and Schmieden [12] was a good candidate but they could not be an actual model of the mandatory theory of nonstandard arithmetic. And, the reasons of this defect are clearly identified (see section 5). However, this does not say the Ω-numbers could not be used at all but, when using these numbers, the properties that could not be obtained are clearly identified. In that sense this helps the development of algorithms that use these numbers.

Figure 3 provides an insight of the size of the development. All proofs are available online[6] and shall be updated when new results are established.

Next steps to progress into this work are to complete the proof of the Least Upper Bound axiom, to formalize an actual constructive model of our abstract integers and to develop formal proofs of correctness of algorithms. For the moment the proof of the Least Upper Bound axiom is rather completed and what is left is reasonably reachable. The formalization of an actual constructive model of our abstract integers is currently faced to the problem to obtain a candidate model of such integers, using the theory developed in [17] enthusiastic preliminary results had already been obtained by the authors of [4]. The last point is currently not investigated.

[6] http://galapagos.gforge.inria.fr

	specifications	proofs
Nonstandard arithmetic	135	60
$\mathcal{HR}_\omega$ and Bridges' axioms	330	1500
(including the least upper bound)	230	500
Laugwitz-Schmieden	90	275

Fig. 3. Key figures of our formal development in Coq

References

1. Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development, Coq'Art: The Calculus of Inductive Constructions.* Springer, 2004.
2. D. Bridges and S. Reeves. Constructive mathematics, in theory and programming practice. Technical Report CDMTCS-068, Centre for Discrete Mathematics and Theorical Computer Science, November 1997.
3. D. S. Bridges. Constructive mathematics: A foundation for computable analysis. *Theor. Comput. Sci.*, 219(1-2):95–109, 1999.
4. A. Chollet, G. Wallet, L. Fuchs, G. Largeteau-Skapin, and E. Andres. Insight in discrete geometry and computational content of a discrete model of the continuum. *Pattern recognition*, 42:2220–2228, 2009.
5. A. Chollet, G. Wallet, L. Fuchs, G. Largeteau-Skapin, and E. Andres. Ω-Arithmetization: a Discrete Multi-resolution Representation of Real Functions. In P. Wiederhold and P. R. Barneva, editors, *Combinatorial Image Analysis: 13th International Workshop, IWCIA 2009*, volume 5852 of *Lecture Notes in Computer Science (LNCS)*, pages 316–329, Mexico, November 2009.
6. Coq development team. *The Coq Proof Assistant Reference Manual, Version 8.2.* LogiCal Project, 2008.
7. F. Diener and G. Reeb. *Analyse Non Standard.* Hermann, Paris, 1989.
8. M. Diener. Application du calcul de Harthong-Reeb aux routines graphiques. In J.-M. Salanskis and H. Sinaceurs, editors, *Le Labyrinthe du Continu*, pages 424–435. Springer, 1992.
9. H. Geuvers, M. Niqui, B. Spitters, and F. Wiedijk. Constructive analysis, types and exact real numbers. *Mathematical Structures in Computer Science*, 17(1):3–36, Mar. 2007.
10. J. Harthong. Une théorie du continu. In H. Barreau and J. Harthong, editors, *La mathématiques non standard*, pages 307–329, Paris, 1989. Éditions du CNRS.
11. M. Huth and M. Ryan. *Logic in Computer Science.* Cambridge University Press, 2nd edition edition, 2004.
12. D. Laugwitz. Ω-calculus as a generalization of field extension an alternative approach to nonstandard analysis. In A. Hurd, editor, *Nonstandard Analysis - Recent developments*, volume 983 of *Lecture Notes in Mathematics*, pages 120–133. Springer, 1983.
13. D. Laugwitz. Leibniz' principle and Ω-calculus. In J. Salanskis and H. Sinacoeur, editors, *Le Labyrinthe du Continu*, pages 144–155. Springer France, 1992.
14. D. Laugwitz and C. Schmieden. Eine erweiterung der infinitesimalrechnung. *Mathematische Zeitschrift*, 89:1–39, 1958.
15. R. Lutz. La force modélisatrice des théories infinitésimales faibles. In J.-M. Salanskis and H. Sinaceur, editors, *Le Labyrinthe du Continu*, pages 414–423. Springer-Verlag, 1992.

16. P. Martin-Löf. *Intuitionnistic Type Theory.* Bibliopolis, Napoli, 1984.
17. P. Martin-Löf. Mathematics of infinity. In *COLOG-88 Computer Logic*, Lecture Notes in Computer Science, pages 146–197. Springer-Verlag Berlin, 1990.
18. E. Nelson. Internal set theory: A new approach to nonstandard analysis. *Bulletin of the American Mathematical Society*, 83(6):1165–1198, November 1977.
19. E. Nelson. *Radically Elementary Theory.* Annals of Mathematics Studies. Princeton University Press, 1987.
20. M. Niqui. Formalising exact arithmetic in type theory. In S. B. Cooper, B. Löwe, and L. Torenvliet, editors, *New Computational Paradigms: First Conference on Computability in Europe, CiE 2005, Amsterdam, The Netherlands, June 8–12, 2005. Proceedings*, volume 3526 of *Lecture Notes in Computer Science*, pages 368–377. Springer-Verlag, 2005.
21. J.-P. Reveillès and D. Richard. Back and forth between continuous and discrete for the working computer scientist. *Annals of Mathematics and Artificial Intelligence, Mathematics and Informatic*, 16(1-4):89–152, 1996.