Interval Computations
No 2(4), 1992

PROOF OF FINITE-DIMENSIONAL INEQUALITIES BY MEANS OF INTERVAL ANALYSIS

P.S.Pankov

In contrast to other methods (algebraic transformations to reduce the given inequality to the known ones, differential calculus to obtain extrema, and Tarski's theory to analyze the inequality by polynomials with rational coefficients) the proposed method is based on the semisolvability of the problem of proving strict inequality on a compact set and of using validating computations. Some methods to reduce inequalities of other types to this kind and references to solved concrete problems are also given.

ДОКАЗАТЕЛЬСТВО КОНЕЧНОМЕРНЫХ НЕРАВЕНСТВ С ПОМОЩЬЮ ИНТЕРВАЛЬНОГО АНАЛИЗА

П.С.Панков

Помимо других методов (алгебраические преобразования для сведения данного неравенства к известным, дифференциальное исчисление для поиска экстремумов, теория Тарского для многочленов с рациональными коэффициентами) предложенный метод основан на использовании полуразрешимости задачи доказательства строгого неравенства на компакте и доказательных вычислений. Также даны некоторые приемы для сведения неравенств других типов к такому типу и ссылки на решенные конкретные задачи.

A literature survey (see, in particular, [1]) shows that, until interval analysis was developed (see [2]), two basic approaches to proving finite-dimensional inequalities had been used: algebraic transformations for reduction to one or several already known inequalities, and differential calculus (theory of extrema of smooth functions).

However, algorithmic solvability conditions (it is possible to construct an algorithm that always stops with a result) were obtained only for polynomials and roots of polynomials with integer coefficients (algebraic numbers).

In [3], algorithmic semisolvability conditions (if a problem has a solution, the algorithm stops) for strict inequalities on compact sets were formulated and certain ways of reducing non-strict inequalities to strict ones were given.

In this paper, we present constructivization and general methods of search for proofs of strict and non-strict inequalities; we also describe the constructed algorithm and some of the results obtained.

In Section 1, we present some well-known as well as some new results of constructive mathematical analysis. In addition, we give some information on algebraic number theory required in the subsequent sections.

Section 2 contains strict statements of algorithmic solvability and semisolvability for problems of proving inequalities for constants (null-dimensional functions) and non-constant functions.

In Section 3, algorithms for obtaining explicit proofs for finite-dimensional domains are described.

In Section 4, we present general methods of human-machine search for proofs of inequalities.

1. Some information on constructive mathematics

It is well known that not every definition of a real number f can lead to an algorithm for calculating f. A necessary component of such an algorithm is an algorithm determining a sequence of rational numbers $\{f_n\}$ that converges to f.

If the assumption that $\{f_n\}$ is not a Cauchy sequence implies a contradiction, the limit f of the sequence is called pseudocomputable [4].

Since the proof ad absurdum does not always yield an algorithm with a specified convergence rate, the definition of a computable number was introduced (a number f such that $\mid f - f_n \mid < 2^{-n}$). See, for instance, [5].

It is well-known that there exist numbers admitting only one-sided algorithmic estimates. In this context, a definition of upper (lower) pseudo-computable numbers was introduced in [4]; namely, $\{f_n\}$ is non-increasing (non-decreasing).

In [6], L.Brower classified computable numbers in terms of algorithmic comparability with rational numbers. In particular, numbers of highest IV order are those for which the problem of comparison with any rational number is algorithmically solvable.

Now we give some information on algebraic number theory (see, for example, [7]). The least degree of an equation with integer coefficients which is satisfied by a given $x \neq 0$ is called the degree $D(x)$ of x, while the maximum of the absolute values of the coefficients (after canceling by the greatest common divisor) is called the height $H(x)$. Let $Q(x) = D(x)H(x)$. One can then get the following estimates:

$$1/Q(x) < \mid x \mid < Q(x) \tag{1}$$

(We do not need sharp estimates or estimates that are close to sharp.)

If z is obtained from algebraic numbers x and y by one of the four arithmetic operations (assuming $y \neq 0$ when one divides by y), then z is also an algebraic number, and we have

$$\begin{gathered} D(z) \leq D(x)D(y), \\ H(x+y) \leq (D(z)(Q(x)+Q(y)))^{D(z)}, \\ H(x*/y) \leq (D(z)Q(x)Q(y))^{D(z)}, \\ D(\sqrt[n]{x}) \leq nD(x),\ H(\sqrt[n]{x}) \leq H(x). \end{gathered} \tag{2}$$

Now we proceed with constructively representable predicates and functions. For brevity, we *shall mark* points, intervals and interval vectors with rational coordinates, that is, quantities that are immediately constructively representable, with the letter K.

The following definition was introduced in [8] (with a short description). A predicate $P(x)$ defined for points of n-dimensional space is called

constructively stable if it is possible to construct an algorithm A_p which stops with a result for K-points z precisely when $P(z)$ is true, and which also gives the radius $A_p(z)$ of a neighbourhood in which the predicate remains true. Moreover, $P(x)$ implies that the set of radii $\{A_p(z)\}$ is bounded from below by a positive number in some neighbourhood of x.

It has been shown (see [4]) that the problem of proving truth of a constructively stable predicate on a closed bounded set in R^n is semisolvable.

We call a function $F(x)$ completely computable if $F(z)$ is a computable number for any K-point z and $F(z)$ is a constructively uniformly continuous function. It has been proven that for such functions the predicate "$F(x) > 0$" is constructively stable.

2. Algorithmic semisolvability and solvability

Theorem 1. *The problems of proving the inequalities $f > 0$ and $f < 0$ for a computable number f and the problem of proving the inequality $g < 0$ for a one-sided (for example, from below) pseudocomputable number g are semisolvable.*

Let us consider an example. In [9], to prove consistency of the obtained conditions by constructing a *concrete* equation, we had to prove that $b = \int_0^\infty \exp(\sigma + i \ln \sigma)\, d\sigma \neq 0$.

The calculations for the real and imaginary parts of b gave $b \in [0.62, 0.69] + i[0.30, 0.37]$, whence $b \neq 0$.

It is known that the general problem of determining the sign of a computable number is algorithmically unsolvable. However, this problem is solvable for constants determined by elementary operations. Existence of algorithms implementing arithmetic operations with algebraic numbers (constructing the corresponding polynomials) immediately follows.

Theorem 2. *If f is a number obtained from integers by a finite number of arithmetic operations and root extractions, then the problem of determining $\operatorname{sgn} f$ is algorithmically solvable. (See the survey in [10].)*

Let us describe an alternative algorithm. Estimate $Q(f)$ using (2) and compute any interval representation f_0 for f with width $W(f_0) < 1/Q(f)$. Then by (1) we have $\operatorname{sgn} f = \operatorname{sgn} f_0$.

The results of Section 1 imply the following theorem:

Theorem 3. *Assume that we have a K-interval vector X and algorithms that yield:*

a) *a K-interval extension $F_0(z)$ of a function $F: X \to R$ for any non-degenerate K-interval vector z;*

b) *a K-number $\delta > 0$ for any K-number $\epsilon > 0$ so that $W(z) < \delta$ implies $W(F_0(z)) < \epsilon$. Then the problem of proving the equality*

$$F(x) > 0 \qquad (x \in X)$$

is semisolvable.

The problem of proving a non-strict inequality as well as the problem of proving an inequality in an unbounded domain for a completely computable function are in general algorithmically unsolvable. A.Tarski has proved a result that includes the following special case:

Theorem 4. *The problems of proving the inequalities $F(x) > 0$ and $F(x) \geq 0$ for a polynomial F with integer coefficients are algorithmically solvable.*

More effective algorithms (see the survey in [11]) were constructed later. As in the proof of Theorem 2, we shall describe the algorithm (for $n = 1$; in this case $D(F)$ should be even) using the interval analysis as much as possible.

Using some minimization algorithm, we may find $f = \inf F$ as a computable number. On the other hand, $f = \min\{F(x) \mid F'(x) = 0\}$ and is an algebraic number, and the problem is reduced to the determination of $\operatorname{sgn} f$.

Though Theorems 2 and 4 provide solvable algorithms, it is more practical to use the algorithms of Theorems 1 and 3 together with the tricks described in Section 4.

3. Explicit proofs

All informative (non-service) messages of a computer can be divided into two classes: those for which it is necessary to mention that the

message was obtained through a certain algorithm and those for which it is not necessary.

This classification divides computer proofs into "program" proofs (that report whether the proof was successful or not) and "explicit" proofs (in which the computer prints a text that enables a person to verify correctness directly, though it would be difficult or even impossible to obtain such a text without a computer). When we get explicit proofs, the problem of minimizing their complexity for direct verification arises. (But the computer may perform many more operations than a "program" proof requires.)

When we look for a proof within the framework of Theorem 3, we have to find a cover $\{Z_j \mid j = 1, \ldots, M\}$ of the domain X such that $F_0(Z_j) > 0$ for all $j = 1, \ldots, M$. Since minimization of M in the multidimensional case is too difficult, in [12] an algorithm that realizes such an optimization in the two-dimensional case was constructed, provided the elements of the cover lie in parallel strips.

When more general inequalities than those described in Theorem 3 are being proved, conditions presented by logical functions of predicates of the form "$F_k(x) > 0$",where F_k is a function (analytically) obtained from F, may arise (see Section 4). So we introduce an indicator function $J_F(Z)$ such that its (integer) value shows the verification complexity of proof of the inequality in Z for a person. (This function must satisfy the natural condition: $(G'' \subset G') \Rightarrow (J_F(G'') \leq J_F(G'))$.

The optimization problem for an explicit proof in a domain X (not necessarily rectangular) then reads as follows:

$$\sum J_F(Z_j) \to \min\,(\cup Z_j \supset X).$$

We introduce the following notation: if $Z \cap X = \emptyset$, then $J_F(Z) = 0$ (this is used when we enclose X in a rectangular domain (the interval vector T). If the interval extensions computed contain 0 (direct proof is not successful), then we set $J_F(Z) = \omega$, where ω is a large number (greater than the maximal permissible verification complexity of a proof).

If the bounds of the Z_j's are given with too many significant digits, it is obvious that the proof will be too complex. So we require that the projections on the i-th axis be multiples of some h_i. Without loss of

generality, we can assume that all $h_i = 1$, i.e., the bounds of T and Z are integers.

Yu.V. Matiyasevich observed that the aforementioned algorithm could often give results that were far from optimal in the most general setting, and proposed the following.

A division of Z into two parallelepipeds will be called a "splitting" of Z. We have to minimize $\sum J_F(Z_j) \to \min$ provided that $\cup Z_j = T$ and that the cover $\{Z_j\}$ was obtained through successive splitting of D.

The following recursive algorithm has the simplest form among all the algorithms solving this problem:

$$J_0(Z) = \begin{cases} J_F(Z) \text{ if the volume of } Z \text{ is equal to 1;} \\ \min(J_F(Z), \min\{J_0(Z') + J_0(Z'')\}) \text{ otherwise.} \end{cases}$$

where the innermost min is taken over all splittings of Z. Then $J_0(T)$ gives the required results.

A corresponding subroutine (with some enhancements that diminish the number of repetitions while searching) has been written in PASCAL–8000.

4. Combined methods for search for proofs of inequalities

Suppose we have to prove an inequality (strict of the form (3) or non-strict) for a finite number of scalar variables in a given domain X.

a) By means of equivalence transformations and change of variables we try to eliminate:

   i) use of transcendental functions of variables;

   ii) calculation of roots other than square roots;

   iii) calculation of square roots and division.

b) If X is not bounded, we try to replace the inequality being proved by an equivalent one with a bounded domain.

   b_1) If the inequality is homogeneous (e.g. geometric) then, without loss of generality, we can assume that some norm of the vector of variables is equal to 1.

b_2) one can make substitutions of the form $z = 1/x$ (for the scalar case), which transform unbounded domains into bounded ones: $(1 \leq x < \infty) \Rightarrow (0 < z \leq 1)$. This may be combined with a study of the asymptotic behaviour of the functions in a neighbourhood of points at infinity (see, e.g., [4]).

c) If the inequality is strict, we jump to f), and otherwise proceed to d).

d) By standard methods of non-validating computations (as S.Ulam proposed) followed by strict proof, we determine the subset $X_0 \subset X$, where $F(x) = 0$. (Usually, X_0 consists of some points or lines.)

e) Separately, we prove the inequality in a sufficiently small neighbourhood X_1 of the set X_0 by the standard methods, or by reduction of this inequality to strict inequalities for other functions corresponding to F, followed by application of validating computations to them. (For example, in [14] it was shown that for a problem of the form $F(x) \geq 0 \quad (0 \leq x \leq x_1)$ we had $F(0) = F'(0) = F''(0) = 0$ and $F'''(x) > 0$.) In the remaining domain $X \backslash X_1$ the equality is strict.

f) For proving a strict inequality in a bounded domain, we use the algorithm of generalized bisection of the domain (see, e.g., [13]), or the algorithm of Section 3 if the inequality is simple enough.

Some results obtained with the help of these methods using the software [15] are described in [3] and [4].

There is also a possibility of using methods of heuristic-logic search as in [16].

References

1. Hardy G.H., Littlewood J.E. and Polya G., *Inequalities*, Cambridge, 1934.

2. Kalmykov S.A., Shokin Yu.I. and Yuldashev Z.H., *Methods of interval analysis*, Nauka, Novosibirsk, 1986. (in Russian)

3. Pankov P.S., *Validating computations on computers*, ILIM Frunze, 1978. (in Russian)

4. Pankov P.S., Bayachorova B.D. and Yugai S.A., *Numerical theorem proving by electronic computers and its application in various branches of mathematics*, Cybernetics **18** no. 6 (1982).

5. Markov A.A. and Nagornyi N.M., *The theory of algorithms*, Nauka, Moscow, 1984. (in Russian)

6. Martin-Löf P., *Notes on constructive mathematics*, Almquist and Wiksell, Stockholm, 1976.

7. Fel'dman N.I., *Approximations of algebraic numbers*, MGU Publishers, Moscow, 1981. (in Russian)

8. Pankov P.S., *Using constructive stability of predicates for automatization of proofs*, Problems of Theoretical Cybernetics: Abstracts of reports of IV All-Union conference, Irkutsk, 1985. (in Russian)

9. Imanaliev M.I. and Pankov P.S., *The phenomenon of a rotating boundary layer in the theory of singularly perturbed systems of ordinary differential equations*, Soviet Math. Dokl. **34** no. 1 (1987).

10. Orevkov V.P., *Some questions of the theory of polynomials with constructive real coefficients*, Trudy MIAN **72**. (in Russian)

11. Vorob'ev N.N. and Grigor'ev D.Yu., *Solution of polynomial inequality systems over real closed fields in subexponential time*, Zap. nauchn. sem. LOMI **174** (1988). (in Russian)

12. Pankov P.S., *The algorithm "Search of short proof for strict inequality within a bounded two-dimensional domain in integer numbers"*, State Fund of algorithms and programs 002378. (in Russian)

13. Pankov P.S., *Algorithms of proving stable statements and global optimization within a bounded domain*, 5250–84 deposited in VINITI. (in Russian)

14. Matiyasevich Yu.V., *One more computer experiment in favour of the Riemann hypothesis*, Cybernetics no. 6 (1982).

15. Pankova G.D., *Software for validating computations and its realization in the operating system OS ES*, Problems of Theoretical Cybernetics: Abstracts of reports of IV All-Union conference, Irkutsk, 1985. (in Russian)

16. Matrosov V.M., Vasil'ev S.N., Karatuev V.G., Kozlov R.I., Sumenkov E.A. and Yadykin S.A., *Algorithms for deducing theorems of the Lyapunov vector function method*, Nauka, Novosibirsk. (in Russian)

Institute for Mathematics of
the Academy of Sciences of
Republic Kyrgyzstan
Leninsky pr. 265-a
720071 Bishkek
Kyrgyzstan