Questions about algebraic properties of real numbers

Henri Lombardi (*)

October 21, 2011

Abstract

This paper is a survey of natural questions (with few answers) arising when one wants to study algebraic properties of real numbers, *i.e.*, properties of real numbers w.r.t. $\{+, -, \times, >, \geq\}$ in a constructive setting.

Introduction

This paper is a survey of natural questions (with few answers) arising when one wants to study algebraic properties of real numbers, *i.e.*, properties of real numbers w.r.t. $\{+, -, \times, >, \geq\}$ in a constructive setting (see [1, 12]).

Why studying constructive real algebra?

A first reason is that constructive real algebra is not well understood! Constructive analysis is much more developped.

From a constructive point of view, real algebra is far away from the theory of discrete real closed fields (which was settled by Artin in order to understand real algebra in the framework of classical logic). Most algorithms for discrete real closed fields fail for Dedekind real numbers, because we have no sign test for real numbers.

Another reason is that within constructive analysis, it should be interesting to drop dependent choice (see [13]). A study of real agebra without dependent choice could help.

Last but not least, understanding constructive real algebra should be a first important step towards a constructive version of O-minimal structures.

Real algebra can be seen instead as the simplest O-minimal structure. Indeed classical O-minimal structures give effectiveness results inside classical mathematics, but they are not completely effective, because the sign test on real numbers is needed for the corresponding "algorithms".

Finally let us mention that we try also to propose a theory developped without using logical absurdity. Fred Richman shows that constructive mathematics are more elegant without dependent choice. The author thinks also that they are more elegant without logical absurdity. Let us remark for example that "Ex falso quodlibet" is easily replaced by "from $1 = 0$ you can prove any positive fact in a commutative ring". Another example: in constructive commutative algebra many theorems become simpler if we allow the trivial ring to be a local ring and a discrete field. E.g., a quotient of a local ring is a local ring, even if we don't know if the quotient is trivial or not.

Acknowlegment: I'm grateful to a referee for his (her) very useful comments and suggestions.

* Equipe de Mathématiques, UMR CNRS 6623, UFR des Sciences and Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE, email: lombardi@math.univ-fcomte.fr

1 Heyting fields ... without logical negation

First let us recall the basic theory of Heyting fields. W.r.t. the original one, we introduce a slight variation, where logical negation (which is $\bullet \Rightarrow \bot$) is replaced by $\bullet \Rightarrow (1 = 0)$.

1.1 Basic theory

Signature: $(\mathbf{K}, = 0, \neq 0, +, -, \times, 0, 1)$.

Here we use $\bullet = 0$ as a unary predicate in order to "simplify" the theory of commutative rings, by using only axioms **F1**. It becomes a "direct theory" with the meaning given in [4]. This allows us to omit axioms for the binary equality $\bullet = \bullet$ and to greatly simplify axioms for commutative rings, which are replaced by the computational machinery in $\mathbb{Z}[x_1, \ldots, x_n]$ which reduces any formula to a normal form. E.g., the axiom $xy = yx$ is replaced by the fact that $pq - qp$ is reduced to 0 for any p, q by the computational machinery in $\mathbb{Z}[x_1, \ldots, x_n]$.

In the sequel the terminology "direct axiom", "simplification axiom", "dynamical axiom", "collapsus axiom" is used as in [4], with the exception of replacing logical absurdity by $1 = 0$.

Another remark about notations, we replace the disjunction symbol $\vee$ after $\vdash$ by a coma, which is an old tradition in the sequent calculus.

Axioms:

F1 $(\mathbf{K}, = 0, +, -, \times, 0, 1)$ is a commutative ring.
I.e., computational machinery of commutative rings, plus three direct axioms for the unary predicate $\bullet = 0$:

$$\vdash\ 0 = 0, \qquad x = 0\ \vdash\ xy = 0, \qquad x = 0,\, y = 0\ \vdash\ x + y = 0.$$

F2 $x^2 = 0\ \vdash\ x = 0$ (simplification axiom)

F3 $x \neq 0$ means x invertible. This corresponds to axioms:

- $\vdash\ 1 \neq 0$ (direct axiom)
- $x \neq 0,\, y = 0\ \vdash\ x + y \neq 0$ (direct axiom)
- $x \neq 0,\, y \neq 0\ \vdash\ xy \neq 0$ (direct axiom)
- $xy = 0,\, y \neq 0\ \vdash\ x = 0$ (simplification axiom)
- $xy \neq 0\ \vdash\ x \neq 0$ (simplification axiom)
- $0 \neq 0\ \vdash\ 1 = 0$ (collapsus axiom)
- $x \neq 0\ \vdash\ \exists y\ xy - 1 = 0$ (dynamical axiom)

F4 $x + y \neq 0\ \vdash\ x \neq 0,\, y \neq 0$ (dynamical axiom)

HF $(x \neq 0\ \Rightarrow\ 1 = 0)\ \vdash\ x = 0$ (complicated axiom)

Definitions:

- $x = y$ means $x - y = 0$
- $x \neq y$ means $x - y \neq 0$

Remark. Axiom **F4** means that the ring is local. Axiom **HF** means that the local ring has its Jacobson radical equal to 0. In other words, an Heyting field is a local ring whose Jacobson radical is reduced to 0. Note also that in a generalized form **F4** could have an arbitrary finite sum in the hypothesis, and the corresponding disjonction in the conclusion. In the case where the finite sum is empty, we get the collapsus axiom but we have to replace the empty disjunction (which is locigal absurdity) by $1 = 0$. ∎

Examples: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(t)$, $\mathbb{C}(t)$, the set of primitive recursive real numbers, are Heyting fields (by $\mathbb{R}(t)$ we mean the ring of fractions $P(t)/Q(t)$ with at least one invertible coefficient for the polynomial $Q(t)$). ∎

Remark. Axiom **HF** is a very unpleasant axiom. It can be seen as a weakened form of the TEM axiom **DF** for discrete fields.

DF $\quad \vdash \; x = 0 \; , \; x \neq 0$

In order to use **HF** it should be necessary to give logical axioms for $\Rightarrow$, leaving (dropping?) the nice setting of dynamical theories. We give here **HF** as an example of what we want to avoid! ∎

Remark. We have given a set of axioms which is not at all a minimal one. E.g., in **F3** the collapsus axiom follows from the first simplification axiom.
If we keep only direct axioms and the collapsus axiom we get the theory of "rings with proper monoid" which "collapses simultaneously" with theory of discrete fields (cf. section 1.3 and [4]).
If we add simplification axioms to the theory of rings with proper monoid we get the theory of "quasi-domains". In this theory we get easily an "ex falso quodlibet": $1 = 0 \vdash x \neq 0$.
Moreover the theory of quasi-domains "proves the same facts" as the theory of discrete fields. ∎

Remark. Since **HF** and **DF** are formulations without logical negation: the trivial ring is allowed to be a discrete field. ∎

1.2 What is an algebraically closed Heyting field?

The following form of FTA for complex numbers was proven by Brouwer: "An homogenous bivariate polynomial with at least one invertible coefficient splits into linear factors".

A carefull analysis shows that dependent choice is used in the proof.

One possibility is to restrict the closure axiom by considering only separable polynomials. Complex numbers agree with this axiom (without using dependent choice). But this solution is too restrictive.

There is a Richman version of FTA without dependent choice [13]. It uses the set of n-multisets of complex numbers, which is constructed as a complete metric space. It should be very interesting to formalize Richman version inside a purely algebraic theory.

1.3 Simultaneous collapses for commutative rings and fields

When one considers a first order theory with only direct axioms, simplification axioms and dynamical axioms, there is a "dynamical interpretation" of the corresponding algebraic structures. Basic ideas of this interpretation are the following ones.

First one sees axioms as deduction rules. Second dynamical algebraic structures are defined by generators and relations. A "fact" inside such a dynamical algebraic structure is given by a predicate where variables have been replaced by closed terms. E.g., in the dynamical field defined by the generator y and the relation $45 = 0$ the fact $15 = 0$ can be proved. But

$x^7 - x^5 - x^3 + x = 0$ (which is true in $\mathbb{F}_5$ and $\mathbb{F}_3$) cannot be proved, and $y^7 - y^5 - y^3 + y = 0$ is not a fact.

Computing inside a dynamical algebraic structure becomes a purely computational machinery, without logic: when there is a disjunction in the conclusion of a dynamical rule, you open two branches; when there is an existential quantifier $\exists t$ you introduce a new formal parameter t. The original idea was the Computer Algebra device D5 explained in [5].

One proves a cut elimination theorem (see [4]): the first order theory with classical logic has exactly the same strength as the purely computational machinery.

So it is possible to speak about a dynamical field given by generators and relations: this is not a usual static object, it is a "dynamical object", where different branches of the computation correspond to different "static structures" corresponding to the dynamical one (i.e., usual models of the theory of fields with the given generators and relations): a dynamical structure appears as an uncompletely specified usual, static, algebraic structure. The bonus is that even if we are unable to construct static structures corresponding to the datas, we make sure computations.

E.g., this gives a clear constructive status to the algebraic closure of a field: consider this field as a dynamical algebraically closed field and make sure computations inside the dynamical structure.

For more details about dynamical algebra and simultaneous collapses see [4].

Theorem 1.1 [4] *Let* $\mathbf{A}$ *be a commutative ring. Let* Z, S *be two subsets of* $\mathbf{A}$. *Consider the* "dynamical field" *defined by these data (*i.e., *let* $x = 0$ *for* $x \in Z$, $x \neq 0$ *for* $x \in S$*). Then the collapsus* $1 = 0$ *occurs simultaneously for the following theories:*

a) Use only direct rules and collapsus.

b) Use direct rules and simplification rules.

c) Use direct rules, dynamic rules and **DF** *(simplification rules and collapsus follow).*

d) Add to the previous theory algebraic closure rules: any monic polynomial of degree ≥ 1 *has a root.*

Moreover the dynamical structures b), c) and d) prove the same facts.

In particular we get the following basic simultaneous collapes.

- A commutative ring which collapses as a dynamical algebraically closed discrete field collapses. In other words: consider a commutative ring given by generators and relations. If you can prove $1 = 0$ by using axioms of algebraically closed discrete fields and classical logic, then you can prove $1 = 0$ by using only axioms of commutative rings, without logic. This is a strong form of what is usually called the formal Nullstellensatz.

- A Heyting field which collapses as an algebraically closed discrete field collapses. In other words: if you can prove $1 = 0$ by using axioms of algebraically closed discrete fields and classical logic, then the Heyting field is trivial.

In particular this allows the following dynamic version of the algebraic closure of an Heyting field $\mathbf{K}$. Consider the structure $\mathbf{K}$ and compute (dynamically) inside this structure by adding algebraic closure axioms. This computation never leads to $1 = 0$, except if $1 = 0$ in $\mathbf{K}$. So equality inside $\mathbf{K}$ does not change when adding algebraic closure axioms. This is a weak form of embedding the Heyting field $\mathbf{K}$ in an algebraically closed field.

It should be better if we were able to construct a Heyting field containing $\mathbb{C}(t)$ where separable polynomials split into linear factors. This seems a priori a very difficult task.

2 Ordered Heyting fields

In this section we discuss the structure of "ordered Heyting fields". More precisely we try to describe the algebraic structure of $\mathbb{R}$, but only w.r.t. "rational operations" (this notion is somewhat vague, but we want to include as rational operations the function sup and functions that can be defined from elements of $\mathbb{R}(t_1, \ldots, t_n)$ on a domain where they are continuous).

2.1 Basic theory

Signature: $(\mathbf{K}, = 0, > 0, \geq 0, +, -, \times, \sup, 0, 1)$.

Abbreviation: $x \neq 0$ is an abbreviation for $x^2 > 0$.

Definitions

- $x = y$ means $x - y = 0$
- $x > y$ means $x - y > 0$
- $x \neq y$ means $x - y \neq 0$
- $x \geq y$ means $x - y \geq 0$

Direct rules

1. $(\mathbf{K}, = 0, +, -, \times, 0, 1)$ is a commutative ring.
2. $\vdash\ 1 > 0$
3. $x = 0\ \vdash\ x \geq 0$
4. $x > 0\ \vdash\ x \geq 0$
5. $\vdash\ x^2 \geq 0$
6. $(x > 0,\ y \geq 0)\ \vdash\ x + y > 0$
7. $(x > 0,\ y > 0)\ \vdash\ xy > 0$
8. $(x \geq 0,\ y \geq 0)\ \vdash\ x + y \geq 0$
9. $(x \geq 0,\ y \geq 0)\ \vdash\ xy \geq 0$

Collapsus axiom

10. $0 > 0\ \vdash\ 1 = 0$

Simplification rules

11. $x^2 \leq 0\ \vdash\ x = 0$
12. $(c \geq 0,\ cs > 0)\ \vdash\ s > 0$
13. $(s > 0,\ cs \geq 0)\ \vdash\ c \geq 0$
14. $(c \geq 0,\ x(x^2 + c) \geq 0)\ \vdash\ x \geq 0$

Dynamic rules

15. $x + y > 0\ \vdash\ x > 0\,,\ y > 0$
16. $xy > 0\ \vdash\ x > 0\,,\ -y > 0$
17. $x^2 > 0\ \vdash\ \exists y\, xy = 1$

Direct rules for sup

18. $\vdash\ \sup(x, y) = \sup(y, x)$
19. $\vdash\ \sup(x, y) \geq x$
20. $\vdash\ (\sup(x, y) - x)(\sup(x, y) - y) = 0$

Discrete ordered fields

DOF $\vdash\ x \geq 0,\ -x > 0$

Heyting ordered fields

HOF $(x > 0 \Rightarrow 1 = 0) \vdash x \leq 0$

Remark. **HOF** is an unpleasant axiom we should want to avoid. ∎

2.2 Simultaneous collapsus and provable facts

In this subsection we are mainly interested by the "basic restricted theory", i.e. the theory of algebraic structures given by the signature $(\mathbf{K}, = 0, \neq 0, > 0, \geq 0, +, -, \times, 0, 1)$ (without sup), and Rules 1 to 17.

Theorem 2.1 [4] *Let* $\mathbf{A}$ *be a commutative ring. Let* Z, P, S *be three subsets of* $\mathbf{A}$. *Consider the "*dynamical preordered ring*" defined by these data (*i.e., *let* $x = 0$ *for* $x \in Z$, $x \geq 0$ *for* $x \in P$, $x > 0$ *for* $x \in S$*). Then the collapsus occurs simultaneously for the following theories:*

a) Use only direct rules.

b) Use direct rules and simplification rules.

c) Use direct rules, dynamic rules and **DOF** *(simplification rules follow).*

d) Add real closure rules: any monic polynomial whose sign changes between a *and* b *has a root on* (a, b)

Moreover the dynamical structures b), c) and d) prove the same facts.

So adding **DOF** as an axiom in an ordered Heyting field does not change facts, and does not produce a collapsus. Samething with real closure rules.

In other words, feel free of using **DOF** and real closure axioms in an ordered Heyting field if you have only to prove a fact.

2.3 Problem with the function sup

The function $(x, y) \mapsto \sup(x, y)$ is well defined on $\mathbb{R}^2$, but the restricted theory of ordered Heyting fields (*i.e.*, the basic restricted theory plus axiom **HOF**) does not prove the existence of a sup z for any x, y, *i.e.*, the following statement is not provable (see [2])

$$\forall x, y\ \exists z \quad (z - x)(z - y) = 0,\ z \geq x,\ z \geq y$$

So the theory has to be improved by adding a symbol for the function sup with axioms 18 to 20.

Properties of sup

Define $\inf(a, b) = -\sup(-a, -b)$. We obtain:

$\vdash\ \sup(x, \sup(y, z)) = \sup(\sup(x, y), z)$	$\sup(x, y) > 0\ \vdash\ x > 0\,,\ y > 0$
$\vdash\ \sup(x + z, y + z) = \sup(x, y) + z$	$x > 0\ \vdash\ \sup(x, y) > 0$
$\vdash\ \sup(x, y) + \inf(x, y) = x + y$	$\sup(x, y) < 0\ \vdash\ x < 0$
$\vdash\ \sup(x, y)\inf(x, y) = xy$	$x < 0,\ y < 0\ \vdash\ \sup(x, y) < 0$
$x = \sup(x, y)\ \vdash\ x \geq y$	$\sup(x, y) \leq 0\ \vdash\ x \leq 0$
$x \geq y\ \vdash\ x = \sup(x, y)$	$x \leq 0,\ y \leq 0\ \vdash\ \sup(x, y) \leq 0$

Remark. The two sets $\{a, b\}$ and $\{\inf(a, b), \sup(a, b)\}$ have the same adherence, which is the set of roots of $(T - a)(T - b)$. Similar things with $(T - a_1) \cdots (T - a_n)$. ■

2.4 Some nonprovable properties in ordered Heyting fields

- $\vdash\ x=0\,,\ x\neq 0$
- $\vdash\ \forall x\ \exists y\ \ x^2y=x$
- $xy=0\ \vdash\ x=0\,,\ y=0$
- $\vdash\ x\geq 0\,,\ x\leq 0$
- $\vdash\ \sup(x,y)=x\,,\ \sup(x,y)=y$
- $(x\leq 0\ \Rightarrow\ 1=0)\ \vdash\ x>0$

For the (Bishop) real number field, the two first assertions are equivalent to **LPO**, the three following ones to **LLPO**, and the last one to **MP**.

2.5 What exactly is available?

Is "real linear algebra" correctly described by our axiomatization (axioms 1 to 20 and **HOF**)? If not, what is missing? Can we avoid **HOF**?

Same questions with real linear programming.

2.6 Other "rational" problems

E.g.,
$$\frac{(ax+by)xy}{x^2+y^2}$$

The above rational function is the prototype of a family (with parameters a,b) of continuous functions definable on $\mathbb{R}^2$ in a rational way.

Nevertheless it seems that the existential statement

$$(*)\qquad \forall a,b,x,y\ \ \exists z\quad z(x^2+y^2)=(ax+by)xy$$

is not provable with our axiomatisation of Heyting ordered fields.

So we have to add axioms as $(*)$, or, better, symbols of functions, each time we have a continuous function which is definable from an element of $\mathbb{Q}(X_1,\dots,X_n)$.

Related question: is it the case that every continuous function defined by an element of $\mathbb{R}(X_1,\dots,X_n)$ is a real point in a continuous family defined over $\mathbb{Q}(X_1,\dots,X_n)$ as in the previous example?

2.7 Locally closed semialgebraic sets: constructive definitions

A *semipolynomial*, or *sup-inf-polinomially-defined (SIPD) function* is given by a term in the language $(\mathbf{K},+,-,\times,\sup,0,1,(x_i)_{i\in\mathbb{N}})$ (with $\mathbb{Q}\subseteq\mathbf{K}$ if $\neg(1=0)$)

Let $\mathbf{R}$ be an ordered field containing $\mathbf{K}$. A *closed (resp. open) semialgebraic set in* $\mathbf{R}^n$ *defined over* $\mathbf{K}$, is a set

$$\{\,x\in\mathbf{R}^n\,|\,h(x)\geq 0\}\quad(\text{resp.}\quad\{\,x\in\mathbf{R}^n\,|\,h(x)>0\,\})$$

where h is an SIPD in n variables over $\mathbf{K}$. Finite "unions" and intersections correspond to sup and inf. Warning: this "union" is *not* equivalent to the pointwise one if we work in a constructive way.

A *locally closed semialgebraic set in* $\mathbf{R}^n$ *defined over* $\mathbf{K}$ is the intersection of a closed and an open semialgebraic sets in $\mathbf{R}^n$ defined over $\mathbf{K}$.

It seems better to avoid other "semialgebraic sets" such as

$$\{(x, y) \in \mathbf{R}^2 \,|\, x \neq 0 \vee x = y = 0\},$$

where the disjunction "$\vee$" leads to too many problems.

3 Real closure properties

Recall the real closure axiom in a discrete setting.

RCF1: Any univariate polynomial P such that $P(a)P(b) < 0$, $a < b$ has a zero on (a, b).

Axiom **RCF1** is not available for real numbers without dependent choice. The following one is constructively valid:

RCF2: Any univariate polynomial P such that $P(a)P(b) < 0$, $a < b$ and $P' > 0$ on (a, b) has a zero on (a, b).

But this is not sufficient. We will need virtual roots. See [11, 3].

3.1 Virtual real roots

Lemma 3.1 *A continuous increasing (resp. decreasing) function f on $[a, b] \subseteq \mathbb{R}$ ($a \leq b$) attains its (unique) minimum absolute value.*

Corollary 3.2 *One can define on the set of real univariate polynomials of (well defined) degree d, d* virtual root functions $\rho_{d,k}$ *($k = 1, \dots, d$) with the following characteristic properties,*

- $f(\rho_{1,1}(f)) = 0$
- $\rho_{d-1,k-1}(f') \leq \rho_{d,k}(f) \leq \rho_{d-1,k}(f')$ *if* $d \geq 2$
- $|f(\rho_{d,k}(f))| \leq |f(x)|$ *if* $\rho_{d-1,k-1}(f') \leq x \leq \rho_{d-1,k}(f')$

(with the convention $f(\rho_{d,0}(f)) = \varepsilon(-1)^d \infty$, $f(\rho_{d,d+1}(f)) = \varepsilon \infty$, where $\varepsilon = \pm 1$ is the sign of the leading coefficient)

Basic properties of virtual real roots

1. If $f(T) = (T - a)(T - b)$ then $\rho_{2,1}(f) = \inf(a, b)$, $\rho_{2,2}(f) = \sup(a, b)$.
2. If $\deg(f) = d$ and $f(x) = 0$ then $\prod_{i=1}^{d}(x - \rho_{d,i}(f)) = 0$.
3. A constructive version of **RCF1**:
   if $\deg(f) = d$, $a < b$ and $f(a)f(b) < 0$ then $\prod_{i=1}^{d} f(\mu_{d,i}(f)) = 0$, where $\mu_{d,i}(f) = \inf(b, \sup(a, \rho_{d,i}(f)))$. This implies **RCF2**.
4. Each $\rho_{d,i}(f)$ is a locally uniformly continuous function, and is a zero of the product $\prod_{k=0}^{d-1} f^{(k)}(T)$.
5. The "Budan-Fourier count" (on an interval) counts the virutal real roots [3].

A result à la Pierce-Birkhoff

An interesting result concerning virtual roots is the following one ([11]):

Theorem 3.3
Let $f : \mathbb{R}^n \to \mathbb{R}$ be a continuous semialgebraic function defined over $\mathbb{Q}$ which is integral over the ring $\mathbb{Q}[X_1, \ldots, X_n]$. Then f is a combination of virtual root functions and polynomials defined over $\mathbb{Q}$.

Remark. In the previous theorem, it is possible to replace $\mathbb{Q}$ by a discrete subfield of $\mathbb{R}$. ∎

Related question: is it possible to replace $\mathbb{Q}$ by $\mathbb{R}$?

Remark. The exact meaning of the hypothesis becomes not so clear. We should need a good definition for: "$f : \mathbb{R}^n \to \mathbb{R}$ is a continuous semialgebraic function."! ∎

3.2 A plausible definition

Definition 3.4 *A* real closed field *is given when you have an (Heyting) ordered field with virtual root functions in each degree satisfying the characteristic properties given in the real number field case.*

NB: We may use only virtual root functions of monic polynomials.

Examples of nondiscrete real closed subfields of $\mathbb{R}$ in this meaning

- Primitive recursive real numbers.
- Polytime computable real numbers.
- Turing computable real numbers.

Related problems

1. Construction of the real closure of an ordered field
2. Other closure properties
3. Projection Theorem
4. Constructive Positivstellensätze

3.3 Construction of the real closure of an (Heyting) ordered field

A priori this could seem not problematic. You add the virtual root functions as (formal) operators. You apply the axioms. From the simultaneous collapsus theorem, no collapsus can occur. So no catastrophe. But this is not sufficient.

E.g., if an axiom gives a conclusion which is a disjunction, how can we find a good branch (this is stronger than: open two branches, if one branch collapses the other is good). The solution would come from the fact that the real closure of a discrete ordered field is *strongly unique* (and the virtual roots are uniquely defined by their defining axioms).

Probably this works, but we need a more precise argument, giving clearly an algorithm.

Remark. Does this show the possibility to add a positive infinitesimal ε to $\mathbb{R}$ and to construct the real closure? No. But the obstacle does not come from the real closure. The problem is that the classical object $\mathbb{R}(\varepsilon)$ is *not* an ordered Heyting field. The fact that $\mathbb{R}(\varepsilon)$ does not collapse as a dynamic discrete ordered field is not sufficient! ∎

Related question: giving a structure or ordered Heyting field over $\mathbb{R}(X)$ is impossible in a constructive way?

3.4 Fundamental Theorem of Algebra

It seems that we can prove constructive versions of the **FTA** (in $\mathbf{R} + i\mathbf{R}$) for a real closed field $\mathbf{R}$ in the above meaning (*i.e.*, with virtual root functions symbols and axioms).

The first one is: any monic separable polynomial splits into linear factors.

A second one is a continuous version. This version gives as particular case a **FTA** "without dependent choice" for $\mathbb{C}$. In degree d the real parts of the d complex roots, enumerated in increasing order, are continuous "integral" semialgebraic functions of the coefficients. Same thing for the imaginary parts. So, applying Theorem 3.3 we can define d^2 continuous functions that "cover the complex roots", $\theta_{d,i}(f)$ $(1 \le i \le d^2)$, with the following meaning:

- $f(z) = 0 \quad \Longrightarrow \quad \prod_{i=1}^{d^2}(z - \theta_{d,i}(f)) = 0$
- for any $J \subseteq \{1, \ldots, d^2\}$ of cardinality $d^2 - d + 1$, $\prod_{i \in J} f(\theta_{d,i}(f)) = 0$.

This version is not as good as the Richman version, but it is a purely algebraic one.

3.5 Other continuous semialgebraic functions

In this subsection we consider other natural closure properties.

Distance map to a located closed semialgebraic set

In constructive analysis a closed subset or $\mathbb{R}^n$ is said to be located if the distance map can be computed. So there is a natural problem: consider a closed semialgebraic set in the constructive meaning (explained in Section 2.7). Assume it is located. In this case can we define the distance map by using only virtual root functions and inverses of everywhere positive polynomials?

First question: Does this work for closed semialgebraic sets defined over $\mathbb{Q}$?

If not, we have to add new symbols for these distance maps in order to give a good description of constructive real algebra.

Related question: Is it the case that a located closed semialgebraic set $S \subseteq \mathbb{R}^n$ appears always as a "real point" $S(\alpha)$ in a family $S(a)$ $(a \in J \subseteq \mathbb{R}^k)$ defined over $\mathbb{Q}$, the distance function $\varphi = d(x, S(a))$ being a continuous semialgebraic function of $(x, a) \in \mathbb{R}^n \times J$. Here φ is defined over $\mathbb{Q}$, J is locally closed.

Projection map on a located closed semialgebraic convex set

Same interrogations. So we are led to the following.

More general continuous semialgebraic functions

Let $\mathbf{R}$ be a discrete real closed subfield of $\mathbb{R}$. Let $S \subseteq \mathbf{R}^n$ a semialgebraic locally closed set. Consider a semialgebraic continuous function $S \to \mathbf{R}$ (let us recall that "semialgebraic continuous function" means a continuous function whose graph is a locally closed semialgebraic set). Such a function has a natural extension to $\mathbb{R}$-points of S, since it is uniformly continuous on each compact, for the natural topology of locally compact metric space of the domain.

Question: Do these functions can be expressed using only virtual root functions and inverses of everywhere positive polynomials?

If it is not the case, we need a better definition for real closed fields.

3.6 The projection theorem

Let $\mathbf{K}$ be a subfield of a discrete real closed field $\mathbf{R}$, $S \subseteq \mathbf{R}^n$ a semialgebraic set defined over the subfield $\mathbf{K}$ and $\pi_n = \mathbf{R}^n \to \mathbf{R}^{n-1} : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$.

The Tarski-Seidenberg projection theorem says that $\pi_n(S)$ is a semialgebraic set defined over $\mathbf{K}$.

We need good constructive versions of the Tarski-Seidenberg theorem when $\mathbf{R}$ is replaced by $\mathbb{R}$. The following weakened version is likely to be constructively valid. Let us call "compact semialgebraic subset of $\mathbb{R}^n$" a located closed bounded semialgebraic set.

Theorem 3.5 *(we hope)*
If S is a compact semialgebraic subset of $\mathbb{R}^n$ then so is $\pi_n(S)$.

If Theorem 3.5 is true, we expect that it will be true for "Heyting real closed fields". Perhaps this would force us to add new axioms in the definition of real closed fields.

3.7 Constructive Positivstellensätze

Let us recall that in the case of a discrete real closed field, the constructive Positivstellensatz follows directly from the simulatneaous collapsus theorem, and from the fact that the formal theory is complete.

The simultaneous collapsus theorem says us how to transform a simple (*i.e.*, dynamical) proof of impossibility (for a system of sign conditions on polynomials) in the real closure into an algebraic identity which shows clearly the impossibility in any ordered field.

Moreover the "cut elimination theorem" shows how to transform a first order proof into a dynamical one.

Most of this remains true in the nondiscrete context. In particular if you find a proof of the impossibility of a system of sign conditions on polynomials in $\mathbf{R}^n$ by using our axiomatisation of real closed fields, you will get a corresponding Positivstellensatz.

Moreover, since our theory is weaker than the discrete one, a proof is more informative and has to give a better form of Positivstellensatz, where the dependence of the algebraic identity w.r.t. the coefficients is best controlled (this dependence must have some continuity properties).

Such kind of continuity results have been obtain by C. Delzell and other authors for the 17-th Hilbert problem and for other variants of Positivstellensätze, in a discrete context (see [6, 7, 8, 9, 10]).

In the paper [9], you find a rather complete bibliography on the subject and a discussion about the consequences of the results for the Bishop real number field.

On the other side the formal theory is no more complete and there is no more a systematic way of testing the compatibility of a system of sign conditions.

References

[1] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag (1985). 1

[2] Coquand T., Lombardi H. *A note on the axiomatisation of real numbers.* To appear. Math. Logic Quarterly (2007) 6

[3] Coste M., Lajous T., Lombardi H., Roy M.-F. *Generalized Budan-Fourier theorem and virtual roots* Journal of Complexity **21** (2005), 479–486. 8

[4] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256. 2, 3, 4, 6

[5] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* EUROCAL '85. Lecture Notes in Computer Science n°204, (Ed. Caviness B.F.) 289–290. Springer 1985. 4

[6] Delzell C. *A continuous, constructive solution to Hilbert's 17^{th} problem.* Inventiones Mathematicae **76**, (1984) 365–384. 11

[7] Delzell C. *Continuous, piecewise-polynomial functions which solve Hilbert's 17th problem.* J. reine angew. Math. **440** (1993), 15773. 11

[8] Delzell C., Gonzalez-Vega L., Lombardi H. *A continuous and rational solution to Hilbert's 17th problem and several Positivstellensatz cases*, in: Computational Algebraic Geometry. Eds. Eyssette F., Galligo A.. Birkhäuser (1993) Progress in Math. n°109, 61–76. 11

[9] Gonzalez-Vega L., Lombardi H. *A Real Nullstellensatz and Positivstellensatz for the Semipolynomials over an Ordered Field.* Journal of Pure and Applied Algebra **90**, (1993) 167–188. 11

[10] Gonzalez-Vega L., Lombardi H. *Smooth parametrizations for several cases of the Positivstellensatz.* Math. Zeitschrift **225**, (1997), 427–451. 11

[11] Gonzalez-Vega L., Lombardi H., Mahé L. *Virtual roots of real polynomials.* Journal of Pure and Applied Algebra **124**, (1998) 147–166. 8, 9

[12] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag (1988). 1

[13] Richman F. *The fundamental theorem of algebra: a constructive development without choice.* Pacific Journal of Mathematics, **196** (2000), 213–230. 1, 3

Contents