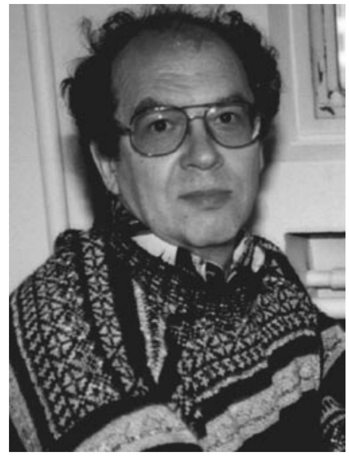

Anatol Slissenko

Anatol Slissenko is a professor of Computer Science at the University Paris 12. Previously he held the positions of Head of the Lab for Theory of Algorithms at the Institute for Informatics of the Academy of Sciences of Russia and Head of the Chair of Computer Science of the University of St. Petersburg, Russia. Prior he was a researcher at the Leningrad Division of the Steklov Institute for Mathematics and Professor at the Leningrad Polytechnical Institute. For about 20 years (1973–1993) he organised the Leningrad Seminar on Computational Complexity at Steklov Institute for Mathematics which essentially influenced the theoretical computer science research in the former Soviet Union. Researchers as D. Grigoriev, A. Chistov, N. Vorobjov Jr. and many others were educated in his seminar. Professor Slissenko graduated from the Leningrad University with a diploma in mathematics (1963); he obtained his PhD degree from Leningrad Division of Steklov Institute, and his second Russian doctorate from Steklov Institute in Moscow. Professor Slissenko was an invited speaker at many conferences, including the International Congress of Mathematicians. He is best known for his real-time string-matching and palindrome recognition algorithms. He worked also in automatic theorem-proving, recursive analysis, algorithmics and theory of computation. His current research is focussed on verification of timed systems, and the problem of the shortest path amidst semialgebraic obstacles.

Leningrad/St. Petersburg (1961–1998): From Logic to Complexity and Further

This survey is a personal recollection of the development of research on computational complexity in St. Petersburg (named Leningrad from 1924 to 1991) in the period 1961–1998. This research was born in the womb of the Leningrad school of mathematical logic, hence a considerable part of this paper is dedicated to the latter. Information on the life, education and research in the Soviet Union is also given. More general remarks on some computer science problems can be found in the concluding part. This survey has been written at a stretch and governed by a flow of (sub)consciousness.

> "A retentive memory may be a good thing, but the ability to forget is the true token of greatness", Elbert Hubbard, *The notebook*, 1927.
>
> "The facts had happened and thus, disappeared. We can at best demand their images from our memory. But our memory is out of our control. Thus we are not responsible for our recollections".[1]

The creation of the Leningrad (St. Petersburg) school of mathematical logic, which gave rise to the research in computational complexity that I am writing about, is mainly due to professor Nikolai Aleksandrovich Shanin (1919–). I was his student and started my research in his seminars. Some features of the system of research and education might be of interest because of their high efficiency in some circumstances and within certain limits. I will not go into technical details (though basic references will be given) but I will write more on human aspects that will be soon completely forgotten. More information concerning the Soviet research related to the subject of this survey can be found in [Yan59] (logic), [Min91,MMO71] (theorem-proving), [Tra87,Tra84,Sli81a] (complexity), [Sli93] (computer science), [BGG97] (decision problems).

The Origins

> "Where is the beginning of that end which terminates the beginning?" Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Translated from Russian.

Research in logic in Leningrad started after 1946 and was initiated and influenced mainly by A. A. Markov Jr. (1903-1979), a son of the famous mathematician A. A. Markov (1856–1922) who is widely known for Markov chains and various other classical results. Before the war of 1941–1945 A. A. Markov was a professor and the head of the chair of geometry at Leningrad State University (maybe, more precisely, at Leningrad National University, as it was subordinated to the Ministry of Superior Education; below it will be referred to as "University"). The famous Soviet geometer A. D. Aleksandrov was at the same chair. Just before the war the Leningrad Division of Steklov Mathematical Institute (LOMI) had been created; it played an exceptional role in the development of mathematics and not only in Leningrad. A. A. Markov has become also a part-time researcher at LOMI.

Somewhere in 1940 Markov started an educational seminar on mathematical logic just to learn it. His PhD student N. Shanin, the source of the information of this seminar, attended the seminar but he did not really participated in its work: he was doing research in general topology. The main interests of A. A. Markov,

[1] The epigraphs without references are either well known or are mine.

though rather diverse, were far from logic. He published papers on dynamic systems, differential equations, analysis, topology and even root separation. One extraordinary participant of this seminar, E. M. Livenson, was a polyglot. He knew the Bible by heart and used it to learn different languages: he took the Bible in an unknown language, after having learnt its basic grammar, and started to read and learn it. E. M. Livenson found in some reports of the London Royal Society a reference to Turing machines and gave a talk on this subject. His own research was on descriptive set theory on which he worked with L. V. Kantorovich, the future Nobel Prize winner in economy. However, at that time he himself developed an algorithm (based on a calculus with invertible rules) of inference search for the classical propositional logic (Gentzen's classical work [Gen34] was not known to him). At that seminar A. A. Markov reviewed the "Foundations of Mathematics" by Hilbert and Bernays [HB34,HB39]. The war which started in the summer of 1941, had interrupted this activity. E. M. Livenson, who lived in a suburb of Leningrad that was occupied by Germans, had disappeared during the war. The institutes of the Academy of Sciences and the University were evacuated to the East of Russia, as German troops started to besiege Leningrad, though they had never seized the city. During the war A. A. Markov was in Kazan.

Initiation of logic and complexity research of A. A. Markov Jr.

> "The parish is like the priest. But where is the cause and where is the effect?"

From 1946 A. A. Markov entirely switched to the theory of algorithms and logic, and he was more and more interested in the foundations of mathematics where he analyzed the intuitionistic critical line initiated by E. Brauer and H. Weyl. Very soon these reflections led him to constructivism (see [NS64]).

His first results on undecidability were obtained in 1946, and started to appear from 1947; in particular, the famous undecidability of the equality of words in finitely defined semi-groups dates from that time. His lectures and seminars attracted his students and collaborators into the research on logic, theory of algorithms and constructivism. Among them the most important role in the development of the Leningrad school of logic and constructivism was played by his collaborator and disciple N. Shanin who was at that time a senior staff member of LOMI, and a part-time professor at the University (for more details on his scientific biography see [MMM$^+$80,MMOS90,Kur59]).

The philosophy of intuitionism was vague. However, the logic was described precisely, and there were approaches to its interpretation (from the A. Kolmogorov's paper [Kol32] up to Kleene's realizability [Kle45]). A. A. Markov wished to develop a precise approach, taking into consideration E. Brauer and H. Weil criticism of the foundations of mathematics. This idea, quite normal for a mathematician, offered also some security from possible political accusations for dragging an "hostile bourgeois philosophy of intuitionism" into Soviet science; the word "constructivism" was itself risky. This idea has proved to be productive for the Leningrad research, independently of constructivism, because such a great scientist as A. A. Markov assured a profound and versatile knowledge of the theory of algorithms and logic. His own contribution includes Markov algorithms [Mar54,MN88] and Markov principle [Mar56,KV65] (giving a non trivial extension of intuitionistic logic within the constructive setting), not to speak about numerous excellent results that were not named after him.

A. A. Markov moved to Moscow at the end of 1955. He was the director of LOMI at that time. In Moscow he headed the chair of mathematical logic at the Faculty of Mechanics and Mathematics at Moscow State University, the highest rank university of USSR. However, by the time of his departure the foundations for further work have already been created. N. Shanin has written a profound paper on embedding operations, generalizing the results of Kolmogorov-Gödel, and some other papers related to constructivism. Moreover, he began to be interested in machine theorem proving that influenced considerably the Leningrad research in logic. Another person who is directly related to computational complexity was G. Tseitin (1936–), at that time a prodigy child who became a student of the University at the age of 16 (in 1952), but actually started to attend courses of A. A. Markov one year before. Two more known researchers, namely, I. Zaslavski (1932–) and E. Nechiporuk (1934–1970) were at the University. I. Zaslavski was a student in 1949–1954, and started to publish his papers from 1953; his first research was in constructive analysis [Zas55a,Zas55b]. Zaslavski was not accepted as PhD student (mainly because of being Jew) and worked in the Institute of Telephone Communications. He was arrested at the end of 1956 for his open protest against the Soviet invasion in Hungary, and was set free in November 1958. He was not permitted to reside in Leningrad and found a position in Erevan (Armenia) where he created a scientific school in the theory of algorithms and logic. Now he has six positions just to survive. As for Nechiporuk, he worked on the complexity of Boolean functions, closer to the research in Moscow, and after his classical results (see [Weg87]) he started a very general study of self-correcting circuits [Edi73]. He suffered from depressions that limited his interaction with people and had committed suicide while being treated in a hospital.

Among various brilliant results due to G. Tseitin, at least three are pioneering: first, an $n^2/\log^2 n$ lower bound on the complexity of Markov algorithms that was proved in 1957, secondly, compression and gap theorems for Markov algorithms proved in 1956 and mentioned in [Yan59] and, thirdly, axioms defining computational complexity and a version of the compression theorem for these axioms. The axioms were exactly the same that were later found by M. Blum [Blu67]. As it was traditional for Soviet mathematical logic this knowledge existed as folklore. The first of these results was at least mentioned in [Bar65]. As for the third one, I learnt it from G. Tseitin (before 1967; R. Freidson also remembers this); one more result on non efficiency of strong lower bounds was mentioned in my survey [Sli81a]. But now it is impossible to trace all this. When I asked G. Tseitin in April 1998 about this axiomatics, he was surprised and asked me what they are about. All these results, though well-known in Russia, had never been published, and the reason was mainly Tseitin's reluctance to write proofs. On the other hand, publishing papers in the USSR was never an easy business. Later G. Tseitin worked more in constructive (recursive) analysis where he proved his famous results on the continuity of constructive functions, and then started to move towards programming and artificial intelligence.

Education in the USSR

> "Nothing is more responsible for the good old days than a bad memory." Franklin P. Adams
>
> "At an exam a Soviet medical student is invited to describe some particular features of two skeletons shown to him. He is silent. No hints work. The examiner says: "Try to recollect what you were studying all these years!" The student exclaims: "Are they really the skeletons of Marx and Engels?!" Soviet joke.

My father, a military topographer, had a possibility to install himself in Leningrad in 1950, after more than 30 years in the service and having spent more than 20 years in expeditions in the Central Asia, Far East and Far North-East of the USSR. He had the rank of colonel, and he was a lecturer in the Military Academy of Communications in Leningrad. He retired in 1955. Such middle-class families were a typical source of university students, in particular, in mathematics. After spending a long time in military camps or small provincial towns, the life in Leningrad was a kind of paradise. After the war, highly demolished Leningrad which heroically resisted the famous 900 days besiege during the war, had a privileged status. Of course, such privileges could not solve desperate problems as the shortage of apartments. My father's family of three (or four when my grandmother was with us) had two small rooms in a four-room apartment without bathroom and hot water. That was considered as good living conditions. Other two rooms were occupied by two families with three persons each. We had to share a small kitchen with one cold water tap. Small kerosene-stoves were used to cook. But theaters, concert halls, libraries, excellent public lectures were superb sources to nourish young brains and souls, though large parts of the world and even Russian culture and science were absolutely invisible.

Schools were different from the point of view of education quality, though all of them were to follow the standard national programs supervised by the government bodies of district or regional level. Happily the school education was doubled by clubs and study groups; they were sufficiently numerous and were organized at houses of culture or pioneer houses (here the word "pioneer" refers to the Pioneers Organization formally controlled by the Communist Party but informally by nobody). My parents had found the only existing elite school with an intensive programme in English, the school No 213. The most paradoxical fact was that this school, though having been created mainly for the children of the Party nomenclature was, by that time, open to all children (via a competition). My parents hired an excellent teacher of English and after one or two years of additional lessons I passed the exams and was accepted. At school, starting from the fourth year, we had about 4-6 exams at the end of each year. The school

No 213 played a crucial role in liberating me from the communist orthodoxy, though pace was too slow.

As for mathematics, in addition to a relatively good national program at school all children had an opportunity to attend different study groups. The University study groups were open and headed by the best students of the Faculty as a kind voluntary public service (it was mandatory "to serve voluntary"). I have started in such a study group headed by V. G. Mazya, who became later a well-known mathematician in analysis (now in Sweden). In addition, I tried to read excellent books for school-children written by high-level mathematicians, for example, "Three Pearls of the Number Theory" by Khinchin. Many schools with various accelerated programmes for some disciplines like foreign languages, physics, mathematics, etc. appeared at some stage. It was harder to be a student there as the accelerated disciplines were taught as additional subjects on top of the national program.

To become a student of the University one had to pass an entrance exam, that is to go through a competition. Usually the Faculty of Mathematics and Mechanics had 3-4 candidates for one place in mathematics (there were about one hundred places for mathematics, one hundred for mechanics and astronomy). I got my baccalaureat in 1958 and became a student of the University the same year at the age of 17. That was a normal age to start. Universities offered only one type of diploma after usually 5 years of study; in some faculties, say, in medicine, the programme lasted longer. Students with good marks were paid scholarships, about 40 roubles (that was slightly less than the minimal salary) or even 60 roubles in case of highest marks. There were four marks: excellent, good, satisfactory, not satisfactory. Later, special scholarships were introduced for students with excellent marks during the first three years. I had such a scholarship that was called Lenin's scholarship; it amounted to 80 roubles. This was a sum that permitted to live in poverty. For the minimal salary one could only not die.

Universities were attractive for their liberalism and intellectual environment, and a rather free access to various lectures. Research positions in sciences or mathematics gave the freedom to work out of the Communist Party control. The extermination of disciplines like economy, philosophy and even genetic had been successfully accomplished earlier; physics and mathematics had been saved by nuclear weapons, avionics and other activities related to arms race. Surely, nuclear physics was considered incomparably superior than mathematics, and mathematical logic was treated as a marginal science in mathematics; its existence was somehow justified only by the appearance of computers. And again, nuclear and aero/hydrodynamic applications of computers were absolute priorities.

The late 50s and the early 60s were a relatively happy time of Khrustchev's era. We could see paintings of Picasso that were not exposed before. Ive Montand, a famous French chansonier, gave concerts in 1956. As a result, French became temporarily popular. He was a communist until he realized a part of the evident truth about the communism. When he had denounced communism, he was immediately officially forgotten. As well as Khrustchev after his dismissal. The next day after Khrustchev's dismissal, no Party official could answer the question "Who was Khrustchev?"

The Faculty was rich in old intelligentsia and outstanding mathematicians. Just to mention a few, one could take courses by L. V. Kantorovich who worked in various fields of mathematics and won a Nobel Prize for his pioneering contribution in mathematical methods in economy, number theory and statistics were represented by Yu. V. Linnik, geometry by A. D. Aleksandrov, algebra by D. K. Faddeyev, differential equations by V. I Smirnov and O. A. Ladyzhenskaya. Students were free to attend any course, and they were numerous. Later these opportunities disappeared, as well as some of these people of high culture and humanistic traditions. Those who came after them, though being good or excellent in research, were too exhausted by poverty and the struggle for existence, and had no access to the sources of culture available to previous generations.

As a first year student I had to start to take courses from the 1st of September according to the official rules of the Ministry. But for the Regional Committee of the Communist Party the laws written by the Communist Government were not compulsory. Thus, we went to gather potatoes in sovkhoz fields ("sovkhoz" is a state owned agricultural farm, similar to kolkhoz, but usually considered as more industrial and closer to communist forms of organization of labor). The weather was bad, the work was hard, only by hands, and as local people explained us, was useless because potatoes were to rest in the field in piles and would rot very soon. This communist absurdity was the core of the system. I gathered potatoes during the following thirty years until perestroika, and nothing changed.

We studied at the University 6 days a week, 6-8 hours a day with 10 minutes breaks every hour. No break for lunch. We spent 8 hours a week on Marxism-Leninism, one day for military preparation. I do not remember much concerning the latter, but as for the communism I learnt not only its practice but also the theory of this criminal ideology : I can say that practice corresponds to theory. In fact, this aggressive way of imposing the communist ideology on clever people had the opposite effect: it formed anti-communists with profound knowledge of all pathological destructiveness of communism.

Student seminars: free choice

> "It ain't the roads we take; it's inside of us that makes us turn out the way we do." O. Henry. *The roads we take.*

From the very beginning students had a variety of seminars where they participated as reviewers of papers that led them very quickly to open problems they could try to solve. The head of a seminar proposed interesting problems of reasonable difficulty. These seminars constituted supplementary units for first and second year students; later students had always optional seminars together with mandatory ones. Very often the results obtained by these younger students were really good and were published in journals. That was the case of Yu. Matiyasevich (1947–) who got his first results in my seminar on theory of algorithms, being a first year student. At the same time staff research seminars were also available to students. D. Grigoriev (1954–) started to participate in the seminar of complexity as a second year student, and arrived in his third year with his now classical results which will be mentioned below. By the third year a student was to chose a specialization, e. g. algebra, geometry, logic (that was at the chair of geometry), etc. and be attached to the corresponding chair. This choice was not very rigid, and later one could change the chair.

When I was a second year student N. Shanin started a course on mathematical logic with accent on proof theory. At the beginning the audience was enormous, I guess more that 200 people; at the end of the second year, and that was the duration of a non standard course, I was the only undergraduate student in the audience (there were several PhD students).

In 1959 the idea of automatic theorem proving was in the air, and publications started to appear. N. Shanin decided to study the question with his students S. Maslov (1939–1982), G. Mints(1939–) and G. Davydov (1939–) and some others who constituted a seminar on logic and theory of algorithms. Later V. Orevkov (1940–) and myself, A. Slissenko (1941–), joined the seminar, and all these people constituted a group on mathematical logic organized by N. Shanin within the Leningrad Division of Steklov Mathematical Institute (LOMI). We worked together for about 20 years.

N. Shanin's non standard idea was to develop a computer algorithm for searching *natural proofs*, firstly in the classical propositional logic. The starting point was the results of G. Gentzen and J. Herbrand. The idea of seeking a natural, human-oriented proof was not popular. As it became clear much later, it was strongly underestimated. But at that time the general belief was that, in spite of the undecidability of first order theories, the arriving computers—with power doubled every 2-3 years—would be able to prove interesting theorems. Further experiences and theoretical studies showed that the universality of these undecidable problems was destructive for general theorem proving algorithms. All the syntactic flexibility, as well as sophisticated programming solutions, used in modern theorem provers do not change the fundamental sources of their inefficiency. However, the inertia is high. I will come back to this point later.

To simplify the task of proof presentation, N. Shanin proposed to take as natural proofs the proofs in a sequent version of Gentzen's natural calculus which contains, in particular, modus ponens. But how to seek a proof? That was a problem that could not be solved by students, especially taking into consideration the goal to implement algorithms on computers.

Steklov Institute Group in Logic

> "The basic modus of Soviet logic: *A implies B, if there is no reasonable way to deduce B from A.*" Experimental fact.

Several words on the organization of theoretical research in the USSR.

Research institutes in the USSR

> "**Theory.** Supposition explaining something, especially one based on principles independent of the phenomena etc. to be explained... . [Gk ... *theōros* spectator f. *thea* spectacle]". The Concise Oxford Dictionary, Fourth Edition. 1951

The best places for research in the former Soviet Union were the institutes of the Academy of Sciences of the USSR or of the associated republics, and universities research institutes. With the collapse of the Soviet Union the Academy was reorganized, and in fact, dismembered into Academies of the Independent States. The largest part has become the Academy of Sciences of Russia. No attempts to save the best part of research had been done, and in consequence, a considerable part of researchers (and one can guess not the worst part) has left for the West. Most institutes exist by letting parts of their buildings to companies making business.

Institutes had permanent positions only for the members of the Academy, though rules were vague. Non-tenured positions were for maximum five years; after each term researchers had to be re-elected by the scientific council. Not re-election was not too rare, especially for junior staff. This system worked well on the whole even within limited resources and the incompetent interference of the Communist Party. But it could not work well in the long term without sufficient resources, strong connections with applications and international competition. One can notice that elite research institutes with very small permanent staff of outstanding scientists exist in many countries, e. g. the Institute for Advanced Studies in the USA, Max-Planck Institute in Germany, I.H.E.S. in France. In the Soviet Union the non-permanent part was larger and more stable, and it was justified by the poverty of the population. All changes were highly difficult to implement.

People having positions in research institutes of the mentioned type were not obliged to teach and could, and had to, concentrate on research. Strictly speaking, there were political limitations on the subjects of research, but starting from the 60s, they were not considerable for sciences, mathematics or computer science. As always in the history of Russia, the competent layer of researchers was very thin and fragile. The number of people involved in applied science was not only inadequately small but also too limited in resources and freedom of action.

For theoretical research the main obstacle was the absence of contacts with the West. The information flow was limited, namely, the libraries were incomplete, reproduction and publication facilities were poor, and information exchange with the West was usually interrupted. On the other hand, the publishing houses "Nauka" ("Science") and "Mir" ("World") provided a good amount of books, the first one of Soviet authors and the second one translations. The amount of available translations from English was much higher than, say, in France nowadays.

As for any visible action, everything was forbidden except things specially approved by the Communist Party Committee. The crucial role in consolidating different research areas from different institutions was played by regular seminars, usually having had their meetings once a week and headed by competent leaders. Reviewing the literature was an important component of this activity. Seminars had no funds, and the only support from host institutions was a room for meetings. Nevertheless people were invited and were eager to give talks hosted by good seminars. The leading seminars were very prestigious, and to give a lecture in such a seminar was considered a sign of recognition. For PhD and second doctorate programmes a talk at an appropriate seminar was mandatory.

In Russia, as well as in USSR, there are two scientific *degrees*: candidate of sciences (physico-mathematical, technical, biological, etc.) and doctor of sciences. Both are validated by the state Higher Certification Committee which awards diplomas. The degree of candidate more or less corresponds to PhD, though, I guess, initially the level of candidate dissertations was, on the whole, higher than that of PhD theses in the West, at least in mathematics and physics. The second degree, to which I will refer to as "second doctorate", was much harder to obtain. In mathematics the most respectable second degree was the one obtained from the Steklov Institute for Mathematics in Moscow (among people mentioned in this survey, Yu. Matiyasevich, G. Makanin and myself got such degrees), or from Moscow or Leningrad Universities. The Steklov Institute was very slow, and many excellent people like D. Grigoriev got their degrees from universities to accelerate the process. Any dissertation had to be "defended" at a Scientific Council appointed by the Higher Certification Committee. The council appoints official opponents (2 for the candidate degree, one of them with second doctorate, and 3 with second doctorate for the doctor degree) and an "external" organization that must give its view on the dissertation. The report of the external organization is to be signed by a known expert in the field and endorsed by the head of the institution or its deputy. The defense procedure is governed by rather strict formal rules, is public, and at a certain moments anyone could pose a question or express on opinion on the subject. Critical remarks and hard questions are usual. The final vote of the Council is secret, and to get the degree two thirds of votes must be positive. But that is not all. The dissertation is to pass through the Certification Committee which could ask for additional assessment and change the decision of the Council. The system worked well for a rather long time but was gradually corrupted by the Communist Party. One of the sources of corruption was represented by classified dissertations (especially of generals) and dissertations of Party functionaries and their relatives.

Besides scientific degrees there exist also scientific *titles* "dotsent" (associate professor), "professor" (full professor) for university people, and "senior scientific collaborator" for researchers. Happily one could get a professor position without the title, but in this case the salary was smaller. In the USSR people were paid not for their work but for position and title, and these had often nothing to do with the qualifications of the person occupying it. I found something similar in Europe. Young brilliant brains normally drain from such systems.

Automatic theorem proving and proof theory

> "To err is human, but to really foul things up you need a computer." Well known.

The creation in 1961 of a group on logic and automatic theorem proving in LOMI was an outstanding organizational success of N. Shanin. The first three members of the his group were G. Davydov, S. Maslov, and G. Mints. One of the obstacles to the creation of the group was the (practically official) anti-Semitism of the administration of the Steklov Mathematical Institute in Moscow headed by academician I. M. Vinogradov, called by L. S. Pontryagin "one of the two greatest mathematicians of the century" (the second was L. S. Pontryagin himself). Steklov people called I. M. Vinogradov "Brother Vanya" (in Russian it is "Uncle Vanya"). He was an anticommunist respected by communist governments. He would criticize the Soviet regime in presence of reliable people; but if someone less reliable appeared in his office he started to attack Jews. His notorious and widely known anti-Semitism was operational mainly inside the Steklov Institute in Moscow.

Uncle Vanya's anti-Semitism gave him particular advantages to avoid any participation in the campaigns of persecutions of dissident scientists. For example, he refused to sign the official letter blaming the known human rights defender academician A. D. Sakharov because he noticed a Jew name among signatories; later he refused to sign any letter using various other arguments. Among the most brilliant jokes concerning his anti-Semitism is the following one. A KGB officer comes to Uncle Vanya and draws his attention to the dissident activity of R. Shafarevich, a member of the Institute. He speaks for a long time and demands "measures" to curb this activity. Uncle Vanya interrupts him and says: "I have studied this question in the deepest way. Shafarevich is not Jew." And that was this final judgement.

Thus, N. Shanin, supported by the then Director of LOMI (who formally was a Deputy Director of I. M. Vinogradov) G. I. Petrashen, has managed to take in LOMI three persons among which one was Jew even according to his passport (G. Mints) and another one had a Jew mother (S. Maslov). Next year V. Orevkov arrived, and in 1963 it was me, and this finishes the first phase of this history. There were other people hired for programming, but they left the group after rather short terms except Alla Sochilina who stayed with us for about 20 years.

The late 50s and early 60s were a time of unlimited believe in the possibilities of computers. Any algorithm will eventually work, that was a widespread point of view.

The principal ideas of the first theorem proving algorithm for classical propositional calculus were developed by N. Shanin. In addition to various considerations to accelerate the inference search, he designed an algorithm transforming a proof of logic sequent calculus to a natural proof.

We started programming in 1963 on a computer "Ural-4" that was situated in the city Penza in the institute that developed that computer. To debug and run programs we traveled there, and the trip took about two days by train.

The programming was in code. Of course, we created some environment but basically it did not change much. In parallel with design and implementation, all members of the group continued their theoretical research either in logic or in constructive analysis, the latter being my case. The program [SDM$^+$83] has been accomplished very quickly and it was a success. Our productivity was more than 30 instructions per day, the design of algorithms included, compared to the average productivity of 2-3 instructions per day of programming only, without design. The program consisted of about 15,000 instructions, and about 30% concerning the transformer into natural proofs was written by myself.

Then the turn of predicate calculus arrived. Almost immediately S. Maslov invented his “inverse method” [Mas64]. Though finally it proved to be, in a way, equivalent to the resolution method [Rob64] that became known to us much later, Maslov’s method worked directly for arbitrary formulas and had an essential flexibility in representing strategies of inference search. Maybe it still has some advantages (for lower level complexity classes), but this question was premature at that time, and nowadays it may be too late to study it. The implementation that we had done showed results that were, in fact, excellent. The computer proved that $\sqrt{2}$ was not a rational number. But our hopes to prove new, interesting theorems had not come true. The following decades, on the whole, did not change the situation from the point of view of really interesting theorems.

This disillusionment caused by the weakness of general provers motivated the search for more efficient automatic provers. So a part of the group passed to proof theory and decidable classes, and another part (consisting of myself)—to computational complexity.

The logic seminar flourished; among participants there were V. Lifschitz (1947–), M. Gelfond (1945–), V. Kreinovich (1952–) (all of them later became professors in the USA), E. Dantsin (1951–) (now a senior researcher in LOMI), N. Kossovski (1945–) (now head of chair of computer science at the St. Petersburg University), S. Soloviev (now a senior researcher at the Institute of Informatics of the Academy of Sciences of Russia), PhD students from other republics as N. Zamov from Tatarstan (now a professor at Kazan University) and many others. The Jewish emigration of the beginning of 70s diminished slightly its rows but not too much. The core stayed intact. The hard blows were Maslov’s death in 1982 and Mints’s departure to Estonia in 1985.

From logic to computational complexity

> “Fast algorithms are too complicated to implement. Simple algorithms are too slow to run. And any program for any algorithm is erroneous.” Known to researchers with vast knowledge.

Two open problems stimulated my switch to computational complexity: first, the fact that theorem proving algorithms were unable to prove really interesting theorems, and, secondly, the fact that the constructive approach to mathematics was, clearly, practically non-constructive. Other members of the group for logic had started to analyze how to get really practical algorithms for theorem proving. The idea of natural sciences approach has appeared, but how to put it into operation having the mentality of mathematical logician? A. A. Markov, who was educated as physicist, and was considered by many as a person with a strong naturalist way of thinking, had shown two examples: to analyze complexity and semantics from the point of view understandability. As for complexity, A. A. Markov had published a paper [Mar57] on Boolean complexity already in 1957. Then in an elegant [Mar64] he used complexity considerations to prove the undecidability of some problems; that was, in fact, the method that was much later associated with Kolmogorov complexity-theoretic approach to undecidability (recall that Kolmogorov paper [Kol65] appeared only in 1965).

The second approach, that is to look at semantics, could be more productive from a practical point of view if realized in the spirit of artificial intelligence. A. A. Markov and N. Shanin continued their profound study of semantics of constructivism which interacted well with the Western research on the semantics of intuitionistic logic, e. g. [Kle60]. Much later N. Shanin declared himself as a "finitist" [Sha87]. There were no direct practical consequences of this approach to theorem proving or other domains of algorithmics, as the complexity of admissible constructions was too high. However, this research influenced the research of some PhD students on characterizations of complexity classes.

Another path was undertaken by S. Maslov though his fate was dramatic. Having obtained his second doctorate in 1972 and being well known in the field for his various results—not only in theorem proving but also in the theory of algorithms, logic (Maslov class) [BGG97]—he had not been promoted to the senior staff by the Council of Steklov Institute of Mathematics in Moscow (MIAN). I guess that the main reason was the traditional anti-Semitism of MIAN leaders, but some role was caused by Maslov's unconventional vision on problems of automation of reasoning. In his arguments he used considerations from various fields of knowledge like semiotics, psychology, linguistics that were always considered as inferior and unworthy of genuine mathematicians by the more traditional mathematicians of MIAN. He left LOMI in 1974 and was a professor and senior researcher in various institutions in Leningrad. He was prevented from going abroad, though he attended the Congress on Logic, Methodology and Philosophy of Science in Amsterdam in 1968. He was monitored by KGB because of his political views and contacts with known dissidents. His interesting ideas on using general deductive systems to model various phenomena of social developments are presented in [Mas87]; another heuristic idea of how to solve hard problems is discussed in the collection [KM97] with a preface by V. Kreinovich [Kre97]. S. Maslov had tragically died in a car accident in the summer of 1982, presumably having fallen asleep while driving. He was not only brilliant, he was a pole of interaction and activity for different people of various domains of research.

Promotion was delayed or impossible (as in the case of Maslov) for all people who entered the field of mathematical logic and theory of algorithms as students of A. A. Markov or N. Shanin. G. Mints, who is a professor of logic at Stanford University from 1991 (he hold the position held before him by Barwise and

Kreisel), simply had no practical possibility to obtain his second doctorate in the 70s though he published very actively in theorem proving, proof theory and semantics (e. g., see [MMO71,Min72b,Min72a]). The worse came when he tried to immigrate in 1979. He left LOMI not to "throw a shadow" on the institute and being prohibited to leave the country, worked as programmer in various institutions (in particular, in the Institute of Meat and Milk Industry in 1984-85) and translated books in logic. He was, in a way, saved by E. Tyugu (now a professor in Stockholm) in 1985 who invited him to Tallinn (the capital of Estonia) as a senior staff member. Their joint work had started earlier and was profitable for both. They found a fascinating representation of Tyugu's program PRIZ in terms of intuitionistic logic [MT82]. Only after perestroika, in 1989 G. Mints had received his second degree (he published by that time more than 150 papers and was well-known in the world since long time). Interestingly, he wrote on complexity as well [Min92].

V. Orevkov was highly appreciated by A. A. Markov for his clever constructive (and, thus, continuous) mapping of the circle into itself without fixed points [Ore64]. He published various papers on recursive analysis, theorem proving, proof theory, and started his research on the complexity of proofs that finally produced this well-known paper [Ore93]. By the time he got his second doctorate in 1990 he had published more that 70 papers.

Exceptionally brilliant, Yu. Matiyasevich appeared in my student seminar on the theory of algorithms in 1965 being a first year student at the University. His first presentation in the seminar was on Kolmogorov algorithms. When studying Post normal systems I posed a question on the possibility to minimize the number of rules and premises in Post normal systems for a concrete problem that I do not remember. In a very short time he proved a general theorem that one axiom and one rule with one premise is always sufficient. Later, these results constituted a part of this PhD thesis. Presumably influenced by G. Tseitin, he moved to undecidability of finitely defined semi-groups where he drastically decreased the number of relations, a fact that impressed J. Cohen at the International Congress of Mathematicians (ICM) in Moscow in 1966. Having touched the string-matching problem he devised in 1969 a real-time algorithm for the case when the text and the pattern arrive simultaneously. The known linear-time algorithm by Morris-Pratt appeared in 1970 [MP97]. Matiyasevich's algorithm was unknown in the West until I wrote about it to Galil in the mid 70s. Very soon Yu. Matiyasevich got to know other members of our logic group. S. Maslov was interested in 1966 in Hilbert's tenth problem which had become from 1967 the main point of Yu. Matiyasevich's interest. He became a PhD student in 1969, and in January 1970 Hilbert's tenth problem has been solved. Clearly, he had to get his second doctorate directly for this result. But, taking into consideration the general attitude towards our group, he firstly got his PhD degree for a part of results obtained during his early student years, and after that he got the second degree and was promoted to a senior staff position. Now Yu. Matiyasevich is the head of laboratory of mathematical logic of LOMI, and consequently the head of the seminar on mathematical logic which is now slowly recovering, though being very far from its best days. In 1997 he was elected a corresponding member of the Academy of Sciences of Russia—better late than never.

One unforgettable event was the International Congress of Mathematicians (ICM) in 1966 in Moscow. All of us gave task. The classics like S. Kleene and A. Church were among the participants. J. McCarthy visited Leningrad after the Congress, and we discussed the automatic theorem proving problem. He predicted that all of us would visit the USA: it proved to be true. V. Livshits even worked with him after his immigration at the beginning of the 70s.

Computational Complexity

> "Everyone considers as the best way the one he is inclined to follow." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Free translation from Russian.

All of us wished to find some rigorous foundations for further research on algorithms. The complexity results of G. Tseitin were known and, quite naturally, young enthusiasts, myself and R. Freidson (1942–), asked him to head a seminar on computational complexity. That happened in March of 1967. By that time I had almost finished my theorem proving activity and got my PhD degree for results in constructive analysis.

Birth of the complexity seminar

> "Sometimes the zeal overcomes the reason." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Free translation from Russian.

The research we started was aimed at lower bounds of computational complexity. G. Tseitin improved his mentioned lower bound for Markov algorithms that invert the words, from $n^2/\log^2 n$ to n^2, and intensified his attacks on propositional validity. He found that many combinatorial problems were polytime equivalent either to satisfiability or validity. His pioneering paper on lower bounds of complexity of propositional proofs [Tse68] (that was an attempt to approach $coNP \neq P$ hypothesis) appeared at that time. It was not an easy job to persuade him to write down his results, that was my main effort as editor. By 1971 G. Tseitin started to loose interest in the seminar, and mainly myself and R. Freidson supervised it.

R. Freidson generalized the classical method for finite automata to real-time algorithms [Fre70] leading to, for example, the impossibility of real-time string-matching on Turing machines of any dimension (here we speak about the hardest case, when the text arrives before the pattern).

I attacked the problem of palindrome recognition on multi-head Turing machines that was very popular at the end of the 60s, and it was conjectured that the real-time recognition of palindromes was impossible. By 1969 it was clear that the conjecture was wrong. The proof based on a direct analysis of periodicities has appeared in [Sli73] that is the longest paper in the history of computer science with a proof of one simply formulated theorem. The drastic simplification of this result by Z. Galil [Gal76], who used basic ideas of [Sli73] and the result [FP74]—this was not known to me while writing [Sli73]—made him famous. As for me, having found no support, I had not even tried to get the second doctorate for this result, though it evidently deserved it. However, I got the first prize of LOMI and was awarded a month extra salary. More essentially, I was lucky to become known in the United States. The paper [Sli73] has been translated into English twice, the first time by Bob Daley in 1974, and the second time on a regular basis (as mentioned in the reference). I received a very warm letter from Albert Meyer whose later support for our research on complexity is hard to overestimate. For several years he was sending us not only important technical reports, but entire volumes of STOC and FOCS symposia which influenced the theoretical research. As for palindrome recognition, using Galil's idea of applying the results of [FP74], I wrote (perhaps) the shortest existing proof of real-time recognizability of palindromes [Sli77].

Somewhere in 1969 I met B. Trakhtenbrot who was an influential figure in the logic and complexity community, and slightly later, L. Levin, brilliant and eccentric. Levin impressed me by his optimal algorithm for recognizing propositional tautologies. The idea is simple: we gradually apply all algorithms to the input, and having got an output, check it for a model. Any algorithm for the propositional tautology will be not better than the functioning of this algorithm up to some multiplicative constant (exponentially depending on the size of the algorithm). This result explained me the importance of a careful interpretation of mathematical results. The notion of optimal algorithm used here is more than dubious as the multiplicative constant may radically change the meaning of the result.

L. Levin presented his candidate dissertation to the anti-Semitic Novosibirsk Council though I warned him. He had been turned down, it was somewhere in 1973. Thus, he was forced to immigrate to the USA, and later he expressed thanks for this turn of events.

The complexity seminar continued to work though its head became less and less visible. Due to recollections of Dima Grigoriev, the last blow was the paper [SM73] by L. Stockmeyer and A. Meyer. G. Tseitin presented this paper himself. All the ideas were well-known to him since long time. And says Dima "he probably understood that the West was strong by its mass research, and exceptional individuals, as himself, would have no chances." And he disappeared. Somewhere at that time N. Shanin was, in a way, pushed out of the Faculty, and thus the first phase of the development of the seminar was over. Happily, Dima Grigoriev had already started to work at the seminar. He was a second year student in the winter of 1973, and he also attacked the lower bound problem.

In September of 1973, being a third year student, D. Grigoriev introduced the notion of matrix rigidity, later also introduced by L. Valiant (the latter did it for Hamming metric while D. Grigoriev used L_1-metric), and applied it to get some lower bounds, now well-known; see the recent review [KR98]. The same year, during a soirée on the occasion of passing an exam on quantum mechanics, D. Grigoriev got an idea to use the uncertainty principle in complexity, and produced Grigoriev's method on time-space trade-off [Sav98]. Using this method he proved an n^2 lower bound for the time-space product for polynomial multiplication, and an n^3 lower bound for matrix multiplication. These results were, in a way, underestimated, and I, as his supervisor, has not done special efforts for a fast publication. They appeared only in 1976 in the Proceedings of LOMI Seminars [Gri76]. Happily, Dima was sufficiently active, and very soon started to find his way to publish his results, a much more efficient approach than rely on me. He got his PhD degree in 1979 having published already many excellent results.

One "dramatic" episode happened at that time at the seminar (as I learnt later from Albert Meyer, similar episodes happened several times in the USA). One of our participants, a really good mathematician, announced a sensational result that $P \subseteq SPACE(\log^2 n)$. Neither G. Tseitin, nor D. Grigoriev nor myself noticed an error that was nontrivial, though I had some unpleasant inner feeling during the talk. We proposed to publish it in the current volume of Proceedings of Seminars of Steklov Institute edited by Yu. Matiyasevich and me, and the text had been included in the volume under preparation. In a couple of days D. Grigoriev found an error, and ran to LOMI where he found Yu. Matiyasevich holding a telegram from G. Tseitin where the latter also signaling the same gap. I had to do the unpleasant job of deleting the text from the issue.

Hard time for the complexity seminar

> "It's desperately bad now. But I am an optimist. Surely, it will become worse." Dima Grigoriev.
>
> "If you wish to be happy, be so." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Translation from Russian.

The Faculty of Mathematics and Mechanics started to move from Leningrad, N. Shanin was pushed out of the Faculty, G. Tseitin had not appeared at the seminar since 1973. Gradually I became the actual head of the seminar on complexity in 1973, and from 1975 the time has become hard. N. Kossovsky was among other participants of the old seminar. Though he did not attend this new seminar, his PhD students A. Beltiukov and S. Pakhomov did, and together with D. Grigoriev and myself we composed a very strong working group. The seminar also participated in joint meetings with the seminar in logic (we were all members of the latter). Verification of proofs during seminars was an usual activity. One outstanding case was the famous Makanin's result on the decidability of equations in free semi-groups. That was his dissertation for the second doctorate, and Yu. Matiyasevich, as a representative of LOMI, had to write one of the reports. Makanin's paper had been accepted to Izvestia of the Academy of Sciences of the USSR, that was one of the most prestigious journals in mathematics in the Soviet Union and with a high international reputation. Makanin made several two-hours presentations at the joint logic-complexity seminar, and during the his fourth talk, at the 8th hour (counted from the beginning) we found a considerable gap in his proof. He had been shocked, and left for Moscow in a state of profound depression, as his paper was in printing. But he has managed to find a patch that was added as a footnote in his paper. That was not the only case when gaps were revealed during the talks, and some of gaps were fatal for final results.

It became clearer and clearer that the problem of lower bounds was much more difficult that one could have thought at the beginning (the same applies to the $P =?NP$ problem), so one reasonable way to advance in lower bounds was to consider more limited models that RAM or Boolean circuits. Thus, the shift towards computer algebra was natural. However, other, more traditional activities went on, e. g. A. Beltuikov introduced the model [Bel79] known as Beltuikov' machine [Clo97] seeking exact descriptions of various complexity classes. Beltuikov's outstanding power was that he was able to review an entire volume of STOC or FOCS proceedings during one or two seminar meetings. S. Pakhomov also worked on complexity classes, that was regarded at that time as a possible approach to $P =?NP$ problem. After having got his PhD, he moved to neurophysiology and worked with the well-known professor N. Bekhtereva. He gave very impressing talks on some algorithmic models of perception.

After 1974 I attacked string-matching on RAMs, hoping to either find a real-time algorithm or prove its impossibility. In 1976 it was clear that a real-time algorithm can be constructed. Here it is important to stress that we deal with the problem when the text arrives before the pattern, and occurrences of the pattern must be detected in real-time while arriving from the latter. As periodicities played a crucial role in the solution, I decided to look at the possibility of finding all of them in real-time in a natural succinct form (otherwise it is impossible as the number of periodicities in a word can be quadratic). That was an erroneous decision. The real-time string-matching algorithm is two or three times simpler than the algorithm finding all periodicities [Sli81b], and though the algorithm in [Sli81b] solves in real-time many known "string-matching" problems (for example, finding maximal repetitions, the longest common substrings etc.) it is reasonable to give string-matching algorithms separately. The paper [Sli81b] is too voluminous and hard to read. An attempt of [Kos94] to simplify the construction contains no proof and repeats general considerations on approximating the suffix tree that can be found in [Sli81b]. Thus up to now, my text, admitting its awful quality of presentation, remains the only source on the subject. This result determined an invitation to the Symposium on Mathematical Foundations of Computer Science in 1979 in Czecho-Slovakia; this time my reputation was much better, and I was permitted to go. This was my first trip abroad. An important point was that Czecho-Slovakia was a "socialist" country, and the Communist Party norm was to start foreign trips with socialist countries. In fact, some people from the USA proposed to send me an invitation (that covered all the expenses, otherwise there was no point of discussion), but when I tried to estimate my chances to get permission Party officials told me something like: "Who are you to speak with you about such a trip?" And indeed, who was I?

In 1981 I received an invitation to attend a meeting in Oberwolfach and finally I was permitted to go. It was in February, and in the train in Germany I met L. Valiant who easily observed my Russian origin looking at my clothes. Unfortunately, permissions to go abroad were not stable. The most regrettable for me was the refusal of the Regional Party Committee to permit me go to a meeting on string-matching algorithms in Italy in the 80s, though Z. Galil had found money to pay all the expenses, including traveling.

The main problem of the seminar on complexity was the lack of young researchers and students; connections with the University were weak, and life was difficult. The salary was low, and the apartment problem seemed unsolvable (I succeeded to get a permission to buy a two pieces apartment in 1973 and stayed since then there with my family of four). We were wasting a lot of time to solve all these problems of basic living. My personal situation was almost desperate in 1975-1976. I was paying for the apartment and my wife, who had to stay often with our little daughter, got no salary. I remained in the junior research staff (palindromes did not help to be promoted). Happily, the logic community supported me, namely, I got a chance to translate the "Design and Analysis of Computer Algorithms" by Aho-Hopcroft-Ullman (with Yu. Matyasevich as editor); then the tough policy of Steklov Institute was weakened, and in 1977 I was promoted to a senior position before formally getting the second degree. There were other forms of support, some opportunities to teach at the Electrotechnical Institute (arranged by R. Freidson who was an associate professor there).

But the research in complexity remained productive. In addition to the results mentioned above I can add the result of D. Grigoriev concerning the relation between real-time calculations on Turing machines of higher dimensions and Kolmogorov algorithms [Gri77] that permitted to fix an imprecision in the paper [Hen66] that was unnoticed since its publication in 1966 and its Russian translation in 1970.

Towards recovery

> "The zeal overcomes everything." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Translated from Russian.

But we had opportunities to move around the country. The community of people doing algorithmics, complexity and logic was not numerous, personal contacts were rather all-embracing. However, joint research with people living in other cities was very difficult. In the 70s people from abroad could be invited by the Academy of Sciences, and we had talks, for example, by G. Kreisel, A. Tarski who were invited due to the efforts of G. Mints and N. Shanin. G. Kreisel, who stayed in Leningrad for a rather long time, impressed me by his vast knowledge in various fields of science and culture. The visit of A. Tarski was very short, I remember that he spoke Russian and was remarkably clear in his presentation.

The external signs of improvement of the state of complexity in the USSR are associated in my memory with the travel to MFCS'79. There I met among many other well-known researchers, J. Hartmanis and K. Mehlhorn. This year 1979 was fruitful for meeting with people. In September we had an International Symposium at Urgench, Uzbekistan, dedicated to al-Khwarezmi (al-Khuwārizmi) who was born in the region. The symposium was organized by the late A. Ershov and D. Knuth, and was attended by numerous computer scientists from the West. In the proceedings [EK81] one can find historical and conceptual papers and photos of many people (captions of Buda and Barzdin must be interchanged), in particular, of some people mentioned in this paper. On their way to Urgench, V. Strassen and E. Specker visited Leningrad before the symposium and we met them in LOMI. All these meetings gave more possibilities to be invited to the West.

On the whole, foreign visitors remained rare and were viewed like Martians. Their visits in the country were not always smooth though they were permanently accompanied by their Soviet colleagues. One curious case happened in the same 1979 with J. Hartmanis. In the summer of 1979, after having visited his motherland Latvia, he decided to make a short stop in Leningrad on his way to one of Scandinavian countries. His Soviet visa expired the day of his arrival. I had some family problems, and asked Dima Grigoriev to take care of him in what concerns his departure. But J. Hartmanis missed his plane and got only a ticket for the next day. When Dima tried to install him in hotels, he got everywhere refusals because of his visa: from the midnight his stay in the Soviet Union became illegal. Thus, they came back to the airport that had a special room for foreigners, and Dima requested the frontier guard on duty whether J. Hartmanis will be permitted to leave tomorrow if he slept somewhere in the city. The guard said that he personally could do it, but tomorrow there would be another guy whose behaviour could not be predicted. To avoid risks, J. Hartmanis was to sleep on a bench at the airport under the continuous supervision of guards. He said later that Dima saved him.

Urgench symposium produced my joint paper with G. Adel'son-Vel'ski [AVS81]. It concerned different approaches to solve NP-hard problems. Among others we mentioned the method developed by S. Maslov. The method [KM97] concerned the propositional satisfiability and was based on the philosophy of 'free choice'. Technically, the main ingredient was a kind of gradient method, but the general vision was wider. The technical part, clearly explained in [Fre96], is the following. Consider a CNF-formula F in n variables $a_1, \ldots, a_n$. As usually, we call variables or their negations *literals*. With every literal a of F we associate a non-negative number $\xi(a)$ called the *defference* of a. The vector $\xi = \langle \xi(a_1), \ldots, \xi(a_n), \xi(\bar{a}_1), \ldots, \xi(\bar{a}_n) \rangle$ is called an *obstacle*. An obstacle ξ defines a Boolean vector $X = \langle x_1, \ldots, x_n \rangle$ if

$$(x_i = 1) \Rightarrow (\xi(a_i) = 0),\ (x_i = 0) \Rightarrow (\xi(\bar{a}_i) = 0),\ \ i = 1, \ldots, n.$$

An obstacle ξ is said to be *correct* if it defines a unique Boolean vector. Let F be of the form $\bigwedge_k D_k$, where D_k are clauses. An *iterative method* for F is given by an operator $K_{R,L}$ of the type $R_+^{2n} \to R_+^{2n}$ which is defined by $2n$ formulas of the form

$$\xi'(a) = R \cdot \xi(a) + L \cdot \sum_{\bar{a} \in D_k} \min_{b \in D_k,\, b \neq \bar{a}} \xi(b). \tag{1}$$

Here a, b are literals from F, and R, L are non-negative constants. The operator $K_{R,L}$ is a piecewise linear continuous homogeneous operator. S. Maslov proved [Mas81,Mas83] that for any K and R the space of obstacles defining the satisfiable Boolean vector for F is an eigenspace of $K_{R,L}$, and the iterations of $K_{R,L}$ converge to a model of satisfiable Tseitin's formulas [Tse68] and 2-CNF-formulas. It follows from the eigenspace property that seeking a model can be reduced to finding linear eigenspaces of $K_{R,L}$.

After Maslov's death in 1982, R. Freidson organized a seminar that invested a considerable effort in analyzing Maslov's method. The seminar worked until 1991 at Leningrad Electrotechnical Institute and gave a good possibility for young researchers, including students, interested in algorithmics of hard problems to work together. In particular, some participants of the logic seminar were there, namely, E. Dantsin, G. Davydov and V. Kreinovich, mentioned above. The seminar had a good reputation, and many known researchers gave talks there.

Grandeur and Decadence

> "Pride goes before destruction, and an haughty spirit before a fall." Proverbs XVI, 18.

In the fall of 1980 I got at last my second doctorate from the Steklov Institute for Mathematics in Moscow for the results on real-time algorithms. This fact was also a tacit recognition of the importance of complexity and algorithmics research by the Academy of Sciences. This action was supported by L. Faddeev, the Director of LOMI, who was elected to the Academy some years ago and was becoming a more and more influential figure at the Department of Mathematics; I guess that his support was essential. There was a minor filth from O. Lupanov as the Dean of the Faculty of Mechanics and Mathematics of the Moscow University. The Faculty had been chosen by the Council for the external report on the dissertation. This paper was signed by A. Kolmogorov. But to be valid this paper had to be endorsed by the Dean, and this endorsement was always automatic especially if signed by a scientist of the caliber of A. Kolmogorov. But O. Lupanov refused to do it, and disappeared. And it was on the eve of the meeting of the Scientific Council where I had to present the dissertation. Happily A. Semenov found a deputy dean who endorsed the paper without discussion.

An official state certificate for my degree arrived very soon, and I could satisfy the bureaucratic demands as professor and organizer of conferences. The same year, with support of LOMI and together with D. Grigoriev, we organized the first Soviet Workshop in Computational Complexity in Leningrad. It was attended by classics like G. Adel'son-Vel'ski (one of the two authors of AVL-trees) and young researchers like L. Khachian—who had already published his polytime algorithm for linear programming. L. Babai was an illegal participant (to make him legal we had to obtain the status of an international workshop which was much harder). He was experienced in illegal visits to Leningrad as he came there before (from Moscow) without official permission. His visit was productive for the graph isomorphism problem, and determined the paper [BGM82]—this was unusual for our practice as, at that time, D. Grigoriev never met his co-author D. Mount. An instructive publication [GS82] written by some participants of this workshop which appeared rather quickly played an essential role in the development of complexity research in the Soviet Union. We had more workshops, in 1983 and 1985; the 1983 one was in Grodno (Belorussia) and gathered together a large amount of researchers. An exceptionally brilliant A. Razborov was among the participants.

In 1981 V. Strassen proposed me as a member of the Panel for Mathematical Aspects of Computer Science of the International Congress of Mathematicians to be held in 1982 in Warsaw (actually, it took place in 1983 because of the political situation in Poland, and the threat of a Soviet invasion). Such a panel consists of about 9 members representing world-wide the field and serves as a consulting body on invited speakers for the Executive Committee that makes the final decision. Now the role of panels is higher than at that time. In the Soviet Union all interaction with ICM was via the National Committee headed by the Director the Steklov Mathematical Institute in Moscow who was considered by the officials as the Chief Mathematician of the USSR. (This structure and mentality were universal, there was a Chief Composer, a Chief Writer etc.) Thus I had to ask permission from I. M. Vinogradov to participate in the Panel. However, first I wrote to the Head of the Panel, that was R. Karp, that I was ready to serve, and then sent a letter to Brother Vanya demanding permission. There had been no answer. On the other hand, this invitation to the Panel, the high appreciation of my results by A. Kolmogorov and the support of L. Faddeev led to the invitation as a 45-minute speaker of the Section of Mathematical Logic of ICM at Warsaw.

As a Panel member I was rather efficient as I knew the situation well, and most part of speakers proposed by myself were accepted. I was also a Panel member for the next ICM (1986, Berkley) for which I proposed as 45-minute section invited speakers D. Grigoriev and R. Krichevsky, and both were accepted; R. Krichevsky was not permitted to go. He was at the Institute of Mathematics of the Siberian Division of the Academy of Sciences, his invitation was a surprise to officials, but from their point of view he had a defect—he was Jew. But other reasons could have been considered; for example, A. Razborov was not permitted to attend the same ICM as an invited section speaker because of some groundless revenge of V. Yablonsky's group that was executed by O. Lupanov as the Dean of the Faculty at Moscow University where A. Razborov was a PhD student. The Dean refused to sign some standard paper concerning A. Razborov. By now all has gone, A. Razborov, who had won a prestigious Nevanlinna Prize (an analogue of Fields Medal) of the International Union of Mathematicians in 1990, is famous all over the world, except maybe France, and Yablonsky people are happy to collaborate with the National French Institute INRIA. By some reason, that I do not know exactly, I was also in the Panel for Mathematical Logic for the ICM of 1990, but there I could not be as efficient as at the Computer Science Section.

Booming of complexity and laboratory for theory of algorithms

"The higher flight — the deeper fall."

In the winter of 1982 L. Faddeev proposed me to organize a laboratory in the Leningrad Institute of Informatics of the Academy of Sciences of the USSR that was created not long ago before and was thought to become the center of computer science research in Leningrad. If I could foresee the perestroika, I would have refused. But the communist regime seemed eternal, and as the head of a lab I could got a 20% increase in salary and a possibility to promote the complexity research in Leningrad. I was always poor, and for a very long time was the world poorest researcher in theoretical computer science for my or higher scientific level. Now maybe I share this title with Yu. Matiyasevich and A. Razborov, but if we take into consideration that I have two children, Yu. Matiyasevich one and A. Razborov no one for the moment, and other living circumstances, I may still hold the title.

The director of that institute was a professor from a military academy who retired in the rank of colonel, and started as a head of computer center of the well-known Physico-Technical Institute of the Academy of Sciences of the USSR. This Center constituted the core of the Institute. The starting activity of the Institute for Informatics (which changed its name several times) was to supply computer resources to the numerous institutes of the Academy of Sciences in Leningrad. It was rather successfully until the invasion of personal computers. But the ambitious (that was good) director wished to make career in the Academy by any means (that was not good). He decided to rely on the support of the Regional Party Committee and not on the quality of research. The style of the Party can be diagnosed as a maniacal syndrome, groundless promises to solve any problem in an incredibly short time. Even to build a supercomputer that will surpass all the existing by the end of the year.

Nevertheless, I moved there, and my first collaborators were A. Chistov (1954–) and S. Evdokimov (1950–), several months later S. Baranov (1950–). The latter was a participant of the initial seminar on complexity, and then switched on programming and got his PhD degree for compiler construction. It seemed quite natural to unite the efforts of people from algorithmics, computer algebra and programming to make a system of symbolic computation for personal computers more advanced then the existing systems that were available, some of them, like SAC-2 of G. Collins and R. Loos, even as source. One way to program it was to use the Forth language perfectly handed by S. Baranov. Yu. Matiyasevich who was doing some computer aided research in number theory was also ready to participate. All we needed were three personal computers and a couple of young programmers. Yu. Matiyasevich and I had written a proposal that was personally handled to the Chairman of the State Committee on

Science and Technology academician G. Marchuk, who later became the President of the Academy of Sciences of the USSR. I have an impression that he did not understand what it was about, and we got no support. The favorable moment has been lost. An attempt to use a Soviet made version of an IBM 360 series computer revealed an error in hardware (that was found by A. Chistov) at a rare moment when the computer functioned. Normally it was out of work. Later S. Baranov had done a direct Forth implementation of SAC-2 system that showed excellent results on small computers, but small computers were not the main trend of software industry — the Moore law governed the market of computers. For S. Baranov it was profitable as this work finally permitted him to get his second doctorate; he become a professor and even get the title of professor. Besides that he headed some Motorola lab in St. Petersburg.

A. Chistov and D. Grigoriev concentrated on computer algebra. In 1982 the fundamental paper [LLL82] has appeared and I proposed them to study it and to look at the case of several variables. Here we were in time. That gave rise to now well-known results of these authors on factorization of polynomials and search of connected components. At the beginning of this activity an unpleasant accident happened. In the first joint preprint on the multivariate case they announced a fast algorithm of factorization for the case of non-separable fields. During their presentation at the complexity seminar I expressed doubts in the validity of this result, but they made a reference to a theorem of Hilbert that implied the result. I could not overcome Hilbert. The minor detail was that this theorem of Hilbert was invalid, and that was known but not to them. So their debut was not quite smooth. Later they were 45-minutes invited speakers at the ICMs in 1986 at Berkeley (D. Grigoriev) and 1990 at Kyoto (A. Chistov).

From 1982 the seminar on complexity started to flourish. The worst was over, new people appeared even in 1979, like N. Vorobjov Jr. (1967–) in 1979 and I. Ponomarenko (1957–) in 1981. Later they joined LOMI when D. Grigoriev became the head of laboratory for algorithmic methods in 1988 (now headed by A. Vershik under some other name). Then came D. Burago (1964–) in 1986, A. Burago (1968–) in 1989, S. Fomin (1958–) in 1991 who were members of my laboratory, and people from other places, namely, A. Barvinok (1963–), D. Ugolev. The results of that time are numerous, of high level and many of them are well-known. They gave better or much better complexity bounds for many problems in computer algebra, in particular, for the factorization of algebraic varieties over algebraically closed fields (A. Chistov, D. Grigoriev [CG82,CG83]), deciding the theory of algebraically closed fields (D. Grigoriev [Gri86]), finding real solutions of polynomial equations (D. Grigoriev, N .Vorobjov [GVJ85]), deciding Tarski algebra (D. Grigoriev [Gri88]), similar problems in differential algebra (D. Grigoriev [Gri89]), consistency of systems of polynomial in exponent inequalities (H. Vorobjov [VJ88]), polytime subclasses of graph isomorphism (I. Ponomarenko [Pon92]), factoring polynomials over finite fields (S. Evdokimov [Evd88]), counting integer points in convex polyhedral and other applications of statistical sums to algorithmics (A. Barvinok [Bar92]), lower bounds for pointer machines (D. Burago [Bur92]), etc. These results constituted several volumes of “Zapiski nauchnikh Seminarov LOMI. Series: Theory of Computational Complexity” edited at the beginning by D. Grigoriev and myself, and later by D. Grigoriev alone. They are all translated into English either as issues of *J. of Soviet Mathematics* or *J. of Mathematical Sciences.*

At the same time people from pure mathematics like D. Burago and S. Fomin continued to work mainly in their particular fields. D. Burago later proved the famous Hopf conjecture (with S. Ivanov) and S. Fomin had a good opportunity to work in combinatorics where he is now well-known.

At the beginning of the 80s I had got two results that I like. The first of them says that for any class of graphs determined by a context-free graph grammar of a certain type the travelling salesman problem can be solved in polytime [Sli82]. This result had been noticed with some enthusiasm, as it gave a general tool of describing polytime subclasses of hard problems, the subject of my permanent interest. However, no essential generalizations have been found, though it contributed to the theory of graph grammars. In fact, this property is similar to the bounded tree-width of Robertson-Seymour which neither have been generalized to get interesting polytime classes of hard problems.

The second result consists of a system of notions to evaluate the quality of knowledge representation. It has some interesting applied consequences and leads to the thesis *“The development of knowledge tends to minimize the entropy of its representation”*. This thesis was not explicitly formulated in [Sli91], thus, I give some ideas here. First, we introduce a general notion of inference of logic formulas (without loss of generality we may consider the first order syntax). Such an inference is determined by a system S of inference rules, each of them being treated as an algorithm transforming proofs, that are lists of formulas labeled as assumptions or conclusions. This general notion of inference defines the relative complexity of a set of formulas Φ with respect to a set of formulas (assumptions) Γ as the shortest inference of all formulas of Φ from Γ. Denote this complexity by $d_S(\Phi|\Gamma)$. Given two proof systems S and V and a natural number ξ we define the ξ-entropy $H_S(\Phi|V,\xi)$ of a set of formulas Φ as the minimum of sizes of proof systems U that are consistent with S and such that $d_{V\cup U}(F) \leq \xi$ for all $F \in \Phi$. The non relative ξ-entropy of Φ with respect to S is defined as $H_S(\Phi,\xi) = H_S(\Phi|\emptyset,\xi)$. This is an analogue of ε-entropy of metric spaces. The system S is a way to represent the knowledge given by Φ. Each domain of knowledge has its favourite range of ξ, that is of “acceptable” lengths of proofs. People of this field do their best to minimize the size of the representation S to justify all “interesting” consequences Φ by reasonably short proofs. In other words, they seek an U mentioned above and replace the initial S by U. One practical consequence is that to construct an efficient proof search computer system one have to base it on user friendly tools of manipulation of knowledge and “almost on-line” strategies. My last Russian PhD student V. Tarasov [Tar96] had implemented this idea for symbolic search of limits, and the results were very promising.

The complexity seminar had no participants from the University. Its stable core was represented by the Institute for Informatics, LOMI and the Institute of Evolutionary Physiology and Biochemistry of the Academy of Sciences of the USSR. The Laboratory of the Physiology of Child gave shelter to A. Barvinok who has the warmest feelings about this laboratory. Another member, the most unusual for the seminar was D. Ugolev, a researcher on the physiology and quality of food. He has a non-mathematical type of mind, but nevertheless he obtained several results concerning algorithmic models, e. g. [USP93], including some complexity estimations. He had many visitors both from the Soviet Union and from abroad. Our frequent speaker was A. Razborov.

Formal promotion also went on smoothly, people got their first and second doctorates in time. Traveling abroad was feasible but for short terms and very uncertain.

Theory of complexity versus computer science

> "One of the greatest sins is to work too much". From an interview of the Director of the Bank "Société Générale" (France), about 1996.

> "One of the symptoms of approaching nervous breakdown is the belief that one's work is terribly important. If I were a medical man, I should prescribe a holiday to any patient who considered his work important." Bertrand Russell, *The Autobiography of Bertrand Russell*, Vol. 2, 1968.

In 1981 I was invited as a part-time professor of the chair of computational mathematics of the Faculty of Physics and Mechanics of the Leningrad Polytechnical Institute. The Faculty had long standing traditions in applied nuclear physics and optimal control. The chair was headed by Professor V. Troitsky who wished to make the computer science education more apt to current demands. So I initiated some reforms introducing or improving courses on basic theory, on networks and distributed algorithms, operating systems and data bases. The attitude towards me was very favorable, and my activity was well accepted by colleagues and Faculty. I was there from 1981 until 1987. This experience was new and interesting, as students were engineering oriented and were interested in other type of research problems than more mathematically oriented people. But we were blocked by the lack of computers.

Somewhere in 1984 the Regional Party Committee, which was the highest and absolute local power, had all of a sudden realized a dangerous lack in technology with respect to the West. The decision was not original. They decided to announce a program that would get rid of the back-log in five years. The programme was called "Intensification-90". It was clear from the beginning that the programme will be on the whole reduced to declarations and demonstrations, but all researchers in computer science were pressed to participate as automation was one of the corner stones of the programme. Some reasonable actions to educate people or improve the education had been done. The programme was considered as terribly important. Tons of methodical papers had been written by the people from the Institute for Informatics. One of our fervent activists had got infarct (now he lives in the USA).

People from industry proposed me to write a curriculum for computer science. I started this work that was supported by G. Tseitin and S. Lavrov (1923–)

who headed the chair of programming at the University and was a known researcher and practitioner in programming. It gave [LST85]. The curriculum was too idealistic and too big to be implemented, but it gave a good point to discuss the situation. It was on the whole supported by A. Ershov, the most dynamic figure in Soviet programming, who organized a public discussion in Moscow. The public reaction was positive; definitely negative was only a representative of the Ministry of the Superior Education who was clearly irritated by the fact that such a programme came not from the Ministry. But all he could show was his definite incompetence in the subject. The programme was read by people responsible for computer science education in the USSR, they criticized, but used it.

Later, in 1987, I was invited to head the chair of computer science at the University, that I accepted and started to function in 1988. With some efforts and support from the Faculty, computer science was separated in an independent discipline with 250 students. I modernized the curriculum, though it was hard to find people to teach such topics as distributed computations and parallelism. The first one was taught by Yu. Matiyasevich, the second one by M. Gordin who worked in probability and later joined LOMI. All that stopped with my departure to France.

Though my teaching and reforming of the educational curriculum were time consuming, they were not useless. My organizational work in the Institute of Informatics implied more dramatic consequences for me. I had no time to continue my research in theory, and what was worse, I had no time to write papers on applied topics where I had done a lot during 1983–1990. The activity gave rise to new laboratories, in technology of programming, signal processing and artificial intelligence, but nothing gave any profit to me. My living conditions remained bad. The administration of the Institute for Informatics actively and explicitly did not like me. In 1990 the colonel director was replace by major-general from the same military academy—the progress took place.

As for more applied aspects of computer science the work usually was blocked because of lack of computers. It was not a problem of money. The Party created enormous and useless institutes with thousands of people. They wasted more than 3 billion roubles (about $600 million if we take the black market exchange rate of dollar) on the absurd programme "Intensification-90", but to support our advanced applied research with 2-3 PCs there were no money. We have done prototypes that showed good results, and got many promises to support that were never realized. Nobody was interested in real progress. It was clear that the system was dead. And it had fallen down instantaneously with Gorbachev.

Some people (not I) had hopes about an improving computer science research when in 1983 the Department of Informatics, Computing Machinery and Automation was created in the Academy of Sciences of the USSR. For me it was clear that the train has gone away. The computing machinery has been destroyed by the stupid Party decision to copy IBM 360 series that was clearly impossible, and had proved to be impossible. The people related to automation, who were elected to the Department, were mostly very far from research, they were from defense industry. Computer science was represented by veteran programmers, people doing numerical methods and Party functionaries. The Party leading role was personified in too many members of that department. One of them, M. L. Aleksandrov, from Leningrad, had been elected as corresponding member. According to the definition of the position of corresponding member, he had to obtain scientific achievements of first-rate importance. His personality was advertised in the most respectable central newspapers like "Izvestia" which published a whole page article on his outstanding qualities. As for his scientific results, I doubt that one can find any traces, though he knew the word "Fortran". After perestroika he made some money by selling computers, then he had stolen one million German marks in cash from a too credulous West German company, and disappeared. People say that Interpol is looking after him since that time. Really outstanding result! The department of informatics must be proud!

Agony and exodus

> "We wished to do it better. But, as always, it turned out for the worse." Victor Chernomyrdin, Russian ex-prime-minister, on the economic reforms, about 1996.

After 1989 the seminar was very strong but the level of living was going down. Communications were becoming better, though the mail was slow and monitored, and the e-mail was of low capacity and unreliable. The perestroika lifted the "iron curtain", but the power inside it continued to be in the hands of communist nomenclature united with more traditional criminals. The nomenclature explicitly switched on making money. The USSR collapsed. The situation in former Soviet republics became bad, even awful. Armenia was without electricity, heating and normal food for about four years. A part of Soviet research had been saved mainly by Soros Foundation with its highly efficient individual support with minimal formalities. Mathematicians got some support from the American Mathematical Society. Later the Western Europe also contributed to this and happily continues to do it. Not long ago the Russian Parliament (Duma)—which is dominated by communists and which did nothing for Russian science (professor's salary stays at about $90 per month)—accused Soros for distroying Russian Science by buying the brains. Ridiculous and insulting.

In 1990 the situation became simply bad, there were food shortages. On the other hand, traveling abroad became almost free. Nevertheless I tried to do research, and an invitation to Buenos-Aires arranged by J. Heintz resulted in a paper on shortest paths amidst semi-algebraic obstacles in the plane. We had found that in that context one can do things in polytime [HKSS91] as compared with higher dimensions where the problem is at least NP-hard.

During that time of permanent stress, the necessity to earn money to support the family had completely exhausted me. My health started to worsen, the brain was paralyzed by the hopeless situation. I was not an exception, the number of suicides and sudden deaths went up. I started to try to find a position somewhere abroad, but in vain. Happily somewhere in 1990 I met Michel de Rougemont who was in St. Petersburg. He invited me to the University Paris-11 in 1991, and then helped me to get a French habilitation as professor from the French Ministry of Education. After some time spent at the University of Poitiers, I obtained a professor position at the University Paris 12. The adaptation was easy. In Poitiers and Paris 12 the environment was friendly and cooperative. There were no essential problems of adaptation. But it took about three years to restore my capacity to think. I was strongly supported by members of my seminar, in particular, D. Burago, and also by my French colleagues.

Many of the mentioned people are scattered all over the world, mainly in the USA: A. Barvinok is at University of Michigan, Ann Arbor, A. Burago at Microsoft, Seattle, D. Burago and D. Grigoriev at Pennsylvania State University, S. Fomin at M.I.T., A. Slissenko at University Paris 12, France, N. Vorobjov, at University of Bath, England, M. Gelfond and V. Kreinovich at University of Texas at El Paso, V. Livschits at University of Texas, Austin, G. Mints at Stanford University.

On the current situation in Russia

> "Blessed is he who expects no gratitude, for he shall not be disappointed".

The state of the research in Russia is desperate. Those who have no permanent or semi-permanent positions in the West and continue to do research are supported by invitations to the West, different Western programs, or are earning money out of research. Russian programmes of support are miserable. For example, G. Tseitin, whose 60s anniversary was marked only by forcing him to retire, worked as programmer in a bank, and now has several contracts with Motorola in St. Petersburg. Nevertheless there are PhD students at LOMI, some of them coming from my last student seminar.

Concluding Remarks

> "...
> Et je m'en vais
> Au vent mauvais
> Qui m'emporte
> Deçà, delà,
> Pareil à la
> Feuille morte".
> P. Verlain, *Chanson d'automne*

On education and research systems

> "Only in the State Service one perceives the Truth." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Free translation from Russian.

In the Soviet system of research and education there were some strong points that deserve to be studied. They concern mainly activities relevant to research. First, the system of school education. Numerous study groups and specialized schools with intensified teaching of selected disciplines give school-children an important freedom of choice to realize their inclinations without missing the standard national minimum. Various olympiads and competitions add some vigor to these specializations. In the university system a reasonable premise is the fixed number of places in universities assured by the State, positions that are to be won via competitions (surely, the system was always more or less corrupted). There are not permanent positions, neither in education nor in research. This permits to get rid of people who do not keep their promises.

The university education and research system was not efficient in the long term because of its centralization and lack of resources from industry. Nevertheless, the system was less centralized than, say, in France, and gave to universities and research institutes enough power to assure high efficiency—at least in theory. The basic principle that a good research in many fields (mathematics, theoretical physics, computer science, etc.) is done by strong individuals or small strong groups of 2-3 persons was partially satisfied by the system. The weak point was the absence of diverse and competitive sources of direct support of research. The latter point is strong in the USA where any researcher can apply to NSF grants directly and where the industry thinks competitively and invests in research. These incentives were absent in the USSR and are absent, in France, and consequences are evident. This defect is aggravated in all West European countries by protectionism. An USA university can invite a brilliant foreigner directly on a permanent position. In Europe this is not the case. E. g. in France everyone must go through the procedure defined by the Ministry (whose essential activity is to change every year the dates and minor bureaucratic procedures, informing the public about all these changes in the last moment). In addition to protectionism, one ought to face the local protectionism which does its best to avoid brilliant people in order not to worry local people incapable to compete at an international level. An international rating of researchers and research groups working in one particular subject, as in chess, could be an important indicator. Why not take it into consideration?

On the notion of algorithm and computational problem

> "Nobody can embrace non-embraceable." Koz'ma Prutkov, *Fruits of Meditation*, 1854-1860. Free translation from Russian.
>
> "The number of posed problems, as well as of obtained results, goes to infinity. Thus, the value of an average one goes to zero." Slissenko's Law.

The failure to get non trivial lower bounds for concrete problems for general enough notions of algorithms (RAM, Boolean circuit) leads to a conjecture that the notions of algorithm and problem are too wide. If we compare any diagonal construction (in a way, all of them are similar) and any algorithm that is of practical importance we can easily see that their computations have completely different structures. In diagonal constructions no "geometry" is visible: they are highly "discontinuous". In practical algorithms, on the contrary, one can intuitively feel something like piecewisely smooth geometry. Such feelings have not been formalized until now, though algebraic decision trees may give some analogy. For the latter there are non trivial lower bounds. If one limits oneself to algorithms whose computations are "piecewise smooth" one can hope to get sufficiently persuasive lower bounds, though not for all possible algorithms, but for algorithms that we can really construct. That is as in mathematics, the general notion of function is not productive, even that of continuous function is too general. Most part of mathematical theories deal with sufficiently smooth operators and varieties. In case of algorithms the "smoothness" is to be understood rather largely, to include, for example, finite automata. To go on further in this direction one may try to look at sets of computations of different algorithms solving the same problem trying to explain their different efficiencies in terms of the structure of their sets of computations. This kind of work, which is in the spirit of natural science, may help.

There is another general question related to the improvement of the value of theory. If we look at known hard problems one can notice that they are over-generalized. But the situation is not too straightforward. Sometimes, as in cryptography, we seek really hard problems with some particular properties. These problems may be of any nature, in particular diagonal constructions are not prohibited (though for the moment they are not productive). Let us consider problems that arise from an activity where we do our best to economize efforts and resources. As an example, compare formulas describing routine properties concerning program specifications, say of timed systems, and formulas used in the proof of undecidability of the corresponding logic. They are quite different *semantically*, that is, the set of models of specification formulas has many structural restrictions that sometimes can be formulated rigorously and can imply decidability. One can conjecture that a more profound analysis of such restrictions may lead even to feasibility of the validity.

This situation of simplicity of concrete instances is more clear for Boolean functions. The known concrete Boolean functions are not as complicated as a random Boolean function. Why we never arrive at really hard instances from natural problems? The philosophical conjecture is that instances are generated on the basis of many laws of nature that impose some smoothness in structure; however, this smoothness is in the semantics and is not visible on the level of the syntax.

Some time ago strong efforts could have noticed in attempts to prove the logical independence of, say $P \neq NP$ conjecture (in the sense that neither it nor its negation is provable in arithmetic). Such a result may be of purely mathematical interest, but not of computer science interest. The thesis is that any "computationally" reasonable problem can be and must be expressible in the form $\forall W M(W)$, where W is a word over some alphabet, and $M(W)$ is a formula with bounded quantifiers built from easily decidable predicates. For such formulas logical independence implies its validity, so is not of much interest for computer science. It is not always the case with known problems, but why $P \neq NP$ conjecture is well formulated? Let's look at it.

Remarks on logical variations of $\boldsymbol{P}$ vs $\boldsymbol{NP}$

> "An open problem, however important it seemed at its birth, finally grows old and dies."

Here are some remarks on the logical form of SAT $\notin \boldsymbol{P}$. For formulas of the form $\forall X F(X)$, where $F(X)$ is bounded quantifier, independence from formal arithmetic implies its validity: if $\forall X F(X)$ is not valid, then for some X_0 the formula $\neg F(X_0)$ must be valid, and arithmetic is complete with respect to quantifier bounded closed formulas. Thus $\exists X \neg F(X)$ is provable that contradicts to the independence.

Consider SAT based version of $\boldsymbol{P} \neq \boldsymbol{NP}$:

$$\forall \alpha(\alpha \text{ is an algorithm recognizing SAT} \rightarrow \text{time complexity of } \alpha \tag{2}$$

$$\text{is superpolynomial}) \tag{3}$$

To fix some notation rewrite it as

$$\forall \alpha(C(\alpha) \rightarrow L(\alpha)), \tag{4}$$

or

$$\forall \alpha(\forall x C'(\alpha, x) \rightarrow \forall k \exists y L'(\alpha, k, y)) \tag{5}$$

where

- $C(\alpha) =_{df} \forall x C'(\alpha, x)$,
- $\forall x C'(\alpha, x) =_{df} \forall x \exists m \exists v (T(\alpha, x, v, m) \,\&\, (v = 0 \leftrightarrow x \in SAT))$,
- T is the Kleene predicate

$$T(\alpha, x, v, m) \leftrightarrow \text{"}\alpha \text{ finishes its work on } x \text{ after exactly } m \text{ steps and}$$

$$\text{outputs } v\text{"},$$

- $L(\alpha) =_{df} \forall k \exists y L'(\alpha, y, k)$,
- $\forall k \exists y L'(\alpha, k, y) =_{df} \forall k \exists y (time_\alpha(y) > |y|^k)$,
- $time_\alpha(y)$ is time complexity of α for argument y.

Clearly, the predicate T is polytime, and the existential quantifiers in $C'(\alpha, x)$ can be bounded: $\exists m \leq 2^{\mathcal{O}(|x|)}$ $\exists v \in \{0, 1\}$; the predicate $time_\alpha(y) > |y|^k$ is polytime; the formula $x \in SAT$ is bounded quantifier.

Thus all unbounded quantifiers are explicitly given in the representation (5). One can transform this formula into the prenex form

$$\forall \alpha \forall k \exists x \exists y (C'(\alpha) \rightarrow L'(\alpha, k, y)) \tag{6}$$

or any other. But there are no visible arguments to bound the quantifier on x, as it is actually a universal quantifier in the premise assertion of correctness of α.

Restrict ourselves to algorithms α whose correctness is provable in a formal system $\mathcal{F}$. To define such algorithms let us introduce the following notation:

$$C_{\mathcal{F}}(\alpha) =_{df} \exists D (D \text{ is a proof in } \mathcal{F} \text{ of } C(\alpha))$$
$$=_{df} \exists D\ PROOF_{\mathcal{F}}(D, \alpha).$$

As a restricted version of (5) we take:

$$\forall \alpha (C_{\mathcal{F}}(\alpha) \to \forall k \exists y L'(\alpha, k, y)). \quad (7)$$

Now the prenex form

$$\forall \alpha \forall D \forall k \exists y (PROOF_{\mathcal{F}}(D, \alpha) \to L'(\alpha, k, y)). \quad (8)$$

of (7) is more tractable.

Restricting the existential quantifier $\exists y$ in (8) may preserve the "physical meaning" of the initial assertion. Thus, the formula

$$\forall \alpha \forall D \forall k \exists y \leq \varphi(\alpha, D, k)(PROOF_{\mathcal{F}}(D, \alpha) \to L'(\alpha, k, y)) \quad (9)$$

with φ fast growing but tractable in the formal system, say hyperhyper exponential, can be considered as a satisfactory version of $\boldsymbol{P} \neq \boldsymbol{NP}$, though it is weaker than the initial formulation (4). This version is of the form for which independence implies validity.

So, there could be two sources of independence which do not imply validity:

(1) algorithms with not provable correctness;

(2) no sequence $\{y_k\}$ providing high complexity, i. e. such that $time_\alpha(y_k) > |y_k|^k$, is representable in a provable way, e. g. every such a sequence is very sparse: $length(y_k)$ grows faster than any provable function.

On computer aided theorem proving versus verification

It does not work but it is dear, and I will keep it on.

The problem of program verification, which exists since long time as a research domain, was not a favourite child of computer science. As a new-comer I could remark that one reason lies in using languages and settings not related to real software engineering and weak theoretical level. Even now many people working in the field do not know enough about industrial programming. Usually verification people invent their language to write program specification motivated by their inner considerations not taking into account the real practice, and give no theoretical analysis. What specifications are considered?

The standard idealized description of software engineering process [Som92] starts from an informal conception phase that must give a requirements definition. It always exists in practice though, as a rule, is vague and incomplete.

Usually program specification is being extracted from the requirements definition without analyzing it, and the later verification at best touches a small part of the requirements definition. On the other hand, it is well known that the most dangerous and difficult to detect errors are either in the requirements definition or in the process of extraction the first program specification that is later refined to an executable program. (Our first experience with this area revealed an error in the algorithm of the founders of the widely analyzed benchmark problem, the Generalized Railroad Crossing, see [BS97].) These phases of program development are verified by model checking in a very restricted and incomplete way. So we have a large gap between requirements definition and program specification, considerable gaps on the way to program in a standard programming language compilable to a executable code, and in addition, a hard to patch gap between the compilable program and the executable program that is of final interest. To prove anything about the latter one must have a formal semantics of the programming language and operating environment. Is it realistic to have all that? I guess no. And even if we have it, is it realistic to verify all? Clearly, not. At least not now. Hence, testing will be crucial for a very long time, and industry will rely more on testing than on verification, though testing is a particular case of the latter. But testing, as it exits, cannot prove the validity of programs. Thus, we have to develop formal methods.

As for testing, practically there is no theory on the subject. By theory I mean provable positive properties of particular feasible testing procedures, that is, something saying that if a given program and tests have these or those properties, then the result of testing guarantees that the program is correct (with respect to a given specification) with this or that probability. The mentioned probability is hard to define in a way interesting for applications if we do not consider only toy examples as linear functions or matrix multiplication for which even a low level formal verification is feasible.

The domain of formal verification looks as a good application field to interactive provers oriented on semantical considerations controlling the inference search. Unfortunately, such provers do not exist, as far as I know. The known one are syntactically controlled as early provers of the 60s. But this can be remedied. A flexible notion to specify programs, which permits to easily change the level of abstraction and is close to logic, are Gurevich machines [Gur95]. Their basic idea was known: to represent a current global state as an interpretation of the appropriate vocabulary. Yu. Gurevich transformed this idea into a system of notions and showed how to apply them. This notion seems of value for problems of verification oriented to logic. It is far from being a tool. But a tool similar in spirit, though more limited from the point of view of logic does exists, that is J.-R. Abrial's **B** [Abr96]. Maybe it is not so hopeless, the verification?

> "Nothing destroys the memory so much as writing memoirs."

Acknowledgments. The present survey is due to the iron grip of B. A. Trakhtenbrot. C. Calude helped me to start it. My colleagues and friends N. A. Shanin, R. Freidson, D. Grigoriev, G. . Mints, V. Orevkov, G. Tseitin, I. Zaslavski,

H. Maranjan, Yu. Matiyasevich, V. Kreinovich, M. Gelfond, V. Livshits, A. Beltiukov, A. Barvinok, D. Burago, N. Vorobjov Jr., S. Evdokimov, I. Ponomarenko provided me with different materials, more than I could use. I am thankful to all of them. The contents is the responsability of my subconsciousness.

References

[Abr96] J.-R. Abrial. *The B-book: Assigning programs to meanings.* Cambridge University Press, 1996.

[AVS81] G.M. Adel'son-Vel'ski and A. Slisenko. What can we do with problems of exhaustive search? In A. Ershov and D. Knuth, editors, *Algorithms in Modern Mathematics. Proc. Intern. Symp., Urgench, Uzbek SSR, September 16-22, 1979*, pages 315–342. Springer Verlag, 1981. Lect. Notes in Comput. Sci, vol. 122.

[Bar65] J. Barzdins. Complexity of recognizing the symmetry on turing machines. In A. A. Lyapunov, editor, *Problems of Cybernetics*, pages 245–248. Nauka, Moscow, 1965. (Russian.).

[Bar92] A. Barvinok. Computing the volume, counting integral points, and exponential sums. In *Proc. of the 8th Annu. ACM Symp. on Computational Geometry*, pages 161–170, 1992.

[Bel79] A. Beltiukov. Machine description and the hierarchy of initial grzegorczyk classes. In Yu. Matiyasevich and A. Slissenko, editors, *Zapiski Nauchnykh Seminarov LOMI. Series: Studies in Constructive Mathematics and Mathematical Logic, 8.*, volume 88, pages 30–46, 1979. (Russian. English: *J. of Soviet Mathematics*, 20(1982).).

[BGG97] E. Börger, E. Grädel, and Yu. Gurevich. *The Classical Decision Problem.* Springer-Verlag, 1997.

[BGM82] L. Babai, D. Grigoriev, and D. Mount. Isomorphism of graphs with bounded eigenvalue multiplicity. In *Proc. of the 14th ACM Symp. Theory of Comput.*, pages 310–324, 1982.

[Blu67] M. Blum. A machine-independent theory of the complexity of recursive functions. *J. Assoc. Comput. Mach.*, 14(2):322–336, 1967.

[BS97] D. Beauquier and A. Slissenko. On semantics of algorithms with continuous time. Technical Report 97–15, University Paris 12, Department of Informatics, 1997. Revised version.

[Bur92] D. Burago. A lower bound for the split-find problem for a pointer machines. *J. of the St. Petersburg Math. Soc.*, 159:23–38, 1992. Amer. Math. Soc. Trans. (2).

[CG82] A. Chistov and D. Grigoriev. Polynomial–time factoring of the multivariable polynomials over a global field. Technical Report E-5-82, Leningrad Division of Steklov Mathematical Institute, Academy of Sciences of the USSR, 1982. 39 p.

[CG83] A. Chistov and D. Grigoriev. Subexponential–time solving systems of algebraic equations. i, ii. Technical Report E-9-83, E-10-83, Leningrad Division of Steklov Mathematical Institute, Academy of Sciences of the USSR, 1983. 119 p.

[Clo97] P. Clote. Non-deterministic stack register machines. *Theor. Comput. Sci.*, 178(1–2):37–76, 1997.

[Edi73] Editorial. On the work of e. i. nechiporuk. In A. A. Lyapunov, editor, *Problems of Cybernetics, vol. 26*, pages 9–18. Nauka, 1973. (Russian).

[EK81] A. Ershov and D. Knuth, editors. *Algorithms in Modern Mathematics. Proc. Intern. Symp., Urgench, Uzbek SSR, September 16-22, 1979.* Springer-Verlag, 1981. Lect. Notes Comput. Sci., vol. 122.

[Evd88] S. Evdokimov. Factoring a solvable polynomial over a finite field and the Generalized Riemann Hypothesis. In D. Grigoriev, editor, *Zapiski Nauchnykh Seminarov LOMI. Series: Theory of Computational Complexity. 5*, volume 176, pages 104–117, 1988. Russian. English: *J. of Soviet Mathematics.*

[FP74] M. Fischer and M. Paterson. String-matching and other products. In *Complexity of Computations. (SIAM-AMS Proc., vol.7)*, pages 113–125, Providence, R. I., 1974.

[Fre70] R. Freidson. A characterization of the complexity of recursive predicates. In *Proc. Steklov Inst. of Mathematics*, volume 113, pages 78–101, 1970. Russian. English: *Proc. Steklov Inst. Math.*, 113(1970):91-117, Amer. Math. Soc.

[Fre96] R. Freidson. Algorithmics of np-hard problems. In *Amer. Math. Soc. Trans. (2) Vol. 178*, pages 1–4. AMS, Providence, R. I., 1996.

[Gal76] Z. Galil. Real-time algorithms for string-matching and palindrome recognition. In *Proc. 8th Annu. ACM Symp. on Theory of Computing*, pages 161–173, 1976.

[Gen34] G. Gentzen. Untersuchungen über das logische schließen. 1, 2. *Mathematische Zeitschrift*, 39:176–210, 405–443, 1934.

[Gri76] D. Grigoriev. An application of separability and independence notions for proving lower bounds of circuit complexity. In Yu. Matiyasevich and A. Slissenko, editors, *Zapiski Nauchnykh Seminarov LOMI. Series: Studies in Constructive Mathematics and Mathematical Logic*, volume 60, pages 38–48, 1976. Russian. English: *J. of Soviet Mathematics*, 14:5(1980).

[Gri77] D. Grigoriev. Embedding theorems for Turing machines of different dimensions and Kolmogorov's algorithms. *Doklady Akad. Nauk SSSR*, 234(1):15–18, 1977. Russian. English: *Soviet Math. Dokl.*, 18:3(1977):588–592.

[Gri86] D. Grigoriev. Complexity of deciding the first–order theory of algebraically closed fields. *Izvestia Akad. Nauk SSSR*, 50(5):1106–1120, 1986. Russian. English: *Math. USSR Izvestia*, 29:2(1987):459–475.

[Gri88] D. Grigoriev. Complexity of deciding tarski algebra. *J. Symp. Comput.*, 5:65–108, 1988.

[Gri89] D. Grigoriev. Complexity of quantifier elimination in the theory of ordinary differential equations. *Lect. Notes in Comput. Sci*, 378:11–25, 1989.

[GS82] D. Grigoriev and A. Slissenko, editors. *Theory of Computational Complexity 1.* Zapiski Nauchnykh Seminarov LOMI. Vol.118. Nauka, Leningrad, 1982. Russian. English: *J. of Soviet Mathematics*, 29(1985).

[Gur95] Y. Gurevich. Evolving algebra 1993: Lipari guide. In E. Börger, editor, *Specification and Validation Methods*, pages 9–93. Oxford University Press, 1995.

[GVJ85] D. Grigoriev and N. Vorobjov Jr. Finding real solutions of systems of algebraic inequalities in subexponential time. *Doklady Akad. Nauk SSSR*, 283(6):1561–1565, 1985. Russian. English: Soviet Math. Doklady, 32:1(1985):316–320.

[HB34] D. Hilbert and P. Bernays. *Grundlagen der Mathematik*, volume 1. Berlin, 1934.

[HB39] D. Hilbert and P. Bernays. *Grundlagen der Mathematik*, volume 2. Berlin, 1939.

[Hen66] F. Hennie. On-line Turing machine computations. *IEEE Trans. Electron. Computers*, EC–15(1):35–44, 1966.

[HKSS91] J. Heintz, T. Krick, A. Slissenko, and P. Solernó. Search for shortest path around semialgebraic obstacles in the plane. In D. Grigoriev, editor, *Zapiski Nauchnykh Seminarov LOMI. Series: Theory of Computational Complexity, 5*, volume 192, pages 163–173, 1991. Russian. English: *J. of Math. Sciences*, 70:4(1994):1944–1949.

[Kle45] S. Kleene. On the interpretation of intuitionistic number theory. *J. Symbolic Logic*, 10:109–124, 1945.

[Kle60] S. Kleene. Realizability and Shanin's algorithm for the constructive deciphering of mathematical sentences. *Logique et Analyse. Nouvelle série*, 3(11–12):154–165, 1960.

[KM97] V. Krenovich and G. Mints, editors. *Problems of Reducing the Exhaustive Search.* AMS Translations, series 2, vol. 178. American Mathematical Society, 1997.

[Kol32] A. N. Kolmogorov. Zur deutung der intuitionistischen logik. *Mathematische Zeitschrift.*, 35(1):58–65, 1932.

[Kol65] A. N. Kolmogorov. Three approaches to defining the notion 'quantity of information'. *Problems of Information Transmission*, 1(1):3–28, 1965. (Russian.).

[Kos94] S. R. Kosaraju. Real-time suffix-tree construction. In *Proc. 26th ACM Annu. ACM Symp. on Theory of Comput.*, 1994.

[KR98] B. Kashin and A. Razborov. Improved lower bounds on the rigidity of hadamard matrices, 1998. To appear. Russian. Translated into English on a regular basis.

[Kre97] V. Kreinovich. S. Maslov iterative method: 15 years later (freedom of choice, neural networks, numerical optimization, uncertainty reasoning, and chemical computing). In V. Krenovich and G. Mints, editors, *Problems of Reducing the Exhaustive Search*, AMS Translations, series 2, vol. 178, pages 175–189. American Mathematical Society, 1997.

[Kur59] A. G. et al Kurosh, editor. *Mathematics in the USSR for 40 years, 1917–1957*, volume 1–2. Fizmatgiz, Moscow, 1959. (Russian).

[KV65] S. K. Kleene and R. E. Vesley. *The Foundations of Intuitionistic Mathematics, Especially in Relation to Recursive Functions.* North-Holland, 1965.

[LLL82] A. Lenstra, H. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. Technical Report Preprint 195/82, Math. Centrum Amsterdam IW, 1982.

[LST85] S. Lavrov, A. Slissenko, and G. Tseitin. Curriculum for informatics and system programming. project. *Microprocessor Devices and Systems*, 4:20–28, 1985. (Russian.).

[Mar54] A. A. Markov. *The Theory of Algorithms.* Proceeding of Steklov Math. Inst., vol.42. AN SSSR, 1954. (Russian).

[Mar56] A. A. Markov. On one principle of constructive mathematical logic. In *Proceeding of the 3d All-Union Mathematical Congress*, volume 2, pages 146–147. Fizmatgiz, 1956. (Russian).

[Mar57] A. A. Markov. On inversive complexity of systems of functions. *Doklady AN SSSR*, 116:917–919, 1957.

[Mar64] A. A. Markov. On normal algorithms computing boolean functions. *Doklady AN SSSR*, 146(5):1017–1020, 1964.

[Mas64] S. Maslov. Inverse method of establishing the deducibility in the classical predicate calculus. *Doklady AN SSSR*, 159(1):17–20, 1964. Russian. English: *Soviet Math. Doklady.*

[Mas81] S. Maslov. Iterative methods in intractable problems as a model of intuitive methods, 1981. (Russian).

[Mas83] S. Maslov. Asymmetry of cognitive mechanisms and its applications. In *Semiotics and Information Science, vol. 20*, pages 3–31. VINITI, Moscow, 1983. (Russian).

[Mas87] S. Maslov. *Theory of Deductive Systems and its Applications.* MIT Press, Cambridge, 1987.

[Min72a] G. E. Mints. Exact estimates of the provability of transfinite induction in the initial segments of arithmetic. *J. Soviet Mathematics*, 1:85–91, 1972.

[Min72b] G. E. Mints. Quantifier-free and one-quantifier systems. *J. Soviet Mathematics*, 1:71–84, 1972.

[Min91] G. E. Mints. Proof theory in the USSR 1925-1969. *J. Symb. Logic*, 52(2):385–424, 1991.

[Min92] G. E. Mints. Complexity of subclasses of the intuitionistic propositional calculus. *BIT*, 32(1):64–69, 1992.

[MMM+80] S. Maslov, Yu. Matiyasevich, G. Mints, V. Orevkov, and A. Slissenko. Nikolai Aleksandrovich Shanin (On his sixtieth anniversary). *Uspekhi Matematicheskikh Nauk*, 35(2(212)):241–245, 1980. (Russian.).

[MMO71] S. Maslov, G. Mints, and V. Orevkov. Mechanical proof-search and the theory of logical deduction the USSR. *Revue Intern. de Philosophie*, 98(4):575–584, 1971.

[MMOS90] Yu. Matiyasevich, G. Mints, V. Orevkov, and A. Slissenko. Nikolai Aleksandrovich Shanin (On his sixtieth anniversary). *Uspekhi Matematicheskikh Nauk*, 45(1(271)):241–245, 1990. Russian. English: *Russian Math. Surveys*, 45:1(1990):239–240.

[MN88] A. A. Markov and N. M. Nagorny. *The Theory of Algorithms.* Mathematics and its Applications. Soviet series, 23. Dordrecht etc.: Kluwer Academic Publishers, 1988. The 2nd edition appeared in 1996 in Russian. It contains A. A. Markov's biography.

[MP97] J. Morris and V. Pratt. A linear pattern-matching algorithm. Technical Report TR-40, Computing Center, University of California, Berkeley, 1997.

[MT82] G. Mints and E. Tyugu. Justification of the structural synthesis of programs. *Sci. Comput. Progr.*, 2:215–240, 1982.

[NS64] N. M. Nagornyi and N. A. Shanin. Andrei Andreyevich Markov (To his sixtieth anniversary). *Uspekhi Matematicheskikh Nauk*, 19(3(117)):207–223, 1964.

[Ore64] V. Orevkov. On constructive mapping on circle into itself. In *Proc. Steklov Inst. of Mathematics*, volume 172, pages 437–461, 1964. Russian. English: *Proc. Steklov Inst. of Mathematics*, 100(1972):69–100, AMS Transl. (2).

[Ore93] V. P. Orevkov. *Complexity of proofs and their transformations in axiomatic theories.* AMS Translations of Mathematical Monographs, vol. 128, 153p. Amer. Math. Soc., 1993.

[Pon92] I. Ponomarenko. Polynomial-time algorithms for recognizing and isomorphism testing of cyclic tournaments. *Acta Appl. Math.*, 29:139–160, 1992.

[Rob64] J. Robinson. On automatic deduction. *Rice Univ. Studies*, 50(1):69–89, 1964.

[Sav98] J. Savage. *Models of Computations.* Addison-Wesley, 1998.

[SDM+83] N. Shanin, G. Davydov, S. Maslov, G. Mints, V. Orevkov, and A. Slissenko. An algorithm for machine search of a natural logical deduction in a propositional calculus. In *The Automation of Reasoning I. Classical Papers on Computational Logic 1957–1966*, pages 424–483. Springer Verlag, 1983. The Russian original appeared as a booklet, published by Nauka (1965, 39pp.).

[Sha87] N. Shanin. On finitary development of mathematical analysis on the base of euler's notion of function. In *The 8th Intern. Congress on Logic, Methodology and Philosophy of Science. Abstracts.*, pages 60–63. Moscow, 1987. vol. 1.

[Sli73] A. Slisenko. Recognizing a symmetry predicate by multihead turing machines with input. In V. Orevkov and N. Shanin, editors, *Proc. Steklov Inst. of Mathematics*, volume 129, pages 30–202, 1973. Russian. English: *Proc. Steklov Inst. of Mathematics*, 129(1976):25–208.

[Sli77] A. Slisenko. A simplified proof of real-time recognizability of palindromes on turing machines. In G. Mints and V. Orevkov, editors, *Zapiski Nauchnykh Seminarov LOMI. Series: Theoretical Applications of Methods of Mathematical Logic, 2.*, volume 68, pages 123–139, 1977. Russian. English: *J. of Soviet Mathematics*, 15:1(1981):68–77.

[Sli81a] A. Slissenko. Complexity problems of theory of computation. *Russian Mathematical Surveys*, 36(6):23–125, 1981.

[Sli81b] A. Slissenko. Detection of periodicities and string-matching in real time. In G. Mints and V. Orevkov, editors, *Zapiski Nauchnykh Seminarov LOMI. Series: Theoretical Applications of Methods of Mathematical Logic, 3.*, volume 105, pages 62–173, 1981. Russian. English: *J. of Soviet Mathematics*, 22:3(1983):1316–1386.

[Sli82] A. Slissenko. Context-free grammars as a tool for describing polynomial-time subclasses of hard problems. *Inform. Process. Lett.*, 14(2):52–56, 1982.

[Sli91] A. Slissenko. On measures of information quality of knowledge processing systems. *Information Sciences: An International Journal*, 57–58:389–402, 1991.

[Sli93] A. Slissenko. A view on recent years of research in theoretical computer science in the former Soviet Union. *RAIRO, Technique et science informatique*, 12(1):9–28, 1993.

[SM73] L. Stockmeyer and A. Meyer. Word problems requiring exponential time: preliminary report. In *Proc. 5th Annu. ACM Symp. on Theory of Comput.*, pages 1–9, Austin, Texas, 1973.

[Som92] I. Sommerville. *Software Engineering.* International Computer Science Series. Addison-Wesley, 1992. 4th edition.

[Tar96] V. Tarasov. *Inference control in expert systems based of explicit meta-rules of inference search.* PhD thesis, St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia, 1996. 132 p.

[Tra84] B. Trakhtenbrot. A survey of Russian approach to perebor (brute-force search) algorithms. *Annals of the History of Computing*, 6(4):384–400, 1984.

[Tra87] B. Trakhtenbrot. Selected developments in Soviet mathematical cybernetics (finite automata, combinatorial complexity algorithmic complexity). Technical Report 73/87, Delphic Associates Incorporated, 1987.

[Tse68] G. Tseitin. On the complexity of proofs in propositional calculus. In A. Slisenko, editor, *Zapiski Nauchnykh Seminarov LOMI, vol. 8*, pages 234–259, 1968. Russian. English: *Studies in Constructive Mathematics and Mathematical Logic*, Plenum Press.

[USP93] D. Ugolev, T. Sokolova, and I. Ponomarenko. On an algorithmic model of non-destructive chemical analyzer for complex biological and ecological systems. *Vestnik S.-Peterburgskogo Universiteta. Series 4.*, 4:49–60, 1993. Russian.

[VJ88] N. Vorobjov Jr. Deciding consistency of systems of polynomial in exponent inequalities in subexponential time. In D. Grigoriev, editor, *Zapiski Nauchnykh Seminarov LOMI. Series: Theory of Computational Complexity. 5*, volume 176, pages 7–40, 1988. Russian. English: *J. of Soviet Mathematics,* 59:3(1992):1322–1360.

[Weg87] I. Wegener. *The Complexity of Boolean Functions.* Wiley-Teubner, 1987.

[Yan59] S. A. Yanovskaya. Mathematical logic and foundations of mathematics. In A. G. et al Kurosh, editor, *Mathematics in the USSR over the forty years 1917–1957*, pages 13–120. Fizmatgiz, Moscow, 1959. (Russian).

[Zas55a] I. Zaslavsky. Invalidity of some theorems of classical analysis in constructive analysis. *Uspekhi Metem. Nauk*, 10(4(66)):209–210, 1955. Russian.

[Zas55b] I. Zaslavsky. Some criteria of compactness of metric and normed spaces. *Doklady Acad. Nauk SSSR*, 103(6):953–956, 1955. Russian.