

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

Nicolas Magaud, Agathe Chollet, Laurent Fuchs

22-24 July 2010

ADG'2010, Munich, Germany

- Constructions and Computations in Geometry
  - Exact Real Computations vs. Approximations
  - How to Handle Continuous Objects in a Discrete Setting ?
- So far, most Formal Proofs do not take Computations/Coordinates Issues into Account.
  - Proj. Geometry : Magaud, Narboux, Schreck (ADG'2008)
  - Geometric Algebras : Fuchs, Thery (ADG'2010)
- Computing is interesting, Reasoning about such Computations is even better
  - Correctness Issues ?

- Exact Geometric Computation (Yap, . . . )
  - A Pragmatic Approach
  - Only recently, some Considerations about the Foundations of the Calculus
- Computable Analysis (Weihrauch, . . . )
  - Foundations of Computation on Real Numbers
  - Correctness Properties of the Calculus

- Working on the Foundational Side. . .
- . . .but with an Effective Model based on Integers
- Getting the Best of the Two Worlds :  
at the same time a Foundational and Practical Approach
- Applications
  - Geometric Algebras  
(They, Fuchs : ADG'2010)
  - Exact Real Functions Representation  
(Chollet, Wallet, Fuchs et al. : IWCIA 2009)
  - Discrete Ellipsis Connectivity  
(Chollet, Wallet, Andres et al. : CompIMAGE 2010)

# The continuum onto a computer ?

## Working relatively to a given scale

- At a given scale ; points are of a specified size.
- We can use as many scales as necessary.
- To obtain enough points between two points ; it is always possible to change the scale.

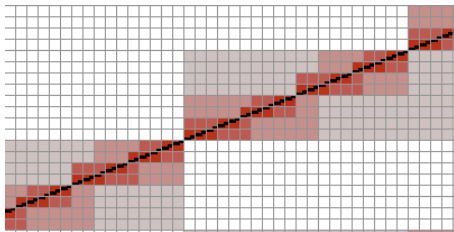


FIG.: A line of slope  $1/2$  represented at different scales.

# The continuum onto a computer ?

## What is used

- A constructive axiomatic of the real line (Bridges, 1999)
  - A way to define what are the **real numbers** that can be **computed**.
- A model of the continuum (Harthong-Reeb, 1984)
  - In order to define what could be the **continuum** in the **discrete world**.
- A nonstandard arithmetic (Laugwitz-Schmieden  $\approx 60$ , Martin-Löf  $\approx 80$ )
  - Define what is **large** and what is **small**.

# A discrete model of the continuum

## Obtain enough numbers between two numbers

- Choose an  $\Omega$ -number  $\omega$  **infinitely large** as new unity  
 $\omega \stackrel{\text{def}}{\equiv} 1_\omega$ .
- Hence, between two integer numbers, there is *as many* integers you want.

## The Harthong-Reeb line

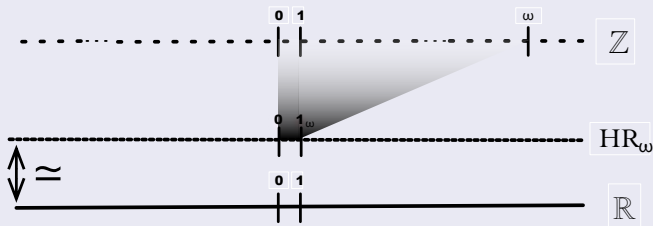
$$\mathcal{HR}_\omega = \{X \in \mathbb{Z}_\Omega, \exists n \in \mathbb{N}, |X| \leq n\omega\}$$

$\mathcal{HR}_\omega$  is a rescaling over  $\mathbb{Z}_\Omega$ .

# A discrete model of the continuum

*The real line  $\mathbb{R}$  is similar to the discrete line  $\mathbb{Z}$  seen from far away.*

## The Harthong-Reeb line





## The Harthong-Reeb line

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

- $X =_\omega Y \Leftrightarrow$  for all  $n$  in  $\mathbb{N}$ ,  $n|X - Y| \leq \omega$
- $X >_\omega Y \Leftrightarrow$  exists an  $n$  in  $\mathbb{N}$ ,  $n(X - Y) \geq \omega$
- $X +_\omega Y =_{def} X + Y$ .
- $X \times_\omega Y =_{def} \lfloor XY/\omega \rfloor$ .
- $0_\omega =_{def} 0$  and  $1_\omega := \omega$ .
- $-_\omega X =_{def} -X$ .
- If  $X$  is such that  $X \neq_\omega 0$   $X^{(-1)}_\omega =_{def} \left\lfloor \frac{\omega^2}{X} \right\rfloor$ .

# An axiomatic presentation of the constructive real line

- In 1999, Douglas Bridges introduced an axiomatic presentation of the constructive real line.
  - It is a system  $(R, +, \times, =, >, 0, 1, \text{Opp}, \text{Inv})$  which satisfies a list of 17 axioms.
  - Let us call a **Bridges-Heyting ordered field** any system which satisfies these axioms.
- These axioms are organized into 3 groups :
  - The first is dedicated to the algebraic operations,
  - The second to the order structure
  - The third to the usual Archimedes' axiom and to a constructive least-upper bound principle.

## Theorem

*The Harthong-Reeb line is a Bridges-Heyting ordered field.*

Here, the Harthong-Reeb line denotes the complete system

$$(\mathcal{HR}_\omega, +_\omega, \times_\omega, =_\omega, >_\omega, 0_\omega, 1_\omega, \text{Opp}_\omega, \text{Inv}_\omega)$$

- This result shows that the Harthong-Reeb line is a nonstandard model of the constructive real line.
- We formalize it in the Coq proof assistant.

## Definition

- Let us consider the sequences  $a = (a_n)_{n \in \mathbb{N}}$  with  $a_n \in \mathbb{Z}$ .
- equipped with the following equality :

$$a = b \text{ if there exists } N \in \mathbb{N} \text{ s.t. } \forall n > N, a_n = b_n.$$

- An  $\Omega$ -integer  $a$  is an equivalence class for this equality. We denote the set of  $\Omega$ -integers by  $\mathbb{Z}_\Omega$ .

## Examples

- $(2, 2, 2, 2, 2, 2, \dots)$  denotes the  $\Omega$ -integer 2.
- $(1, 5, 4, 2, 2, 2, \dots) = (2, 2, 2, 2, 2, 2, \dots)$  are in the same equivalence class.

# Basic Operations for Laugwitz-Schmieden Integers

## Operations and relations on $\mathbb{Z}_\Omega$ :

- $a + b =_{def} (a_n + b_n)$  and  $-a =_{def} (-a_n)$  and  $a \times b =_{def} (a_n \times b_n)$ ;
- $a > b =_{def} [(\exists N \forall n > N) a_n > b_n]$  and  $a \geq b =_{def} [(\exists N \forall n > N) a_n \geq b_n]$ ;
- $|a| =_{def} (|a_n|)$ .

## Two classes of elements :

- $a = (a_n)_{n \in \mathbb{N}}$  is **standard** if  $\exists p \in \mathbb{Z}$  such that  $\exists N \in \mathbb{N}, \forall n > N, a_n = p$  otherwise  $a$  is **nonstandard**.
- $a = (a_n)_{n \in \mathbb{N}}$  is **infinitely large** if  $(a_n)$  is increasing ( $\lim a_n \simeq +\infty$ ).

What we get is a nonstandard theory of the arithmetic (that was defined by Laugwitz et Schmieden).

Operations and relations on  $\mathbb{Z}_\Omega$  :

- $a + b =_{def} (a_n + b_n)$  and  $-a =_{def} (-a_n)$  et  $a \times b =_{def} (a_n \times b_n)$ ;
- $a > b =_{def} [(\exists N \forall n > N) a_n > b_n]$  et  $a \geq b =_{def} [(\exists N \forall n > N) a_n \geq b_n]$ ;
- $|a| =_{def} (|a_n|)$ .

Two classes of elements :

- $a = (a_n)_{n \in \mathbb{N}}$  is **standard** if  $\exists p \in \mathbb{Z}$  s.t.  $\exists N \in \mathbb{N}, \forall n > N, a_n = p$
- $a = (a_n)_{n \in \mathbb{N}}$  is **infinitely large** if  $(\lim a_n \simeq +\infty)$

- The usual properties true on  $\mathbb{Z}$  are not always verified for Laugwitz-Schmieden Integers. For instance

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

is not valid : e.g. take  $a = ((-1)^n)_{n \in \mathbb{N}}$  and  $b = ((-1)^{n+1})_{n \in \mathbb{N}}$ .

- Laugwitz-Schmieden is not an actual model of the NS Integers we use to build the  $\mathcal{HR}_\omega$  line.
- Nevertheless we can prove

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

because we have a decidability property for  $\mathbb{Z}$ .

- The Coq Proof Assistant :  
*Interactive Theorem Proving and Program Development*
  - Formal Definitions of Concepts
  - Formal Proofs of Properties
- Formalizing using Modules
  - A Module Specification : NS Integers
  - A Functor defining Harthong-Reeb Line on top of it
  - A (partial) Implementation of NS Integers -  
Laugwitz-Schmieden



# A Theory of Non-Standard Integers

- Basic Constructions and Operations

```
Parameters A:Type  a0:A  a1:A.
```

```
Parameter plusA : A -> A -> A.
```

```
Parameter leA : A -> A -> Prop. (?<=)
```

```
Parameter absA : A-> A.
```

- Properties

```
Parameter plus_neutral : forall x, 0 + x = x.
```

```
Lemma Ath : ring_theory a0 a1 plusA multA ...
```

```
Add Ring A_ring : Ath (abstract).
```

```
Parameter abs_triang :
```

```
forall x y, |x+y| ?<= |x| + |y|
```

We have an element  $w$ , which is positive.

The predicate  $\text{lim}$  is defined through the following rules :

(LIM1) *The integer 1 is limited.*

(LIM2) *The sum and the product of two limited integers are limited.*

(LIM3) *There exists integers which are not limited.*

(LIM4) *If  $X$  is limited and  $|Y| \leq |X|$ , then  $Y$  is itself limited.*

# Building the Harthong-Reeb Line $\mathcal{HR}_w$

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

```
Definition HRw := {x:A | P x }.
```

```
Lemma Padd : forall x y, P x -> P y -> P ( x + y ).
unfold P; intros x y Hx Hy.
elim Hx [...]
Qed.
```

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

# Algebraic Axioms (R1)

The group (R1) deals with the algebraic structure :

$$(R1.1) \quad x + y = y + x$$

$$(R1.2) \quad (x + y) + z = x + (y + z)$$

$$(R1.3) \quad 0 + x = x$$

$$(R1.4) \quad x + (-x) = 0$$

$$(R1.5) \quad xy = yx$$

$$(R1.6) \quad x(yz) = (xy)z$$

$$(R1.7) \quad 1x = x$$

$$(R1.8) \quad xx^{-1} = 1 \text{ for } x \neq 0$$

$$(R1.9) \quad x(y + z) = xy + xz$$

# The second group of axioms (R2)

The second group (R2) deals with the properties of the order and links it to the previously-proved algebraic properties :

$$(R2.1) \quad \neg((x > y) \wedge (y > x))$$

$$(R2.2) \quad (x > y) \Rightarrow \forall z((x > z) \vee (z > y))$$

$$(R2.3) \quad \neg(x \neq y) \Rightarrow x = y$$

$$(R2.4) \quad (x > y) \Rightarrow \forall z((x + z) \vee (y + z))$$

$$(R2.5) \quad ((x > 0) \wedge (y > 0)) \Rightarrow xy > 0$$

# The third group of axioms (R3)

Special Properties of the order relation :

(R3.1) *Archimedes Axiom.*

For all  $x \in R$ , there exists  $n \in \mathbb{Z}$  s.t.  $n > x$ .

(R3.2) *The constructive Upper-bound principle.* Let  $S$  be a non-empty subset of  $\mathcal{HR}_w$  s.t.

- $\exists b \in \mathcal{HR}_w \forall s \in S \ b \geq s$
- $\forall \alpha, \beta \in \mathcal{HR}_w \ (\beta > \alpha) \Rightarrow (\forall s \in S \ \beta \geq s) \vee (\exists s \in S \ s > \alpha)$

Then, there exists  $b \in \mathcal{HR}_w$  which is an upper bound of  $S$  :

- $\forall s \in S \ b \geq s$
- $\forall b' \ (b > b') \Rightarrow (\exists s \in S \ s > b')$

# Proof Techniques and Adequacy

- Symbolic computation requires more precise proofs.  
Let  $x$  be an integer (in  $\mathbb{Z}$ ,  $\mathbb{N}$  or  $\mathbb{A}$  ?)
- It avoids shortcuts, e.g. `HRwdiff / HRwequal`
- Modules and modules types to distinguish between theories and models of such theories.
- Proof-irrelevance : Objects of  $HR_\omega$  are equal regardless of the way the property  $P$  is shown
- High-level tools to avoid technical proofs : `Add Ring`
- Formalizing helps improving the writing of informal proofs.

- Non Standard : a real theory to talk about infinitesimals.
- Approximations are replaced by Infinitesimals.
- A scalable framework : one can change its point of view to have as many points as we want inbetween 2 given points of the line (this is achieved by changing the scale).
- A comprehensive framework to reason about geometric constructions
- Formalizing in Coq improves the confidence in the proofs, makes them more precise.



- Completing the Formalization  
(esp. w.r.t. the upper bound property)
- A really constructive model : Martin-Löf model
- Applications to Discrete Geometry
  - Proving formally formulas used to compute the intersection of discrete lines are sound.
  - Discrete Circles