On computable fields of reals and some applications

Victor Selivanov[1]

A.P. Ershov IIS SB RAS (Novosibirsk)

A joint work with Svetlana Selivanova (KAIST)

WDCM-Conference, Novosibirsk, 24.07.2020

Contents

1. Introduction
2. Computable structures and computable fields.
3. Computably presentable fields of computable reals.
4. Applications to linear algebra.
5. Applications to PDEs.
6. Polynomial-time and primitive recursive versions.
7. Some open questions.

Introduction

The algorithms used in mathematics-oriented software can be divided into two big classes: symbolic algorithms which aim to find precise solutions, and approximate algorithms which aim to find "good enough" approximations to precise solutions. The symbolic algorithms are implemented e.g. in computer algebra systems or SMT-solvers while the approximate algorithms - in numerical analysis packages.

The both classes of algorithms are widely used in applications and in mathematical research. The symbolic algorithms correspond well to computations on discrete structures (with mathematical foundations in the classical computability and complexity theory) while the approximate algorithms - to computations on continuous structures (with mathematical foundations in the field of computability and complexity in analysis evolving under the slogan "Exact real computation").

Introduction

Exact real computation means finding an approximate solution to a numerical problem with guaranteed precision. Finding such a solution is of crucial importance for safety-critical applications but it often requires much additional work because it needs a sophisticated algorithm and careful estimations of approximations made during the computation.

In some cases the statement of a guaranteed-precision version of some problem on a continuous structure (which requires numerical mathematics and/or computable analysis) reduces it to a problem on a discrete structure which enables to apply the classical computability and complexity theory.

Introduction

In this talk we discuss two topics. First, we establish close relations of computably presentable fields of reals to the ordered field of computable reals.
Second, we partially fill the gap between the symbolic and numeric computations by applying the results about computable ordered field of reals to proving the computability (in the precise sense of TTE-approach to computations on continuous structures going back to A. Turing and systematized in the school of K. Weihrauch, among others) of solution operators for some systems of PDEs, based on well known numerical methods based on difference schemes.

Constructive structures

Definition. A structure $\mathbb{B} = (B; \sigma)$ of a finite signature σ is called constructivizable iff there is a numbering β of B such that all signature predicates and functions, and also the equality predicate, are β-computable. Such a numbering β is called a constructivization of $\mathbb{B}$, and the pair $(\mathbb{B}, \beta)$ is called a constructive structure.

Obviously, $(\mathbb{B}, \beta)$ is a constructive structure iff given a quantifier-free σ-formula $\phi(v_1, \ldots, v_k)$ with free variables among $v_1, \ldots, v_k$ and given $n_1, \ldots, n_k \in \mathbb{N}$, one can compute the truth-value $\phi^{\mathbb{B}}(\beta(n_1), \ldots, \beta(n_k))$ of ϕ in $\mathbb{B}$ on the elements $\beta(n_1), \ldots, \beta(n_k) \in B$.

Strongly constructive structures

Definition. A structure $\mathbb{B} = (B; \sigma)$ of a finite signature σ is called strongly constructivizable iff there is a numbering β of B such that, given a first-order σ-formula $\phi(v_1, \dots, v_k)$ with free variables among $v_1, \dots, v_k$ and given $n_1, \dots, n_k \in \mathbb{N}$, one can compute the truth-value $\phi^{\mathbb{B}}(\beta(n_1), \dots, \beta(n_k))$ of ϕ in $\mathbb{B}$ on the elements $\beta(n_1), \dots, \beta(n_k) \in B$. Such a numbering β is called a strong constructivization of $\mathbb{B}$, and the pair $(\mathbb{B}, \beta)$ is called a strongly constructive structure.

Note that we used above "Russian" terminology; the equivalent "American" notions for "constructivizable" and "constructive" are "computably presentable" and "computable", resp.
The notion of a strongly constructive structure is equivalent to the notion of a decidable structure in the western literature.

Examples

We illustrate the introduced notions by some number structures. Let $\mathbb{N} = (N; <, +, \cdot, 0, 1)$ be the ordered semiring of naturals, $\mathbb{Z} = (Z; <, +, \cdot, 0, 1)$ the ordered ring of integers, $\mathbb{Q} = (Q; <, +, \cdot, 0, 1)$ the ordered field of rationals, $\mathbb{R} = (R; <, +, \cdot, 0, 1)$ the ordered field of reals, $\mathbb{R}_c = (R_c; <, +, \cdot, 0, 1)$ the ordered field of computable reals, and $\mathbb{R}_{\mathrm{alg}} = (A; <, +, \cdot, 0, 1)$ the ordered field of algebraic reals (by definition, the algebraic reals are the real roots of polynomials with rational coefficients).

Then the structures $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are constructivizable but not strongly constructivizable; the structure $\mathbb{R}_{\mathrm{alg}}$ is strongly constructivizable; the structure $\mathbb{R}_c$ is not constructivizable.

Computable fields

Based on the notion of a computable structure, the computability issues in algebra and model theory were thoroughly investigated. In particular, a rich and useful theory of computable fields was developed.

For instance, M. Rabin in 1960 has shown that the algebraic closure of a computable field is computably presentable. Around 1970, Yu.L. Ershov and independently E.W. Madison have shown that the real closure of a computable ordered field is computably presentable.

Since the ordered field $\mathbb{Q}$ of rationals is computably presentable, the field $\mathbb{C}_{\mathrm{alg}} = (C_{\mathrm{alg}}; +, \times, 0, 1)$ of complex algebraic numbers and the ordered field $\mathbb{R}_{\mathrm{alg}} = (R_{\mathrm{alg}}; \leq, +, \times, 0, 1)$ of algebraic reals are computably presentable.

Computable reals

The field $\mathbb{R}_c$ of all computable reals is countable, real closed, and not computably presentable. But, in some sense, it is "partially computably presentable".

Let $\varkappa$ be a constructivisation of $\mathbb{Q}$ and $\{\varphi_n\}$ be the standard computable numbering of all computable partial functions on $\mathbb{N}$. Define a partial function ρ from $\mathbb{N}$ onto $\mathbb{R}_c$: $\rho(n) = x$ iff φ_n is total, $|\varkappa\varphi_n(i) - \varkappa\varphi_n(i+j)| < 2^{-i}$, and $\{\varkappa\varphi_n(i)\}_i$ converges to x.

The four arithmetical operations are computable, the relation $<$ is c.e., and the equality is co-c.e. w.r.t. ρ.

Computable fields of reals

A numbering μ is *reducible* to a (partial) numbering ν ($\mu \leq \nu$), if $\mu = \nu \circ f$ for some computable function f on $\mathbb{N}$.

Proposition 1. Let $\mathbb{B}$ be a computable ordered subfield of $\mathbb{R}$, and β be a constructivisation of $\mathbb{B}$. Then $\beta \leq \rho$, in particular $\mathbb{B} \subseteq \mathbb{R}_c$ (cf. Madison 1970).

Proposition 2. Let $\mathbb{B}$ be a subfield of $(\mathbb{R}; +, \cdot, 0, 1)$ and β be a constructivisation of $\mathbb{B}$ such that $\beta \leq \rho$. Then β is a constructivisation of the ordered field $(\mathbb{B}; <)$.

Proposition 3. Let $\mathbb{B}$ be a real closed subfield of $(\mathbb{R}; +, \cdot, 0, 1)$ β be a constructivisation of $\mathbb{B}$. Then β is a strong constructivisation of the ordered field $(\mathbb{B}; <)$.

Adjoining computable reals

We add the following theorem to the results of the previous slide. The theorem relates constructive fields of reals to the field $\mathbb{R}_c$ of computable reals.

Theorem. Let $\mathbb{A} \subseteq \mathbb{R}_c$ be constructivisable and $b \in \mathbb{R}_c$. Then there is a strongly constructivisable real closed $\mathbb{B} \subseteq \mathbb{R}_c$ such that $A \cup \{b\} \subseteq B$.
Thus, the union of all computably presentable real closed fields of reals is $\mathbb{R}_c$.

Cf. an independent result by R. Miller and V. Ocasio Gonzalez.

Example: For any fixed computable real matrix there is a strongly constructive real closed subfield $(\mathbb{B}, \beta)$ of $\mathbb{R}_c$ containing all the matrix coefficients.

Computability in linear algebra

Let $(\mathbb{B}, \beta)$ be a strongly constructive real closed ordered subfield of $\mathbb{R}_c$. Then one can compute, given a polynomial $p(x) = a_0 + a_1 x^1 \cdots + a_k x^k$ with coefficients in $\mathbb{B}$ (i.e., given a string $n_0, \ldots, n_k$ of naturals with $\beta(n_0) = a_0, \ldots, \beta(n_k) = a_k$) the string $r_1 < \cdots < r_m$, $m \geq 0$, of all distinct real roots of $p(x)$ (i.e., a string $l_1, \ldots, l_m$ of naturals with $\beta(l_1) = r_1, \ldots, \beta(l_m) = r_m$), as well as the multiplicity of any root r_j.

Spectral decomposition of a symmetric real matrix $A \in M_n(\mathbb{R})$ is a pair $((\lambda_1, \ldots, \lambda_n), (\mathbf{v}_1, \ldots, \mathbf{v}_n))$ where $\lambda_1 \leq \cdots \leq \lambda_n$ is the sequence of all eigenvalues of A (each eigenvalue occurs in the sequence several times, according to its multiplicity) and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a corresponding orthonormal basis of eigenvectors.

Proposition. Let $(\mathbb{B}, \beta)$ be a strongly constructive real closed ordered subfield of $\mathbb{R}_c$. Given a symmetric $n \times n$-matrix A with coefficients in $\mathbb{B}$, one can compute its spectral decomposition.

Computability in linear algebra

A *matrix pencil* is a pair (A, B) (often written in the form $\lambda A + B$) of real non-degenerate symmetric matrices such that A is positive definite (all its eigenvalues are positive). By *spectral decomposition* of such a pencil we mean a tuple

$$((\lambda_1, \dots, \lambda_n), (\mathbf{v}_1, \dots, \mathbf{v}_n), (\mu_1, \dots, \mu_n), (\mathbf{w}_1, \dots, \mathbf{w}_n))$$

where $((\lambda_1, \dots, \lambda_n), (\mathbf{v}_1, \dots, \mathbf{v}_n))$ and $((\mu_1, \dots, \mu_n), (\mathbf{w}_1, \dots, \mathbf{w}_n))$ are spectral decompositions of the symmetric matrices A and D^*L^*BLD respectively, where L is the matrix formed by vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ written as columns and $D = \mathrm{diag}\{\sqrt{\lambda_1}, \sqrt{\lambda_2}, \dots, \sqrt{\lambda_n}\}$.

Proposition. Given a matrix pencil $\lambda A + B$ in a computable real closed field of reals, one can compute its spectral decomposition.

Computability in linear algebra

The status of spectral decomposition in computable analysis is quite different. Martin Ziegler and Vasco Brattka (based on old results by F. Rellich) have shown that the spectral decomposition of symmetric real matrices is not computable in the Turing sense (because it is not continuous). But this problem becomes computable if the number of distinct eigenvalues of the matrix is given as input.

This research was a motivation for our work because the second author was interested in the symmetric hyperbolic systems of PDEs, and difference schemes used in numeric methods for solving such systems require to compute spectral decompositions of symmetric matrices and matrix pencils.

Computability of PDEs

We consider the initial-value problem

$$\begin{cases} A\frac{\partial \mathbf{u}}{\partial t} + \sum_{i=1}^{m} B_i \frac{\partial \mathbf{u}}{\partial x_i} = f(t,x), \ \ t \geq 0, \\ \mathbf{u}|_{t=0} = \varphi(x_1, \dots, x_m). \end{cases} \tag{1}$$

Here $A = A^* > 0$ and $B_i = B_i^*$ are constant symmetric $n \times n$-matrices, $t \geq 0$, $x = (x_1, \dots, x_m) \in Q = [0,1]^m$, $\varphi : Q \to \mathbb{R}^n$ and $\mathbf{u} : [0, +\infty) \times Q \rightharpoonup \mathbb{R}^n$ is a partial function acting on the domain H of existence and uniqueness of the Cauchy problem (1). The solution $\mathbf{u}$ depends continuously on $\varphi, f, A, B_1, \dots, B_m$.

Computability of PDEs

Symmetric hyperbolic systems are used to describe a wide variety of physical processes like those considered in the theories of elasticity, acoustics, electromagnetism etc., see e.g. [Friedrichs 1954, Godunov 1971,76, Landau, Lifschitz 1986 etc.].

They were first considered in 1954 by K.O. Friedrichs. He proved the existence theorem based on **finite difference approximations**, in contrast with the Schauder-Cauchy-Kovalevskaya method based on approximations by analytic functions and a careful study of infinite series. The methods of Friedrichs are used to construct different stable difference schemes, in particular the Godunov scheme we used in our works.

The notion of a hyperbolic system (applicable also to broader classes of systems) is due to I.G. Petrovski.

Questions

Questions: Is the solution **u** computable

I. from given initial conditions φ and right-hand part f (with fixed computable coefficients),
II. from φ, f **and** coefficients A, B_i

and in which sense?

III. If yes, what is the complexity of computations?

Most of (few) papers on computability of PDEs rely on explicit solution formulas. As is well-known, **explicit solution formulas exist rarely**. Even for the simplest example of the wave equation the computability of the solution operator for boundary-value problem was formulated in [Weirauch, Zhong 2002] as an open question, and we have not seen any paper where this question would be answered.

Our results provide, in particular, a positive answer to this question for dissipative boundary conditions.
We hope that our methods can be applied to study computability of many other PDEs in the framework of computable analysis going back to A. Turing (1937) and A. Grzegorczyk (1957), recently developed by M. Pour El, J. Richards, Ker-I Ko, K. Weihrauch and others.

Results on computability in PDEs

I. For fixed computable matrices, the solution operator $(\varphi, f) \mapsto \mathbf{u}$ of (1), (2) is computable provided that the first and second partial derivatives of φ, f are uniformly bounded.

II. 1) The operator $(A, B_1, \ldots, B_m) \mapsto H$ is computable;
2) The solution operator $(\varphi, f, A, B_1, \ldots, B_m, n_A, n_1, \ldots, n_m) \mapsto \mathbf{u}$ of (1), (2) is computable under some additional spectral conditions on A, B_i.
Here n_A is the cardinality of spectrum of A (i.e. the number of different eigenvalues);
n_i are the cardinalities of spectra of the matrix pencils $\lambda A - B_i$.
Eigenvectors are in general not computable!
3) The solution operator $(\varphi, f, A, B_1, \ldots, B_m) \mapsto \mathbf{u}$ of (1) is computable when the coefficients of A, B_i run through an arbitrary computable real closed subfield of $\mathbb{R}$.

Bit complexity version

Based on deep facts of Computer Algebra, Alaev and S. have shown PTIME-presentability of $\mathbb{R}_{\mathrm{alg}}, \mathbb{C}_{\mathrm{alg}}$, and PTIME-computability of some versions of root-finding in these fields. We used this to establish upper bounds of bit complexity of some problems in linear algebra and PDEs. Examples:

Theorem. 1) For any fixed $n \geq 1$, there is a polynomial time algorithm which, given a symmetric matrix $A \in M_n(\mathbb{A})$, computes a spectral decomposition of A.
2) There is a polynomial time algorithm which, given a symmetric matrix $A \in M_n(\mathbb{Q})$, computes a spectral decomposition of A uniformly on n. The same holds if we replace $\mathbb{Q}$ by $\mathbb{Q}(\alpha)$ where α is any fixed algebraic real.

Similar results hold for matrix pencils.

Bit complexity version

Theorem. Let $m, n \geq 2$ be any fixed integers. Given $A, B_1 \ldots, B_m \in M_n(\mathbb{A})$, one can find the domain H of existence and uniqueness of the Cauchy problem (1) in polynomial time. Given also $a, M > 0$, $\varphi_1 \ldots, \varphi_n \in \mathbb{Q}[x_1 \ldots, x_m]$, $f_1 \ldots, f_n \in \mathbb{Q}[t, x_1 \ldots, x_m]$ with some quantities bounded by M, one can compute in exponential time a rational $T > 0$ with $H \subseteq [0, T] \times Q$, a spatial rational grid step h dividing 1, a time grid step τ dividing T and a rational h, τ-grid function $v : G_N^\tau \to \mathbb{Q}$ s. t. $||\mathbf{u} - \widetilde{\upsilon\,|}_H||_{sL_2} < a^{-1}$.

Our methods apply only to algebraic matrices because it is currently open whether there is a PTIME-presentable real closed field of reals which contains a transcendental number.

Primitive recursive version

Recently, we developed a PR-version of our approach, in particular of the Ershov-Madison theorem. A numbering $\alpha : \mathbb{N} \to \mathbb{R}$ is a *PR-archimedean field*, if $A = rng(\alpha)$ is an ordered subfield of $\mathbb{R}$, all $+, \cdot, -, ^{-1}, <, =$ are α-PR, and $\alpha(n) < f(n)$ for a PR-function f. Examples of typical results:

Theorem. Given a PR-archimedean field α, one can find a PR-archimedean field $\hat{\alpha}$ s.t. $\alpha \leq \hat{\alpha}$ and $\hat{A}$ is the real closure of A.

Theorem. If α is a PR-archimedean field with PR-splitting then $\hat{\alpha}$ and the algebraic closure $\overline{\alpha}$ have PR-root-finding.

Primitive recursive version

For any PR-archimedean field α, $A \subseteq \mathbb{R}_p$ — the field of PR-reals (the limits of PR fast Cauchy sequences of rationals). The field $\mathbb{R}_p$ is real closed (P. Hertling) and not computably presentable (N. Khisamiev).
The union of PR-archimedean fields coincides with $\mathbb{R}(\varkappa)$ — the set of PR reals b such that the sign of polynomials in $\mathbb{Q}[x]$ at b is checked primitive recursively. Probably, there is a PR real which is not in $\mathbb{R}(\varkappa)$.

Many transcendental reals (in particular, the Euler number e) may be included in PR-archimedean fields.

Many results of the first part extend to PR-computations on the reals. In particular, the Jordan form of a complex matrix over a PR-archimedean field with PR-splitting is PR-computable.

Proof sketch of Ershov-Madison's

We use the (slightly modified) construction of Madison: given a constructivization α of an ordered field $\mathbb{A}$, a constructivization $\widehat{\alpha}$ of the real closure $\widehat{\mathbb{A}}$ is defined as follows. Let $P(i,k)$ mean that either α^*_i is the zero polynomial (i.e., all coefficients of α^*_i are zero) or α^*_i has at most k roots in $\widehat{\mathbb{A}}$. Then $\widehat{\alpha}(\langle i,k\rangle)$ is defined as follows: if $P(i,k)$ then $\widehat{\alpha}(\langle i,k\rangle)=0$, otherwise $\widehat{\alpha}(\langle i,k\rangle)$ is the $(k+1)$-st (w.r.t. $<$) root b of α^*_i in $\widehat{\mathbb{A}}$ (i.e., $\alpha^*_i(b)=0$ and there are precisely k roots of α^*_i in $\widehat{\mathbb{A}}$ strictly below b).

Tarski elimination implies that $\widehat{\alpha}$ is indeed a constuctivisation. This proof uses the search through $\mathbb{A}$, hence it does not automatically yield the PR-version. Instead, we use Sturm isolation.

Proof sketch of PR Ershov-Madison's

1. There is a PR function f such that all real roots of any non-zero polynomial $\alpha_i^* \in \mathbb{A}[x]$ are in the interval $(-f(i), f(i))$. In particular, $\widehat{\alpha}(\langle i,k\rangle) < f(i)$ for all i, k (so $(\widehat{\mathbb{A}}, \widehat{\alpha})$ is PR-archimedean provided that it is a PR ordered field).

2. Given a polynomial $p \in \mathbb{A}[x]$ of degree > 1, one can primitive recursively find the Sturm sequence of polynomials $\mathrm{sseq}(p) = (p_0, p_1, \ldots, p_m)$ in $\mathbb{A}[x]$ with the following property: the number of real roots of p in any interval $(a, b]$ equals $v(a) - v(b)$ where $v(c)$, for $c \in \mathbb{R}$, is the sign alternation number in the sequence $(p_0(c), p_1(c), \ldots, p_m(c))$.

3. Given a non-zero polynomial $p \in \mathbb{A}[x]$ and $a, b \in \mathbb{Q}$, one can primitive recursively find the number of real roots of p in the interval $(a, b]$, as well as the number of all real roots of p.

Proof sketch of PR Ershov-Madison's

4. Given a polynomial $p \in \mathbb{A}[x]$ of degree $m \geq 2$, one can primitive recursively find a positive rational number $\delta_p < \Delta_p$ where Δ_p is the smallest distance between distinct roots of p.

5. Given a non-zero polynomial $p \in \mathbb{A}[x]$ and a positive rational number ε, one can primitive recursively find a sequence $I_1 < \cdots < I_l$ (where $l \geq 0$ is the number of real roots of p) of pairwise disjoint rational intervals of length $\leq \varepsilon$ which separate the real roots of p, i.e. every I_j contains precisely one real root of p.

6. Operations $+, \cdot, -, ^{-1}$ on $\widehat{A}$ are $\widehat{\alpha}$-PR.

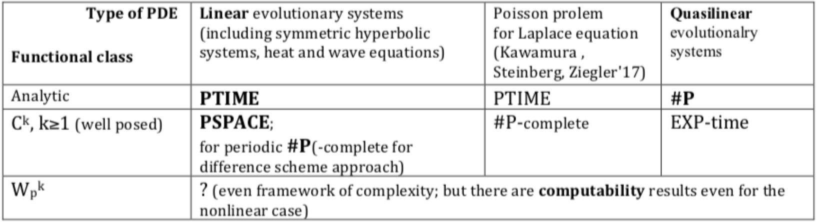
7. The relation $\leq$ on $\widehat{A}$ is $\widehat{\alpha}$-PR.

Some open questions

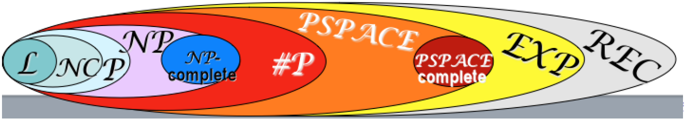
1. Is there a field which is PR constructivizable in signature $\{+,\cdot,^{-1}\}$ but not PR constructivizable in signature $\{+,\cdot,-,^{-1}\}$? Is there a field which is PR constructivizable in signature $\{+,\cdot,-\}$ but not PR constructivizable in signature $\{+,\cdot,-,^{-1}\}$?
2. Is there a PR field $(\mathbb{B},\beta)$ such that the property of being a reducible polynomial is β^*-PR but $(\mathbb{B},\beta)$ does not have PR splitting?
3. Is there a PR ordered subfield $(\mathbb{A},\alpha)$ of the reals which is not PR-archimedean?
4. Is it true that the algebraic closure of any PR field is PR-constructivizable?
5. Is there a PR-constructive algebraically closed field which does not have PR root-finding?
6. Is there $\alpha\in \mathit{pr}(\mathbb{R})$ such that $\widehat{\alpha}\not\in \mathit{prs}(\mathbb{R})$?
7. Describe the degree spectrum of the ordered field $\mathbb{R}_p$.

PS. Complexity Classification of PDEs

- Exact real computation approach (fixed initial data)
- A rigorous way to **classify** existing analytic/numerical algorithms for solving PDEs, by means of classical discrete **complexity** hierarchy; and finding new **optimal** algorithm for **exact** computation [Koswara, Pogudin, Selivanova, Ziegler, 19-20]



Type of PDE **Functional class**	**Linear** evolutionary systems (including symmetric hyperbolic systems, heat and wave equations)	Poisson prolem for Laplace equation (Kawamura , Steinberg, Ziegler'17)	**Quasilinear** evolutionalry systems
Analytic	**PTIME**	PTIME	**#P**
C^k, k≥1 (well posed)	**PSPACE**; for periodic **#P**(-complete for difference scheme approach)	#P-complete	EXP-time
W_p^k	? (even framework of complexity; but there are **computability** results even for the nonlinear case)		



THANK YOU FOR YOUR ATTENTION!!