On the computational complexity of algebraic structures

Victor Selivanov[1]

A.P. Ershov IIS SB RAS (Novosibirsk)

International Conference
"Algebra, Analysis, and Geometry"
August 24 2021, Kazan

Contents

Introduction

"Structure" in this talk always means "countably infinite algebraic structure of a finite signature". Computable structure theory (CST) is a well established branch of computability theory. The key notion here is that of a computably presentable structure, i.e. a structure isomorphic to a computable structure (a structure is computable if its universe is $\mathbb{N}$ and all signature functions and relations are computable). Using this notion, computability issues in algebra and model theory were thoroughly investigated.

Since CST is based on the general computability and often uses the unbounded search through universes of structures, it is not well suited for computer implementations where one has to pay attention to the complexity of algorithms and of structure presentations.

Introduction

Applicable versions of computable structures are important but much less investigated. In this talk we survey some recent results (mostly joint with P. Alaev or S. Selivanova) on two important classes of more feasible structures, namely PTIME-presentable and PR-presentable structures.

PTIME is well established as the most important complexity class for applications. Strictly speaking, most of feasible computational tasks are in this class. The great success of computer algebra in applications and in scientific computing is based on the fact that many basic structures are PTIME-presentable, and many important algorithms are in PTIME.

The importance of PR-presentability stems from the fact that it is in some respect close to feasible presentability but technically much easier, and has much better closure properties.

Introduction

Although the upper complexity bounds for a PR-algorithm may be awfully large, this is a principal improvement compared with the general computability where estimation of complexity is impossible in principle. In fact, PR-presentability of a structure may often be improved even to PTIME-presentability.

Recently, there was a renewed interest in PR structures which are recognized as a principal model for an emerging new paradigm of computability — the so called online computability. PR-solvability of a problem yields a solution algorithm which does not use an exhaustive search through a structure (usually written as unbounded WHILE...DO..., REPEAT...UNTIL..., or μ operator).

Computably presentable structures

D e f i n i t i o n. 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.

The "Russian" terminology used above was introduced by A.I. Mal'cev; the equivalent "American" notions for "constructivizable" and "constructive" are "computably presentable" and "computable", resp.

PR-presentable structures

PR-versions of the notions defined above are obtained by changing "computable" to "PR" in the definitions above. In particular, for numberings β and γ, β is *PR-reducible* to γ (in symbols $\beta \leq_{PR} \gamma$) iff $\beta = \gamma \circ f$ for some PR function f on $\mathbb{N}$, and β is *PR-equivalent* to γ (in symbols $\beta \equiv_{PR} \gamma$) iff $\beta \leq_{PR} \gamma$ and $\gamma \leq_{PR} \beta$. For $\nu : \mathbb{N} \to B$, a relation $P \subseteq B^n$ on B is ν-PR if the relation $P(\nu(k_1), \ldots, \nu(k_n))$ on $\mathbb{N}$ is PR. A function $f : B^n \to B$ is ν-PR if $f(\nu(k_1), \ldots, \nu(k_n)) = \nu g(k_1, \ldots, k_n)$ for some PR function $g : \mathbb{N}^n \to \mathbb{N}$. A structure $\mathbb{B} = (B; \sigma)$ is *PR-constructivizable* iff there is a numbering β of B such that all signature predicates and functions, and also the equality predicate, are β-PR. Such β is called a *PR-constructivization* of $\mathbb{B}$, and the pair $(\mathbb{B}, \beta)$ is called a *PR structure*.

PR functions

The PR functions are generated from the distinguished functions $o = \lambda n.0$, $s = \lambda n.n + 1$, and $I_i^n = \lambda x_1, \ldots, x_n.x_i$ by repeated applications of the operators of composition and primitive recursion. Thus, any PR function is represented by a "correct" term in the partial algebra of functions over $\mathbb{N}$. Intuitively, any total function defined by an explicit definition using (not too complicated) recursion is PR; the unbounded μ-operator is of course forbidden but the bounded one is possible.

Consider the structure $(\mathcal{N}; +, \circ, J, s, q)$ where $\mathcal{N} = \mathbb{N}^{\mathbb{N}}$ is the set of unary functions on $\mathbb{N}$, $+$ and $\circ$ are binary operations on $\mathcal{N}$ defined by $(p + q)(n) = p(n) + q(n)$ and $(p \circ q)(n) = p(q(n))$, J is a unary operation on $\mathcal{N}$ defined by $J(p)(n) = p^n(0)$ where $p^0 = id_{\mathbb{N}}$ and $p^{n+1} = p \circ p^n$, s and q are distinguished elements defined by $s(n) = n + 1$ and $q(n) = n - [\sqrt{n}]^2$ where, for $x \in \mathbb{R}$, $[x]$ is the unique integer m with $m \leq x < m + 1$.

Punctual structures

PR-presentable structures were introduced by A.I. Mal'cev in 1961 After a long break, PR-structures appeared as an intermediate stage of proving PTIME-presentability (Grigorieff, Cenzer-Remmel). After another break, PR-structures appeared as a promising candidate for capturing the on-line (or punctual) structures which give a practically relevant alternative to computable structures (Bazhenov-Downey-Kalimullin-Melnikov). A structure is *punctual* if it is isomorphic to a PR structure with universe $\mathbb{N}$. There is a PR graph which is not punctual (Kalimullin-Melnikov-Ng). We give a characterisation of punctual structures in the Mal'cev terminology.

P r o p o s i t i o n (Selivanova-S.) An infinite structure $\mathbb{B}$ is punctual iff it has a PR-constructivization β which is PR-infinite (i.e., there is a PR function f such that $\beta(f(i)) \neq \beta(f(j))$ whenever $i \neq j$.).

P-presentable structures

A structure is *P-presentable* if it isomorphic to a P-computable structure (the universe and all signature operations and relations are polynomial-time computable). The "Russian"-style version looks as follows:

By a *P-naming* we mean any function whose domain is a P-computable set of words over Σ. A P-naming μ is *P-reducible* to a P-naming ν (in symbols, $\mu \leqslant_P \nu$) if $\mu = \nu \circ f$ for a P-computable function $f : dom(\mu) \to dom(\nu)$, and μ, ν are *P-equivalent* (in symbols, $\mu \equiv_P \nu$) if $\mu \leqslant_P \nu$ and $\nu \leqslant_P \mu$. By a *P-naming of a set S* we mean a P-naming ν with $rng(\nu) = S$. A structure $(A; \sigma)$ is *P-constructivisable* if there is a P-naming α of A such that all the signature functions and predicates, as well as the equality predicate on A, are P-computable w.r.t. α. Such a P-naming is called a *P-constructivisation of* $(A; \sigma)$, and $((A; , \sigma), \alpha)$ is called a *P-constructive structure*.

P-presentable structures

Obviously, any P-presentable structure is P-constructivisable.

T h e o r e m (Alaev-S). Let $\mathbb{A}$ be a P-constructivisable structure. Then any its finitely generated structure is P-presentable.

Is it true that every P-computable quotient structure is P-computably isomorphic to a P-computable structure?

T h e o r e m (Alaev-S). (1) Suppose that P=NP. Then every P-computable quotient-structure $\mathbb{A}$ is P-computably isomorphic to some P-computable structure $\mathbb{B}$.
(2) Suppose that P$\neq$NP and, moreover, $\Sigma_2^p \neq \Pi_2^p$. Then there is a P-computable quotient-structure of the empty signature which is not P-computably isomorphic to a P-computable structure.

P-presentable structures

It is well known that there is a computable structure which is not PR-presentable, and there is a punctual structure which is not P-constructivisable.

T h e o r e m (Alaev, after Cenzer-Remmel). Every computable locally finite structure is P-presentable.

Many works in CST investigate the notion of computable categoricity (going back to Mal'cev). The PTIME version of this theory is much easier:

T h e o r e m (Alaev). Every P-computable infinite structure $\mathbb{A}$ has a P-computable copy which is not P-isomorphic to $\mathbb{A}$.

Computably presentable number fields

Theory of computable rings and fields is very rich. With any numbering β of a ring $\mathbb{B}$ we associate the numbering β^* of the ring $\mathbb{B}[x]$ as follows: $\beta^*(\langle i_0, \ldots, i_n \rangle) = \beta(i_0)x^0 + \cdots + \beta(i_n)x^n$ where $\langle i_0, \ldots, i_n \rangle$ is a PR coding of the finite non-empty strings of natural numbers. Iterating this construction, we obtain for each n the numbering $\beta^{[n]}$ of $\mathbb{B}[x_0, \ldots, x_n]$ (identifying $\mathbb{B}[x_0, \ldots, x_{n+1}]$ with $\mathbb{B}[x_0, \ldots, x_n][x_{n+1}]$): $\beta^{[0]} = \beta^*$, $\beta^{[n+1]} = (\beta^{[n]})^*$. Clearly, if β is a PR-constructivization then so is every $\beta^{[0]}$, and the evaluation function $ev_n : \mathbb{B}[x_0, \ldots, x_n] \times \mathbb{B}^n \to \mathbb{B}$ is PR w.r.t. the corresponding numberings.

It is well known that all standard functions and relations of polynomial arithmetics (like computing GCD or derivative) are computable. For most of them it is straightforward to check that they are PR.

Computably presentable number fields

Let $\mathrm{c}(\mathbb{R})$ consist of all $\alpha : \mathbb{N} \to \mathbb{R}$ such that $(\mathbb{A}, \alpha)$ is a constructive ordered field of reals. Let $\mathrm{cs}(\mathbb{R})$ be the set of all $\alpha \in \mathrm{c}(\mathbb{R})$ that have computable splitting, i.e., given a polynomial in $\mathbb{A}[x]$, one can compute its canonical decomposition to irreducible polynomials.

Given $\alpha \in \mathrm{c}(\mathbb{R})$, we define $\widehat{\alpha} : \mathbb{N} \to \mathbb{R}$. Let $P(i, k)$ mean that either α_i^* is the zero polynomial or α_i^* has at most k real roots. 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. $<$) real root b of α_i^* (i.e., $\alpha_i^*(b) = 0$ and there are precisely k real roots of α_i^* strictly below b). Then $\widehat{\alpha}$ is a numbering of the real closure $\widehat{\mathbb{A}}$ of $\mathbb{A}$.

Let also $\bar{\alpha}$ be the induced numbering of the algebraic closure $\overline{\mathbb{A}}$ of $\mathbb{A}$ (considered as a subfield of $\mathbb{C}$), i.e. $\bar{\alpha}\langle n_1, n_2 \rangle = (\widehat{\alpha}(n_1), \widehat{\alpha}(n_2))$.

Computably presentable number fields

P r o p o s i t i o n (after Rabin and Ershov-Madison). If $\alpha \in \mathrm{c}(\mathbb{R})$ then $\widehat{\alpha} \in \mathrm{cs}(\mathbb{R})$ and $\overline{\mathbb{A}}$ is a computable field with splitting.

A real x is *computable* if it is the limit of a computable sequence $\{q_i\}$ of rationals with $|q_i - q_{i+1}| < 2^{-i}$. The field $\mathbb{R}_c$ of all computable reals is countable, real closed, and not computably presentable.

T h e o r e m (Selivanova-S). (1) If $\alpha \in \mathrm{c}(\mathbb{R})$ then $\widehat{\mathbb{A}}$ is an ordered subfield of $\mathbb{R}_\mathrm{c}$.
(2) For any finite set $F \subseteq \mathbb{R}_c$ there is $\alpha \in \mathrm{c}(\mathbb{R})$ such that $F \subseteq A$.
(3) $\mathbb{R}_\mathrm{c} = \bigcup\{A \mid \alpha \in \mathrm{c}(\mathbb{R})\} = \bigcup\{\mathrm{A} \mid \alpha \in \mathrm{cs}(\mathbb{R})\}$.

In particular, 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.

PR-presentable number fields

By a classical theorem of Artin and Schreier, for any ordered field $\mathbb{A}$ there exists an algebraic ordered extension $\widehat{\mathbb{A}} \supseteq \mathbb{A}$ which is real closed.
Yu.L. Ershov and independently E.W. Madison proved a computable version of the Artin-Schreier theorem: if $\mathbb{A}$ is constructivizable then so is also $\widehat{\mathbb{A}}$.
We make search for a PR analogue of the Ershov-Madison theorem. Our proof below works only for *PR-Archimedean fields* which we define as the PR ordered subfields $(\mathbb{A}, \alpha)$ of $\mathbb{R}$ such that there is a PR function f with $\forall(\alpha(n) \leq f(n))$.

T h e o r e m (Selivanova-S). If $(\mathbb{A}, \alpha)$ is a PR-Archimedean subfield of $\mathbb{R}$ then so is also $(\widehat{\mathbb{A}}, \widehat{\alpha})$.

PR root finding

A computable field $(\mathbb{B}, \beta)$ *has computable root-finding* if, given a polynomial $p \in \mathbb{B}[x]$ of degree > 1, one can compute a (possibly, empty) list of all roots of p in $\mathbb{B}$. By Frölich-Shepherdson, $(\mathbb{B}, \beta)$ has computable root-finding iff it has computable splitting. As usual, the notion of PR root-finding is obtained by changing "computable" to "PR".

P r o p o s i t i o n (Selivanova-S). A PR field has PR root-finding iff it has PR splitting.

T h e o r e m (Selivanova-S). 1. If $\alpha \in \mathrm{pras}(\mathbb{R})$ then $(\widehat{\mathbb{A}}, \widehat{\alpha})$ and $(\overline{\mathbb{A}}, \overline{\alpha})$ have PR root-finding.
2. If $\alpha \in \mathrm{pras}(\mathbb{R})$ then $\widehat{\alpha} \in \mathrm{pras}(\mathbb{R})$.

PR fields vs PR reals

We search for a PR-analogue of the following fact: for any finite set F of computable reals there is a computable real closed ordered subfield $(\mathbb{B}, \beta)$ of the computable reals such that $F \subseteq B$. In particular, the union of all computable real closed fields of reals is the field $\mathbb{R}_{\mathrm{c}}$ of computable reals.

The PR-analogue of $\mathbb{R}_{\mathrm{c}}$ is the ordered field $\mathbb{R}_{\mathrm{p}}$ of PR reals. A real a is PR if $a = \lim_n q_n$ for a PR sequence $\{q_n\}$ of rational numbers which is fast Cauchy, i.e. $|q_n - q_{n+1}| < 2^{-n}$ for all n.
The PR-analogue of the results above is only partial:

P r o p o s i t i o n (Selivanova-S). Every PR ordered field of reals is a subset of $\mathbb{R}_{\mathrm{p}}$ but the union of such fields is a proper subset of $\mathbb{R}_{\mathrm{p}}$.

PR fields vs PR reals

Nevertheless, there is an easy criterion (a bit cumbersome formulation is omitted) of when a tuple of PR reals may be adjoined to a given PR-Archimedean field of reals. From this criterion we can deduce the following.

T h e o r e m (Selivanova-S). There is a PRAS-field of arbitrary transcendence degree. The ordered fields $\mathbb{Q}(e)$ and $\mathbb{Q}(\pi)$ (hence also $\widehat{\mathbb{Q}(e)}$ and $\widehat{\mathbb{Q}(\pi)}$) are PRAS-fields.

In contrast, we currently do not know any example of a PTIME-presentable field of reals containing a transcendental number. There is a PRAS-field which is not PTIME-presentable.

P-presentable number fields

With any $\alpha \in R_{\mathrm{alg}}$ we associate the unique pair (p_α, k) where $p_\alpha \in \mathbb{Q}[x]$ is the minimal (hence, irreducible) unitary polynomial of degree ≥ 1 with $p_\alpha(\alpha) = 0$, and k satisfies $\alpha = \alpha_k$ where $\alpha_1 < \cdots < \alpha_m$ is the increasing sequence of all real roots of p_α. The standard binary encoding $\mathrm{b} : \mathbb{Q} \to \{0,1\}^*$ induces an encoding $\mathrm{b} : \mathbb{Q}[x] \to \{0,1,*\}^*$, which associates with a polynomial $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$ if $n \neq 0$, the code $\mathrm{b}(a_n) * \cdots * \mathrm{b}(a_0)$. Now we associate with any $\alpha \in R_{\mathrm{alg}}$ the word $\mathrm{b}(p_\alpha) * \mathrm{b}(k)$ where (p_α, k) is the pair from the previous slide, which yields an injection $\mathrm{b} : R_{\mathrm{alg}} \to \{0,1,*\}^*$.

Let now $\mathbb{R}_1 = (R_1; \leqslant, +, \times, 0, 1)$, where $R_1 = \mathrm{b}(R_{\mathrm{alg}})$, be the isomorphic copy of $\mathbb{R}_{\mathrm{alg}}$ induced by b; we call it the *order presentation of* $\mathbb{R}_{\mathrm{alg}}$.

Complexity of order presentations

The bijection $\mathrm{b} : R_{\mathrm{alg}} \to R_1$ and the Gauss representation $z = x + iy$ of complex numbers induce a bijection between $R_1 \times R_1$ and C_{alg}. By encoding again the elements of $R_1 \times R_1$ by words in a finite alphabet in a standard way, we obtain a bijection $\mathrm{b} : C_{\mathrm{alg}} \to C_1$ which induces an isomorphism $g : \mathbb{C}_{\mathrm{alg}} \to \mathbb{C}_1 = (C_1; +, \times, 0, 1)$. Informally, $\mathbb{C}_1$ is the product $\mathbb{R}_1 \times \mathbb{R}_1$.

T h e o r e m (Alaev-S, after many facts of computer algebra). The structures $\mathbb{R}_1$ and $\mathbb{C}_1$ are p-computable, and the operations $-x$ and $1/x$ in these fields are also p-computable. As a corollary, $\mathbb{R}_{\mathrm{alg}}$ and $\mathbb{C}_{\mathrm{alg}}$ are p-computably presentable.

Sign presentation

Now we define other natural presentations of $\mathbb{R}_{\mathrm{alg}}$ and $\mathbb{C}_{\mathrm{alg}}$ known in the literature. For any polynomial $p \in \mathbb{Q}[x]$ of degree $n \geq 1$ without multiple roots, let $p'(x), p''(x), \ldots, p^{(n-1)}(x)$ be the sequence of its derivative polynomials. For any $x \in \mathbb{R}$, let $\bar{\varepsilon}_p(x) = (\varepsilon_1(x), \ldots, \varepsilon_{n-1}(x))$ where $\varepsilon_i(x) = 1, 0, -1$ iff $p^{(i)}(x)$ is resp. positive, zero, or negative. It is known that $\bar{\varepsilon}_p(\alpha) \neq \bar{\varepsilon}_p(\beta)$ whenever α and β are distinct roots of $p(x)$. Associate with any $\alpha \in R_{\mathrm{alg}}$ the unique pair $(p_\alpha, \bar{\varepsilon}_{p_\alpha}(\alpha))$, and let R_2 be the set of codes of such pairs in a natural word encoding based on the above-mentioned encoding of rational polynomials and a natural encoding of sequences of $1, 0, -1$. Let $\mathbb{R}_2 = (R_2; <, +, \times, 0, 1)$ be the isomorphic copy of $\mathbb{R}_{\mathrm{alg}}$ induced by the bijection $\alpha \mapsto (p_\alpha, \bar{\varepsilon}_{p_\alpha}(\alpha))$. We call the presentation $\mathbb{R}_2$ of $\mathbb{R}_{\mathrm{alg}}$ *sign presentation*.

Interval presentations

We can also code a real $\alpha \in \mathbb{R}_{\mathrm{alg}}$ by a pair $(p(x), I)$, where $p(x) \in \mathbb{Q}[x] \setminus \{0\}$, $p(\alpha) = 0$, and $I = (a, b]$ is an isolating rational interval for α including α and no other roots of $p(x)$. Call two pairs *equivalent*, $(p_1(x), I_1) \sim (p_2(x), I_2)$, if they encode the same real. Let
$A_3 = \{\mathrm{b}(p(x)) * \mathrm{b}(a) * \mathrm{b}(b) \mid p(x) \in \mathbb{Q}[x], a, b \in \mathbb{Q}$ and $(p(x), I = (a, b])$ encodes some $\alpha \in \mathbb{R}\}$,
let $E_3 \subseteq A_3 \times A_3$ be the relation corresponding to the equivalence of pairs, and let $R_3 = A_3/E_3$ be the corresponding quotient-set. Let $\mathbb{R}_3 = (R_3; <, +, \times, 0, 1)$ be the corresponding isomorphic copy of $\mathbb{R}_{\mathrm{alg}}$.

We call this presentation of $\mathbb{R}_{\mathrm{alg}}$ the *interval presentation*.

Equivalence of presentations

A similar interval presentation of $\mathbb{C}_{\mathrm{alg}}$ is also known in the literature. We say that a triple (p, I, K), where p is a polynomial and I, K are rational intervals as above, *defines the number* $z \in \mathbb{C}$ if z is the unique root of p in the rectangle $I + iK$. Let C be the set of codes of such triples (p, I, K) in a natural encoding, $\gamma : C \to C_{\mathrm{alg}}$ be the surjection defined similarly to the previous paragraph (of course, γ is not a bijection), and E be the corresponding equivalence relation on C. Then we have a presentation of $\mathbb{C}_{\mathrm{alg}}$ as a quotient-structure $\mathbb{C}_2 = (C/E; +, \times, 0, 1)$.

T h e o r e m (Alaev-S). The quotient-structures $\mathbb{R}_2, \mathbb{R}_3$ are p-computably isomorphic to $\mathbb{R}_1$ and are therefore p-computable. The quotient-structure $\mathbb{C}_2$ is p-computably isomorphic to $\mathbb{C}_1$ and is therefore p-computable.

Rational polynomial evaluation

T h e o r e m (Alaev-S). There exists an algorithm which, given $k \geqslant 1$, $\alpha_1, \ldots, \alpha_k \in C_{\mathrm{alg}}$ and $t(x_1, \ldots, x_k) \in \mathbb{Q}[x_1, \ldots, x_k]$, finds $\beta = t(\alpha_1, \ldots, \alpha_k) \in C_{\mathrm{alg}}$.
Let $n_i = \deg[\alpha_i]$ for each $i \leqslant k$, and let $n = \max_{i \leqslant k}\{n_i\}$. Then the working time of the algorithm is bounded by $(n_1 n_2 \cdots n_k)^c L^d$, or $n^{ck} L^d$, where c, d are some constants and L is the input length. In particular, for a fixed k we get a p-computable function that evaluates polynomials from $\mathbb{Q}[x_1, \ldots, x_k]$. Also, $\deg[\beta] \leqslant \prod_{i \leqslant k} \deg[\alpha_i]$.

It might be shown that the algorithm of this theorem cannot work in polynomial time uniformly on k even when evaluating the polynomials $x_1 + \cdots + x_k$.

Computing roots of algebraic polynomials

We consider equations of the form

$$t_e(\alpha_1,\ldots,\alpha_k)x^e+\ldots+t_1(\alpha_1,\ldots,\alpha_k)x+t_0(\alpha_1,\ldots,\alpha_k)=0, \quad (1)$$

where $\alpha_1,\ldots,\alpha_k \in C_{\rm alg}$ and $t_j(\bar{x}) \in \mathbb{Q}[x_1,\ldots,x_k]$. The problem is to find a list of (codes of) all roots from given $\mathrm{b}(\alpha_1)\,\&\,\cdots\,\&\,\mathrm{b}(\alpha_k)$ and $\mathrm{b}(t_0(\bar{x}))\,\&\,\cdots\,\&\,\mathrm{b}(t_e(\bar{x}))$. The form (1) is convenient since our algorithm remains polynomial for fixed k even if e grows.

T h e o r e m (Alaev-S). There exists an algorithm which, given $k \geqslant 1$, $\alpha_1,\ldots,\alpha_k \in C_{\rm alg}$ and polynomials $t_0(\bar{x}),\ldots,t_e(\bar{x}) \in \mathbb{Q}[x_1,\ldots,x_k]$, finds a list $\beta_1,\ldots,\beta_g \in C_{\rm alg}$ of all complex roots of (1).
The working time of the algorithm is estimated as $(n_1 n_2 \cdots n_k)^c L^d$, or $n^{ck} L^d$, where c, d are constant. In particular, if k is fixed or $n = 1$, we get a p-time algorithm for root-finding. Furthermore, $\deg[\beta_j] \leqslant e \prod_{i\leqslant k} \deg[\alpha_i]$ for $j \leqslant g$.

Applications to linear algebra

We describe some applications of the above results to spectral problems. There are several variations of such problems, for simplicity we consider only the typical example of such a problem for symmetric real matrices. The problem is rather subtle, e.g. the spectral decomposition of a symmetric 2×2-matrix is not computable (Ziegler-Brattka, after Rellich) but it becomes computable (even for $n \times n$-matrices uniformly on n) if matrix coefficients range over any fixed computable ordered field of reals.

As is well known, all eigenvalues of any symmetric real matrix are real. *Spectral decomposition* of such a matrix $A \in M_n(\mathbb{R})$ is a pair $((\lambda_1, \ldots, \lambda_n), (\mathrm{v}_1, \ldots, \mathrm{v}_n))$ where $\lambda_1 \leq \cdots \leq \lambda_n$ is the non-decreasing spectrum of A and $\mathrm{v}_1, \ldots, \mathrm{v}_n$ is a corresponding orthonormal basis of eigenvectors, i.e. $A\mathrm{v}_i = \lambda_i \mathrm{v}_i$ for $i = 1, \ldots, n$.

Applications to linear algebra

T h e o r e m (Selivanova-S). 1. Let $\alpha \in \mathrm{c}(\mathbb{R})$. Given n and a symmetric matrix $A \in M_n(\widehat{\mathbb{A}})$, one can compute a spectral decomposition of A uniformly on n. In particular, any computable symmetric real matrix has a computable spectral decomposition.

2. Let $\alpha \in \mathrm{pras}(\mathbb{R})$. Given n and a symmetric matrix $A \in M_n(\widehat{\mathbb{A}})$, one can primitive recursively find a spectral decomposition of A uniformly on n. In particular, this applies to matrices with coefficients in $\widehat{\mathbb{Q}(e)}$ or in $\widehat{\mathbb{Q}(\pi)}$.

3. For any fixed $n \geq 1$, there is a polynomial time algorithm which, given a symmetric matrix $A \in M_n(\mathbb{R}_{\mathrm{alg}})$, computes a spectral decomposition of A. This does not work uniformly on n.

We consider the initial-value problem

$$\begin{cases} A\frac{\partial \mathrm{u}}{\partial t} + \sum\limits_{i=1}^{m} B_i \frac{\partial \mathrm{u}}{\partial x_i} = f(t,x), \ \ t \geq 0, \\ \mathrm{u}|_{t=0} = \varphi(x_1, \ldots, x_m). \end{cases} \tag{2}$$

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

PR-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?

Results on computability in PDEs

I. For fixed computable matrices, the solution operator $(\varphi, f) \mapsto$ 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 $(\varphi, f, A, B_1, \ldots, B_m, n_A, n_1, \ldots, n_m) \mapsto$ 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 $(\varphi, f, A, B_1, \ldots, B_m) \mapsto$ u of (1) is computable when the coefficients of A, B_i run through an arbitrary computable real closed subfield of $\mathbb{R}$.

PR-computability on $\mathcal{N}$

For any $n \geq 0$, any term $t = t(v_1, \ldots, v_n)$ of the Robinson algebra determines the n-ary operator t on the Baire space $\mathcal{N} = \mathbb{N}^{\mathbb{N}}$ by setting $\mathrm{t}(g_1, \ldots, g_n)$ to be the value of t for $v_i = g_i$. Such operators are called PR. We give an example.

Let Ca be the set of sequences $q \in \mathbb{Q}$ such that $\varkappa \circ q \in \mathbb{Q}^{\mathbb{N}}$ is fast Cauchy, where $\varkappa$ is a bijective PR-constructivization of $\mathbb{Q}$. Let $\tilde{q}(n) = q(n)$ if $\forall i < n(|\varkappa(q_i) - \varkappa(q_{i+1})| < 2^{-i})$ and $\tilde{q}(n) = q(i_0)$ otherwise, where $i_0 = \mu i < n(|\varkappa(q_i) - \varkappa(q_{i+1})| \geq 2^{-i})$. Note $\tilde{q} \in \mathrm{Ca}$ for $q \in \mathcal{N}$, and $\tilde{q} = q$ for $q \in \mathrm{Ca}$, in particular $\mathrm{Ca} = \{\tilde{q} \mid q \in \mathcal{N}\}$.

Then $q \mapsto \tilde{q}$ is a unary PR operator on $\mathcal{N}$ which is a retraction.

PR-computability on metric spaces

We transfer primitive recursiveness on $\mathcal{N}$ to that on $\mathbb{R}$. Namely, we define $\gamma(q) = \lim_n \varkappa(\tilde{q}(n))$ and call this γ the *Cauchy representation* of $\mathbb{R}$.

A function $f : \mathbb{R}^{n+1} \to \mathbb{R}$ is called PR if $f(\gamma(p_0), \ldots, \gamma(p_n)) = \gamma(g(p_0, \ldots, p_n))$ for some PR function $g : \mathcal{N}^{n+1} \to \mathcal{N}$.

More generally, we can straightforwardly define PR metric spaces and PR-computability of functions between such spaces using standard Cauchy representations (the only difference with the classical definition is that now the distance between points in the specified dense set is required to be uniformly PR).

PR-computability of PDE

T h e o r e m (Selivanova-S). Let $M, p \geq 2$ be integers. Then the solution operator $(A, B_1, \ldots, B_m, \varphi) \mapsto \mathrm{u}$ for (2) is a PR-computable function (uniformly on m, n) from $S_+ \times S^m \times C_s^{p+1}(Q, \mathbb{R}^n)$ to $C_{sL_2}^p(H, \mathbb{R}^n)$ where S and S^+ are respectively the sets of all symmetric and symmetric positively definite matrices from $M_n(\widehat{\mathbb{A}})$, $||\frac{\partial \varphi}{\partial x_i}||_s \leq M$ and $||\frac{\partial^2 \varphi}{\partial x_i \partial x_j}||_s \leq M$ for $i, j = 1, 2, \ldots, m$.

T h e o r e m (Selivanova-S). Let $M, p \geq 2$ be integers and $A, B_1, \ldots, B_m \in M_n(\mathbb{R}_{\mathrm{p}})$ be fixed matrices satisfying the conditions in (2). Then the solution operator $\varphi \mapsto \mathrm{u}$ for (2) is a PR-computable function (uniformly on m, n) from $C_s^{p+1}(Q, \mathbb{R}^n)$ to $C_{sL_2}^p(H, \mathbb{R}^n)$, with the same constraints on φ as in the previous theorem.

PR-computability in PDE

T h e o r e m (Selivanova-S). Given integers $m, n, a \geq 1$, matrices $A, B_1 \ldots, B_m \in M_n(\widehat{\mathbb{A}})$, and rational functions $\varphi_1 \ldots, \varphi_n \in \widehat{\mathbb{A}}(x_1 \ldots, x_m)$, $f_1 \ldots, f_n \in \widehat{\mathbb{A}}(t, x_1 \ldots, x_m)$ as in (2), one can primitive recursively uniformly on m, n, a compute 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 an h, τ-grid function $v : G_N^\tau \to \widehat{\mathbb{A}}$ such that $||\mathrm{u} - \widetilde{v\,|_H}||_{sL_2} < a^{-1}$, where $\widetilde{v\,|_H}$ is the multilinear interpolation of the restriction of the grid function v to H.

Conclusion

Our results stress interesting interaction between symbolic algorithms (which aim to find precise solutions), and approximate algorithms (which aim to find "good enough" approximations to precise solutions). The symbolic algorithms implemented e.g. in computer algebra systems correspond well to computations on discrete structures (with mathematical foundations in the classical computability and complexity theory). The approximate algorithms are included into numerical mathematics packages and correspond well to computations on continuous structures (with mathematical foundations in the field of computability and complexity in analysis).

Conclusion

Fast progress of computation theory in the last decades made informal descriptions of several algorithms in the standard texts in algebra and analysis insufficient and sometimes even incorrect. They typically remain correct when interpreted in countable discrete structures (like computable ordered field of reals), though a finer distinction between general computability and feasible computability is desirable.

Some popular algorithms of linear algebra interpreted in continuous structures (like the real or complex numbers) become even incorrect; it seems desirable to add corresponding comments (which refer to computable analysis approach) in new editions of such textbooks.

THANK YOU FOR YOUR ATTENTION!!

References

- Basu S., Pollack R. and Roy M. *Algorithms in Real Algebraic Geometry*. Springer, Heidelberg, 2006.
- Brattka V., Hertling P. and Weihrauch K. A tutorial on computable analysis. In: New Computational Paradigms (edited by S. Barry Cooper, Benedikt Löwe, Andrea Sorbi), 2008, pp. 425–491.
- Evans L.C. *Partial Differential Equations*. Graduate Studies in Mathematics, v. 19, American Mathematical Society, 1998.
- Friedrichs K.O. Symmetric hyperbolic linear differential equations. *Communication on Pure and Applied Mathematics*, 7 (1954), 345–392.

References

- Godunov S.K. and Mikhailova T.Yu. *Represetations of the Rotation Group and Spherical Functions* (Russian). Nauchnaya Kniga, Novosibirsk, 1998.
- Godunov S.K. *Equations of Mathematical Physics* (in Russian). Nauka, Moscow, 1971.
- Godunov S.K., ed. *Numerical Solution of Higher-dimensional Problems of Gas Dynamics* (in Russian). Nauka, Moscow, 1976.
- Gordienko V.M. Un probleme mixte pair l'equation vectorielle des ondes: Cas de dissipation de l'energie; Cas mal poses. C.r. Acad. Sci., 288, No 10 (1979), Xerie A.P., 547–550.

References

- Godunov S.K. and Ryaben'kii V.S. *Introduction to the Theory of Difference Schemes* (in Russian). Fizmatgiz, Moscow, 1962. English translation: *Difference Schemes: An Introduction to the Underlying Theory (Studies in Mathematics and Its Applications)* Elsevier Science Ltd (June 1987).
- Gay W., Zhang B.-Y., Zhong N. Computability of solutions of the Korteweg-de Vries equation *Mathematical Logic Quarterly*, v. 47 (1), 2001, P. 93?110.
- John F. *Lectures on Advanced Numerical Analysis*. Gordon and Breach, Science Publishers, Inc., 1966.
- Ker-I Ko. *Complexity Theory of Real Functions*. Birkhäuser, Boston, 1991.

References


Kulikovskii A.G., Pogorelov N.V. and Semenov A.Yu. *Mathematical Aspects of Numerical Solution of Hyperbolic Systems*. Chapman & Hall/CRC Press, Boca Raton, 2001.


Landau L.D., Lifshits E.M., Kosevich A.M. and Pitaevskii L.P. *Theory of Elasticity. Third edition*. Reed Press, Oxford, 1986.


Landau L.D., Lifshits E.M. and Pitaevskii L.P. *Electrodynamics of Continuous Media. Second edition*. Pergamon Press, Oxford, 2004.


Petrovskii I. Über das Cauchysche Problem für Systeme von partiellen Differenzialgleichungen. *Rec. Math. (Matematicheskii Sbornik)*, 2(44), 1937, 814–868.

References

- Selivanova S.V. and Selivanov V.L. Computing solution operators of symmetric hyperbolic systems of PDEs. *Journal of Universal Computer Science*, v.15 (6), 2009, P. 1337–1364.
- Tarski A. *A Decision Method for Elementary Algebra and Geometry*,University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.
- Weihrauch, K. *Computable Analysis*. Berlin, Springer, 2000.
- Weihrauch K. and Zhong N. Is wave propagation computable or can wave computers beat the Turing machine? *Proceedings of the London Mathematical Society*, 85(2), 2002, 312–332.

References


Weihrauch K. and Zhong N. Computing the solution of the Korteweg-de Vries equation with arbitrary precision on Turing machines. *Theoretical Computer Science*, 332(1-3), 2005, 337–366.


Weihrauch K. and Zhong N. Computing Schrödinger propagators on Type-2 Turing machines. *J. Complexity (JC)*, 22 (6), 2006, P. 918–935.


Weihrauch K. and Zhong N. An Algorithm for Computing Fundamental Solutions. *SIAM J. Comput. (SIAMCOMP)*, 35 (6), 2006, P.1283–1294.