Budan-Fourier Count and Constructive Real Algebra

Henri Lombardi

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

Meeting M.A.P. Trieste, 25/08/2008

Introduction

We examine natural questions arising when one wants to study "open" algebraic properties of real numbers, (*i.e.*, properties of real numbers w.r.t. $\{0,\ 1,\ +,\ -,\ \times,\ >\}$) in a constructive setting as in [2, Bishop&Bridges] and [17, Mines,Richman&Ruitenburg].

New results by Daniel Bembe [3] on the Budan-Fourier count show that virtual real roots should be a good way to attack some problems.

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 real numbers in a constructive context, 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 [18, Richman]). 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".

Contents

1 Descartes rule and beyond

1.1 Descartes rule and Budan-Fourier count

Descartes [4], [1].
Budan-Fourier [5, Budan] , [13, Fourier], [1].

1.2 Budan's proof and algebraic certificates

[5]
[3]
Comparison with algebraic certificates for Sturm's count

2 Virtual real roots

2.1 Basic lemmas and definitions

Lemma 2.1 *A continuous strictly monotonic function f on $[a,b] \subseteq \mathbb{R}$ $(a \leq b)$ attains its (unique) minimum absolute value.*

Lemma 2.2 *(algebraic mean value theorem)*
A polynomial function f on $[a,b] \subseteq \mathbb{R}$ $(a \leq b)$ whose derivative is > 0 on $]a,b[$ is stricty increasing. This works also on any ordered field because

$$f(b) - f(a) = (b-a)\,\delta$$

where δ is a positively weighted sum of

$$f'(a + k_i(b-a)), \qquad k_i \in \mathbb{Q} \cap]0,1[\ .$$

Warning: $1/(x^2-2)$ is well defined and has a positive derivative on $\mathbb{Q} \cap [-2,0]$ ∎

Corollary 2.3 *One can define on the set of monic real univariate polynomials of degree d, d* virtual root functions *$\rho_{d,k}$ $(k = 1,\ldots,d)$ with the following characteristic properties (with the convention $f(\rho_{d,0}(f)) = (-1)^d\,\infty$, $f(\rho_{d,d+1}(f)) = \infty$),*

- $$f(\rho_{1,1}(f)) = 0 \qquad (f(X) = X + b,\ \rho_{1,1}(f) = -b)$$
- $$\rho_{d-1,k-1}(f') \leq \rho_{d,k}(f) \leq \rho_{d-1,k}(f') \qquad (d \geq 2,\ k = 1,\ldots,d)$$
  (in fact use $\frac{f'}{d}$ in order to get a monic polynomial)
- *(minimizing the absolute value)*
  $$x \in [\,\rho_{d-1,k-1}(f'),\ \rho_{d-1,k}(f')\,] \quad \Rightarrow \quad |f(\rho_{d,k}(f))| \leq |f(x)|$$

2.2 Basic properties of virtual real roots

[16] and [8]. Recall that f is monic.

1. If $\rho_{d,k}(f) < x < \rho_{d,k+1}(f)$ then $\text{sign}(f(x)) = (-1)^{k+d} \quad (0 \leq k \leq d+1)$
2. If $f(T) = (T-a)(T-b)$ then $\rho_{2,1}(f) = \inf(a,b)$, $\rho_{2,2}(f) = \sup(a,b)$.
3. If $\deg(f) = d$ and $f(x) = 0$ then $\prod_{i=1}^{d}(x - \rho_{d,i}(f)) = 0$.
4. A constructive version of real closure property:
   if $\deg(f) = d$, $a < b$ and $f(a)f(b) < 0$ then $\prod_i f(\mu_{d,i}(f)) = 0$, where i corresponds to the Budan counts in a and b.
5. Each $\rho_{d,i}(f)$ is a locally uniformly continuous function, and is a zero of the product $\prod_{k=0}^{d-1} f^{(k)}(T)$.
6. The "Budan-Fourier count" (on an interval) counts the virtual real roots on the interval.

A result à la Pierce-Birkhoff

An interesting result concerning virtual roots is the following one ([16]):

Theorem 2.4
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 Ordered Heyting fields

In this section we discuss the "open" structure of "ordered Heyting fields".
See also [4], [9], [6], [7].

3.1 Basic theory

Signature: $(\bullet + \bullet,\ -\bullet,\ \bullet \times \bullet,\ 0,\ 1,\ \bullet > 0)$.

Abbreviations

- $x > y$ (or $y < x$) means $x - y > 0$
- $x \neq y$ means $(x-y)^2 > 0$

We try to avoid completely $\bullet = 0$ and $\bullet \geq 0$, as they are "negative". So the following direct rule 1. means to drop the usual equational axioms and to give the authorization of replacing any expression in $\mathbb{Z}[x_1, x_2, x_3, \ldots]$ (where $x_i's$ are either indeterminates or elements in $\mathbf{K}$) by another expression which is equal in the formal ring of polynomials $\mathbb{Z}[x_1, x_2, x_3, \ldots]$.

Direct rules

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

Collapsus axiom

6. $0 > 0\ \vdash\ x > y$

Simplification rules

7. $-x^2 > 0\ \vdash\ 0 > 0$
8. $x > 0,\ xy > 0\ \vdash\ y > 0$

Dynamic rules

9. $x + y > 0\ \vdash\ x > 0\,,\ y > 0$
10. $xy > 0\ \vdash\ x > 0\,,\ -y > 0$
11. $xy > 0\ \vdash\ x > 0\,,\ -x > 0$
12. $x^2 > 0\ \vdash\ \exists y\, xy = 1$

Discrete ordered fields

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

Heyting ordered fields

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

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

3.2 Simultaneous collapsus and provable facts

Theorem 3.1 [9] *Let* **A** *be a commutative ring. Let* Z, P, S *be three subsets of* **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 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 field if you have only to prove a fact.

Remark. This theorem was settled for a theory with $=$, $\geq$ and $>$. One can deduce a version with only $>$, $=$ and the theory given here. ∎

3.3 Some nonprovable properties in ordered Heyting fields

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

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

4 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 [16, 8].

4.1 A plausible definition

Definition 4.1 *A* real closed field *is given when you have an 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.

4.2 Construction of the real closure of an 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?

5 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 a good constructive axiomatisation of real closed fields, you will get a corresponding Positivstellensatz.

Moreover, since construcdtive theories are 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 [10, 11, 12, 14, 15]).

In the paper [14], 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] S. Basu, R. Pollack,M.-F. Roy, *Algorithms in real algebraic geometry*, Springer (2003). 4

[2] Bishop E., Bridges D. *Constructive Analysis*. Springer-Verlag (1985). 2

[3] Bembe D. *An algebraic certificate for Budan's Theorem*. Preprint (2008). 2, 5

[4] Bochnak J., Coste M., Roy M.-F. *Géometrie Algébrique Réelle*. Springer-Verlag. Ergeb. M. no 11. 1987.
There is a later english version. 4, 8

[5] Budan de Boislaurent F. *Nouvelle méthode pour la résolution des équations numériques d'un degré quelconque*, Paris, (1807). Réédition (1822), complétée, notamment avec le mémoire soumis à l' Académie des Sciences en 1811. 4, 5

[6] Coquand T. *Real Spectrum*. Technical report, (1999). 8

[7] Coquand T., Lombardi H. *A note on the axiomatisation of real numbers*. Math. Logic Quarterly. **54** (3), (2008), 224–228. 8

[8] Coste M., Lajous T., Lombardi H., Roy M.-F. *Generalized Budan-Fourier theorem and virtual roots* Journal of Complexity **21** (2005), 479–486. 7, 11

[9] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze*. Annals of Pure and Applied Logic **111**, (2001) 203–256. 8, 9

[10] Delzell C. *A continuous, constructive solution to Hilbert's 17th problem*. Inventiones Mathematicae **76**, (1984) 365–384. 13

[11] Delzell C. *Continuous, piecewise-polynomial functions which solve Hilbert's 17th problem*. J. reine angew. Math. **440** (1993), 15773. 13

[12] 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. 13

[13] Fourier J. *Analyse des équations déterminées*, F. Didot, Paris (1831). 4

[14] 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. 13

[15] Gonzalez-Vega L., Lombardi H. *Smooth parametrizations for several cases of the Positivstellensatz*. Math. Zeitschrift **225**, (1997), 427–451. 13

[16] Gonzalez-Vega L., Lombardi H., Mahé L. *Virtual roots of real polynomials*. Journal of Pure and Applied Algebra **124**, (1998) 147–166. 7, 11

[17] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra*. Springer-Verlag (1988). 2

[18] Richman F. *The fundamental theorem of algebra: a constructive development without choice*. Pacific Journal of Mathematics, **196** (2000), 213–230. 2