Proving and Computing in Coq with the Harthong-Reeb line using Ω-integers:

Exact Real Computations with a Discrete Geometry Perspective

Nicolas Magaud
joint work with Laurent Fuchs,
initial contributions by Agathe Chollet and Guy Wallet

12-15 May 2014

TYPES'2014, IHP, Paris, France

Outline

Motivations and Context

Constructions and Computations in Geometry

- Exact Real Computations vs. Approximations
- How to Handle Continuous Objects in a Discrete Setting ?

Handling Geometric Computations in Formal Proofs ?

- e.g. Geometric Algebras : Fuchs, Thery (ADG 2010)
- Real Computations are Isolated, but Eventually Exact Real Computation is Required

Computing and Reasoning using the Same Framework

- Computing is Interesting
- Reasoning about such Computations is even Better

Our Goal

Foundational but Pratical as well

- Working on the Foundational Side...
- ...but with an Effective Model based on Integers
- Relies on Mathematical Results presented by Chollet et al. in PR2008 and TCS2012

Several Concrete Applications so far

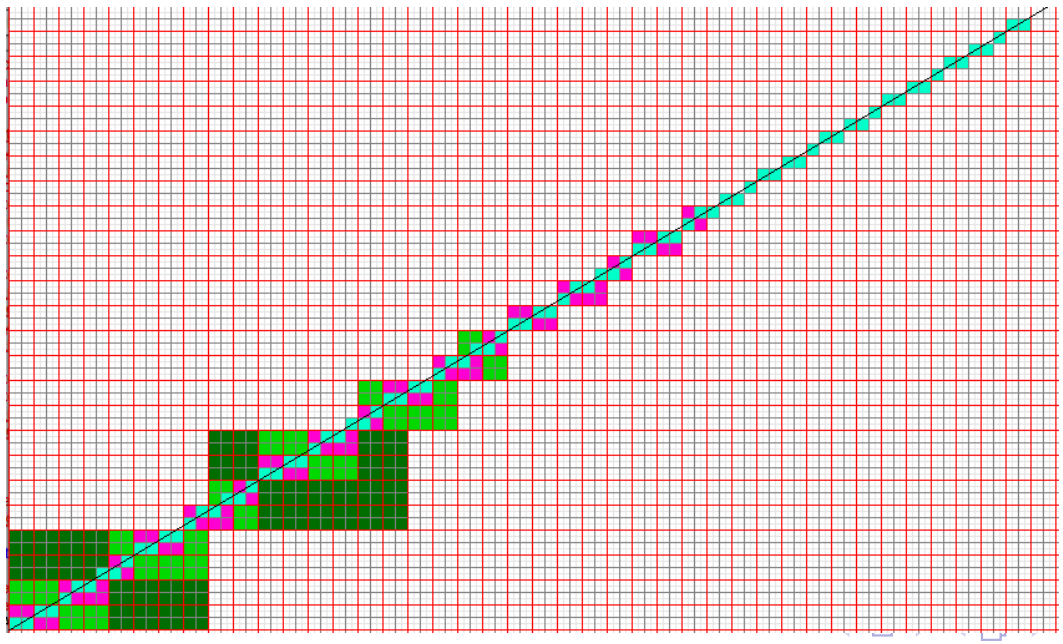
- Exact Real Functions Representation
  (Chollet, Wallet, Fuchs et al. : IWCIA 2009)
- Discrete Ellipsis Connectivity
  (Chollet, Wallet, Andres et al. : CompIMAGE 2010)
- Arithmetization of A Circular Arc
  (Richard, Wallet, Fuchs et al. : DGCI 2009)

Outline

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.



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 infinitely large integer ω as new unit $1_\omega =_{def} \omega$.
- Distinguish between 2 classes of elements : limited/standard or infinitely large
- Hence, between two integer numbers, there is *as many* integers as you want.

The Harthong-Reeb line

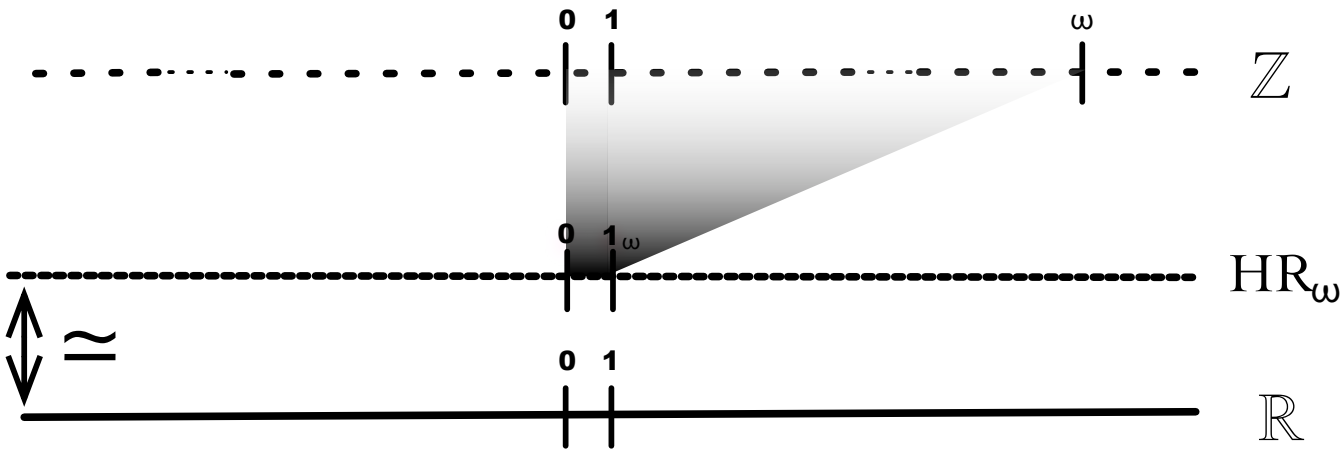
$$\mathcal{HR}_\omega = \{X \in \mathbb{Z},\ \exists n \in \mathbb{N},\ |X| \leq n\omega\}$$

$\mathcal{HR}_\omega$ is a rescaling over the chosen non-standard arithmetic.

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

Operations

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 $1_\omega =_{def} \omega$.
- $-_\omega X =_{def} -X$.
- If X is such that $X \neq_\omega 0 \quad X^{(-1)_\omega} =_{def} \left\lfloor \frac{\omega^2}{X} \right\rfloor$.

Axiomatic Presentation of the Constructive Real Line

Douglas Bridges (1999)

- A system $(R, +, \times, =, >, 0, 1, \mathrm{Opp}, \mathrm{Inv})$ which satisfies a list of 17 axioms.
- We shall call a Bridges-Heyting ordered field any system which satisfies these axioms.

Three Groups of Axioms

- Algebraic Operations
- Order Structure
- Archimedes' axiom and a Constructive Least-Upper Bound Principle

$\mathcal{HR}_\omega$ is a Bridges-Heyting ordered field

Theorem

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

Here, the Harthong-Reeb line denotes the complete system

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

Corollary

This result shows that the Harthong-Reeb line is a nonstandard model of the constructive real line.

Which Integers can be used to build the Harthong-Reeb line ?

- An interface : Axiomatic Non-Standard Integers
- An Implementation : Laugwitz-Schmieden Integers

Outline

A Theory of Non-Standard Integers

- A parameter type A (denoting non-standard integers)
- Usual operations +,-,*, <,$\leq$ and their properties
- Elements of $\mathcal{HR}_\omega$ are elements of A together with a proof that $\exists n : A, \texttt{lim}\ n \wedge 0 < n \wedge (|x| \leq n * w)$.

Extra-properties regarding non-standard features

(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 (e.g. ω).*

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

(LIM5) ...

Induction principle, LIM5 and overspill principle

- These three parameters allow to extend computing and reasoning to non limited integers such as ω.
- Induction principle

```
Parameter nat_like_induction :
 forall P : A -> Type,
 P a0 ->
 (forall n:A, (lim n /\ 0 <= n) ->
    P n -> P (plusA n a1)) ->
 forall n:A, (lim n /\ 0<= n) -> P n.
```

- (LIM5) Extends sequences defined on limited integers to infinitely large indices
- (Overspill) Extends properties which hold for limited integers to infinitely large integers

Algebraic Axioms for $\mathcal{HR}_\omega$(R1)

Algebraic Structure

(R1.1) $x + y =_w y + x$
(R1.2) $(x + y) + z =_w x + (y + z)$
(R1.3) $0 + x =_w x$
(R1.4) $x + (-x) =_w 0$
(R1.5) $xy =_w yx$
(R1.6) $x(yz) =_w (xy)x$
(R1.7) $1x =_w x$
(R1.8) $xx^{-1} =_w 1$ for $x \neq 0$
(R1.9) $x(y + z) =_w xy + xz$

The second group of axioms for $\mathcal{HR}_\omega$(R2)

Properties of the order w.r.t. the algebraic properties

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

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

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

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

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

The third group of axioms for $\mathcal{HR}_\omega$(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 $\mathcal{HR}_\omega$ s.t.

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

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

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

Outline

Laugwitz-Schmieden

How constructive is the numerical system $\mathcal{HR}_\omega$?

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

Examples

- $(2, 2, 2, 2, 2, 2, \ldots)$ denotes the Ω-integer 2.
- $(1, 5, 4, 2, 2, 2, \ldots) \equiv (2, 2, 2, 2, 2, 2, \ldots)$
- $\omega = (2^0, 2^1, 2^2, 2^3, 2^4, 2^5, \ldots)$

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

Three 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 ($\lim a_n \simeq +\infty$).
- $a = (a_n)_{n\in\mathbb{N}}$ is limited if $\exists p \in \mathbb{Z}$ such that $\mathtt{std}\ p \wedge 0 \leq p \wedge |a| < p$.

Not Quite A Model for Our Non-Standard Integers

The usual properties which hold for $\mathbb{Z}$ are not always verified for Laugwitz-Schmieden Integers.

For instance

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

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.

- Work-around : proposing an alternative set of axioms (only axioms R2.2, R2.3 and R3.2 -the least upper bound principle- need to be fixed [Chollet et al. TCS 2012])
- It requires, either restricting the elements of $\mathcal{HR}_\omega$ or changing the axioms statements.

Work-around : the *congruent* relation

The *congruent* relation and Axiom R2.3

$x = (x_n)$ and $y = (y_n)$ of $\mathcal{HR}_\omega$ are *congruent* ($x \triangle y$) if

$$(\forall r \in \mathbb{N})(\exists K \in \mathbb{N})(\forall k \geq K)(\forall l \geq K) \quad \left| \frac{x_k - y_k}{\omega_k} - \frac{x_l - y_l}{\omega_l} \right| \leq \frac{1}{r}$$

- fixing R2.3 into R2.3' :
  $\forall x, y \in \mathcal{HR}_\omega,\ x \triangle y \wedge \neg(x \neq_\omega y) \rightarrow x =_\omega y.$

Axioms R2.2 and R3.2

- Ad-hoc axioms R2.2' and R3.2' are tuned to fit into Laugwitz-Schmieden integers.
- It leads to an alternative version of the continuum [Chollet et al, TCS2012]. The proofs are formalized in Coq and thus confirmed to be correct.

Updating the Least Upper Bound Principle (R3.2)

- If S is a nonempty subset of $\mathcal{HR}_\omega$ that is bounded above relative to the relation $\geq_\omega$ and such that for all $(\alpha, \beta) \in \mathcal{HR}_\omega^2$ where β is an upper bound of S and $\alpha \in S$ and *for*$(a, b) \in \mathcal{HR}_\omega^2$ such that $\alpha \leq_\omega a \leq_\omega b \leq_\omega \beta$, either b is an upper bound of S or else there exists $s \in S$ with $s >_\omega a$. Then there exists an element $\tau \in \mathcal{HR}_\omega$ which is a least upper bound of S in the following weak meaning :
  - I' $\forall \mu <_\omega \tau, \exists s \in S$ such that $\mu <_\omega s$ (identical to I)
  - II' $\forall \delta \in \mathcal{HR}_\omega$ such that $\tau <_\omega \delta$, $(\exists b \text{ upper bound of } S) \tau \leq_\omega b <_\omega \delta$
- Proving this statement is completely different from the initial proof of *R*3.2. It inspects the actual elements of the sequences denoting Laugwitz-Schmieden integers and creates elements such as τ using ranks in the sequences (Set-exists is required).

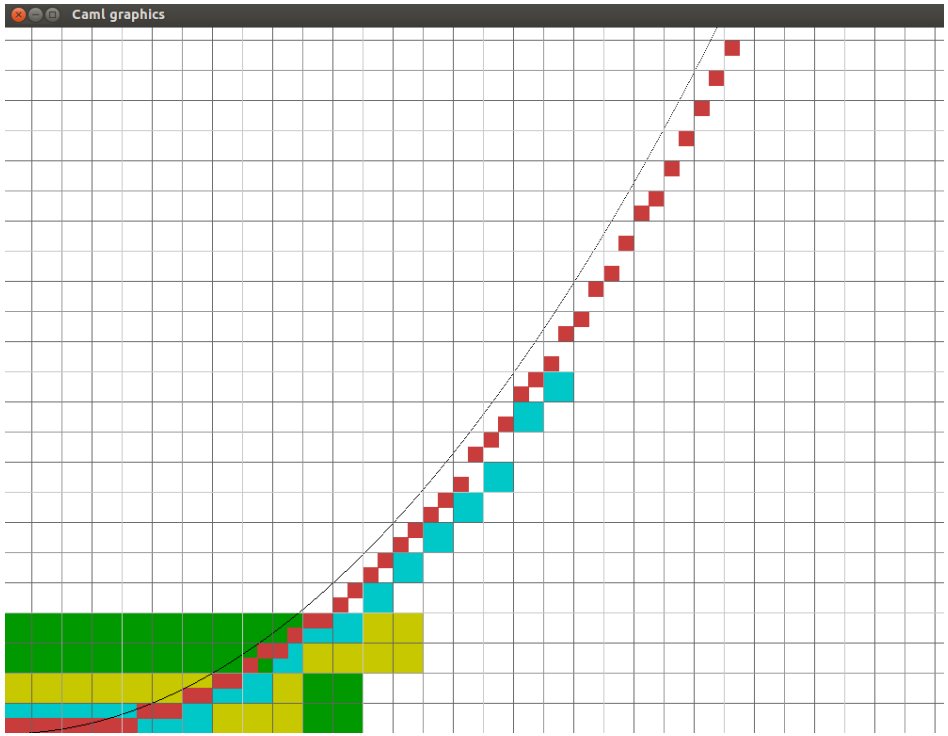
Work-around : Choosing a (Stable) Subset of $\mathcal{HR}_\omega$

Considering only elements of $\mathcal{HR}_\omega$congruent to 0

- They are Cauchy sequences, when viewing them as rationnals (after dividing by ω)
- They correspond to Bishop constructive reals
- It should be possible to connect them to CoRN and prove that they are isomorphic to the constructive reals of CoRN (work in progress)

Computing Continuous Functions

- The arithmetization of the function $t \mapsto \frac{t^2}{6}$.



- Computed using code extracted from Coq into Ocaml
- Uses Euler Scheme to compute approximations of the continuous function $X : T \mapsto X(T)$ which is the solution of $X' = F(X, T), X(A) = B$. Here, $F(X, T) = T/3$.

Technical Aspects/Problems in the Formal Proofs

Proof-irrelevance

For all functions with preconditions, we rely on proof-irrelevance in Prop.

Parametricity

Parametrizing decision procedures (such as omega) like we do for rings.

Σ-types for Existentials

Set-exists constructions (Σ-types) are required to complete the proof of the weak least upper bound principle, and well as the connection to CoRN.

Dependent Rewriting

Dependent Rewriting with an Alternative Equality (which is decidable, but is not Leibnitz equality) is needed

Outline

Summary

A non-standard approach

- 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).

What we formalized in Coq so far

- Proofs of Bridges axioms using the axiomatic description
- Computations (Ocaml extraction) and Proofs using an actual implementation of non-standard integers based on Laugwitz-Schmieden integers
- Available as a browsable development on the web

Future Work

Work in progress

- Switching from *Prop-exists* to *Set-exists*
- Connecting our development to CoRN
- Computing continuous functions inside Coq (instead of extracting in Ocaml)

Longer term goals

- Applications to geometric predicates computations (orientation, in-circle, etc.)
- Computing linear transformations in discrete geometry such as rotations (an on-going research project with the discrete geometry team in Strasbourg)