A Fundamental Problem of Mathematical Logic

Jan Krajíček

Mathematical Institute of the Academy of Sciences
Žitná 25, Praha 1, 115 67, Czech Republic
krajicek@earn.cvut.cz

A fundamental open problem of mathematical logic and simultaneously the main problem of computational complexity theory is the following one.

> **Problem (an informal formulation):** *What is the most efficient way of deciding whether a propositional formula is satisfiable or not?*

It is a problem addressing a quite rudimentary topic at a fundamental level and having far-reaching connections to other parts of logic, mathematics and philosophy. Moreover, the research stimulated by this problem consistently generates interesting results and intrigued notions.

The $\mathcal{P} =_? \mathcal{NP}$ is the most famous technical version of the problem, see [15]. It asks whether there can be an algorithm deciding the satisfiability of formulas and running in time polynomial in the size of the formula. The size of a formula (or a proof) is the total number of symbols in it. This is proportional to the number of bits needed to encode the formula for a machine.

The main question about propositional calculus is whether there is a propositional proof system in which every tautology has a short proof (of size polynomial in the size of the tautology).

The main problem in bounded arithmetic is whether it is a finitely axiomatizable theory. This appears to be rather remote from the problem considered above but we shall see that it is not.

In the following five sections we briefly explain in a not too technical language the problems in all three areas (Sections 1 - 3) and the connections between them (Sections 4 and 5). The last section describes some recent work and formulates a technical problem which is currently investigated.

The paper is aimed at non-specialists. The text is accompanied by extensive references to original sources. However, most of the material can be found in the monograph [26] which an interested reader may use as an entrance into the field.

1 Computational Complexity

SAT is the set of satisfiable propositional formulas in the De Morgan language 1 (truth), 0 (false), $\vee$ (or), $\wedge$ (and) and $\neg$ (not). The set SAT is in $\mathcal{NP}$, the

* This is an outline of my *Collegium Logicum* lecture *Bounded arithmetic, propositional logic and complexity theory* delivered in the Kurt Godel Society on December 12, 1994.

class of sets accepted by a non-deterministic polynomial-time Turing machine; the machine simply guesses a truth assignment and accepts only if it is indeed a satisfying assignment.

$TAUT$ is the set of tautologies in the same language. Clearly, $\phi \in SAT$ iff $\neg\phi \notin TAUT$. Hence the complement $\setminus TAUT$ of $TAUT$ is in $\mathcal{NP}$. That is, $TAUT$ itself is in $co\mathcal{NP}$, the class of the complements of $\mathcal{NP}$-sets. Cook's theorem [15] says that

1. $\mathcal{NP} = co\mathcal{NP}$ iff $SAT \in co\mathcal{NP}$ iff $TAUT \in \mathcal{NP}$.
2. $\mathcal{NP} = \mathcal{P}$ iff $SAT \in \mathcal{P}$ iff $TAUT \in \mathcal{P}$.

This is the so called $\mathcal{NP}$-completeness of SAT and the $co\mathcal{NP}$-completeness of $TAUT$.

The trivial algorithm checking all possible truth assignments to the atoms in the formula is, essentially, the most efficient algorithm known (in other words: nothing is known). The number of truth assignments is 2^n where n is the number of atoms. As n might be close to the size of the formula this means that the trivial algorithm runs almost in exponential time.

Considerably more is known about the mutual relation between SAT and other decision problems in combinatorics or number theory; these are the $\mathcal{NP}$-completeness results, see [19]. There are also proofs that algorithms from some restricted classes of algorithms are not more efficient (in a substantial way) than the trivial algorithm. Here belong lower bounds to the circuit-size for various circuit models: constant depth ([1, 18, 55, 46, 54]) and monotone ([45, 6, 5]); see [9] (or [26, Chpt.3]) for an overview.

2 Propositional Logic

F (for a *Frege system*) is the often used propositional calculus in the language of SAT based on a finite number of axiom schemes and the modus ponens:

$$\frac{\phi \quad \neg\phi \vee \psi}{\psi}$$

as the only inference rule. SF (for F with *substitution*) is F augmented by the substitution rule:

$$\frac{\phi(p_1, \ldots, p_n)}{\phi(\psi_1, \ldots, \psi_n)}$$

allowing to infer in one step any substitution instance of an already derived formula (see [26, Chpt.4]).

It is a fundamental problem whether every tautology ϕ admits a proof in F or in SF of size polynomial in the size of ϕ. No non-trivial lower bounds are known (but non-trivial upper bounds for particular ϕ are known, e.g. [11] or [26, Chpt.13]).

Assume that every tautology would indeed admit polynomial size F-proofs. Then $TAUT \in \mathcal{NP}$ and hence $\mathcal{NP} = co\mathcal{NP}$. This is because a machine which guesses a polynomial size string and then accepts iff the string is an F-proof of the formula would be a non-deterministic acceptor of $TAUT$ running in polynomial time. With a suitable definition of a propositional proof system (as in [17]) the statement that $\mathcal{NP} = co\mathcal{NP}$ is actually equivalent to the statement that there is a propositional proof system in which all tautologies have polynomial size proofs (see [26, Chpt.4]. In fact, if such a proof system exists it could be formulated as an extension of SF by a polynomial-time set of tautologies as new axioms, see [28] or [26, Chp.14].

Obviously then, one expects that no proof system admits polynomial size proofs for all tautologies (as $\mathcal{NP} \neq co\mathcal{NP}$ is a generally accepted conjecture). This was, however, demonstrated only for some particular subsystems of F. Most notable examples are resolution ([20]), constant-depth systems ([2, 24, 33, 44]) and constant-depth systems augmented by additional axiom-schemes expressing various combinatorial principles ([3, 50, 8, 4, 7, 51]), see [26, Chpts.4 and 12]. Nothing is known for the constant-depth systems if the language contains also the equivalence connective $\equiv$. To prove a lower bound for such systems is the most accessible problem at present.

All known lower bounds fit into one methodological framework, the so called *partial boolean valuations* defined in [25]. It was proved there that, in principle, a valid lower bound for SF can be proved by a construction of a suitable partial boolean algebra and a map of formulas into it. However, such a construction is quite complicated even for the restricted cases considered above, see [26, Chpt.13].

3 Bounded Arithmetic

Bounded arithmetic is a subsystem of Peano Arithmetic in which the induction axioms are restricted to bounded formulas only. It was proposed by [38]. Several other systems, differing in the language and in the particular class of bounded formulas for which the induction is assumed, were defined and studied since then ([16, 39, 40, 41, 10]). Here we shall consider only the theory S^1_2 of [10], perhaps the most important one in the present context (see [26, Chpt.5]).

The language of S^1_2 is a bit richer then the language of Peano Arithmetic: $0, 1, +, \cdot, =, \leq$. In addition, it has three extra function symbols $|x|$ (the length of the dyadic numeral of x, $|x| = \lceil \log_2(x+1) \rceil$ for $x > 0$), $\lfloor \frac{x}{2} \rfloor$ and $x \# y$ (standing for $2^{|x|\cdot|y|}$). This language was motivated by the initial functions used for the machine-independent characterization of the polynomial-time functions by [14].

The class of bounded formulas in this language is stratified into levels $\Sigma^b_1 \subseteq \Sigma^b_2 \subseteq \ldots$ in a manner analogous to the arithmetical hierarchy $\Sigma^0_1 \subseteq \Sigma^0_2 \subseteq \ldots$. The first and most straightforward connection of bounded arithmetic to complexity theory is that bounded formulas define exactly those subsets of $\mathbf{N}$ which are in the polynomial-time hierarchy $\mathcal{PH}$ of [37], and the Σ^b_i-formulas define the sets from the i^{th}-level of $\mathcal{PH}$. In particular, the Σ^b_1-formulas define exactly the $\mathcal{NP}$-sets. See also [26, Chpt.3].

S_2^1 is axiomatized by a finite number of axioms codifying the basic recurrence properties of the functions in the language (the set $BASIC$ in [10]), and the following form of the induction axiom:

$$A(0) \wedge \forall x (A(x) \to A(x+1)) \longrightarrow \forall x A(|x|)$$

accepted for all Σ_1^b-formulas A. This form of induction is called the *length induction.*

The main theorem of [10], the so called *witnessing theorem*, stretches the correspondence between bounded formulas and sets from $\mathcal{PH}$ further. Namely, a function is Σ_1^b-definable in S_2^1 iff it is a polynomial-time function (and analogously for $i > 1$). See also [26, Chpt.7].

A particular instance of the finite axiomatizability problem (see [26, Chpt.10]) is whether already S_2^1 proves the length-induction for all bounded formulas and not just for Σ_1^b-formulas. Obviously, if for every bounded formula $A(x)$ there is a Σ_1^b-formula $B(x)$ such that S_2^1 proves $\forall x (A(x) \equiv B(x))$, then the answer is yes. This hypothesis is abbreviated by the phrase that S_2^1 proves that $\mathcal{PH} = \mathcal{NP}$. More interestingly, a form of the converse also holds: if S_2^1 entails the length-induction for all bounded formulas then the polynomial-time hierarchy collapses (to $\mathcal{PH} = \Sigma_2^p$ by [32]) and collapses even provably in S_2^1 (see [12, 56]).

The finite axiomatizability problem thus asks whether there is a model of bounded arithmetic in which $\mathcal{PH}$ does not collapse (and, in particular, in which there is no proof system in which all tautologies would have polynomial-size proofs in any proof system).

4 Propositional Logic and Bounded Arithmetic

Let T be a theory capable of coding finite strings. For example, $T = S_2^1, PA$ or ZFC. For simplicity assume that the language of T contains the language of S_2^1 and that $T \supseteq S_2^1$. There is a Π_1^b-formula (a negation of a Σ_1^b-formula) $Taut(x)$ such that for every propositional formula ϕ, $Taut(\lceil\phi\rceil)$ holds about the string $\lceil\phi\rceil$ encoding ϕ iff ϕ is a tautology. $Taut(\lceil\phi\rceil)$ is a bounded sentence and hence, if true, can be proved in T. This T-proof can be interpreted as a proof of ϕ in a propositional proof system P_T determined by T. Hence a theory can be thought off as a propositional proof system.

Let $A(x)$ be an arithmetical formula and n a number. Any string $\epsilon = (\epsilon_0, \ldots, \epsilon_{n-1}) \in \{0,1\}^n$ defines a number $\tilde{\epsilon} := \sum_{i<n} \epsilon_i \cdot 2^i$ and so $A(x)$ defines a Boolean function $f_{A,n}$:

$$f_{A,n}(\epsilon) := \begin{cases} 1 \text{ if } A(\tilde{\epsilon}) \text{ holds} \\ 0 \text{ otherwise} \end{cases}$$

Moreover, if $A(x)$ is a Π_1^b-formula then for every n there is a propositional formula $||A||^n$ in atoms $p_0, \ldots, p_{n-1}, q_1, \ldots, q_t$ of size polynomial in n such that:

$$f_{A,n}(\epsilon) = 1 \ \text{ iff } \ ||A||^n(p_i/\epsilon_i, \overline{q}) \in TAUT \ .$$

This is a corollary of the $co\mathcal{NP}$-completeness of $TAUT$, see [16, 28] or [26, Chpt.9].

Let P be a proof system. With this translation a P-proof of the formula $||A||^n$ can be interpreted as a proof of the arithmetic sentence $\forall x, |x| \le n \rightarrow A(x)$ in a theory T_P determined by P. Hence a propositional proof system can be considered as an arithmetical theory.

We have the following correspondence between arithmetic and propositional proof systems:

1. If T proves $\forall x A(x)$, where A is a Π_1^b-formula, then the formulas $\phi_n := ||A||^n$ are tautologies and there is a polynomial-time function constructing from $1 \ \ldots \ 1$ (n-times) a P_T-proof of ϕ_n.
2. If ϕ_n is a sequence of tautologies having polynomial-size P-proofs definable in T_P, then T_P proves $\forall x Taut(\lceil \phi_x \rceil)$. If $\phi_n = ||A||^n$ then T_P proves also $\forall x A(x)$.

Moreover (see [28] or [26, Chpt.9]):

3. T and $T_{(P_T)}$ prove the same $\forall \Pi_1^b$-formulas, and P and $P_{(T_P)}$ have proofs of same sizes (up to a polynomial increase).

What is most striking however, is that there are pairs (T, P) of a *natural* theory T and a *natural* propositional proof system P enjoying such a correspondence. *Natural* means that the systems were defined and studied prior to such a correspondence.

The best example is the pair (S_2^1, SF). In particular, any finite combinatorial principle (like the pigeonhole principle and similar), formalizable by a $\forall \Pi_1^b$-formula, is provable in S_2^1 iff the tautologies ϕ_n, encoding that the principle holds in structures of size n, have uniformly definable polynomial-size SF-proofs.

The following papers are related [16, 40, 28, 29, 34, 35, 25], or see [26, Chpt.9].

5 Further Connections to the Complexity Theory

The connections explained in Sections 3 and 4 establish a strong link of bounded arithmetic to complexity theory. The deepest among those is, in my opinion, the relation between the finite axiomatizability problem and the collapse of the polynomial-time hierarchy from [32]. This problem can be viewed also from the following angle.

It often happens that an important problem in a field of mathematics inspires two types or research. The research of the first type attempts to answer weaker variants of the original problem. The research of the second type tries to verify the conjectured solution of the problem in a class of structures similar to the structure intended in the original formulation of the problem. Both seem to be quite essential for a development of methods needed for a full solution of the problem.

Algebraic geometry and number theory provide good examples. Hilbert's 10^{th} problem for the field of rationals (about algorithmic solvability of Diophantine equations over $\mathbf{Q}$) inspires decision procedures for classes of equations and unsolvability results for bigger classes of first-order formulas over $\mathbf{Q}$, but also proofs of Matijasevic theorem [36] for various function fields over a finite field which bear relation to $\mathbf{Q}$, see [42, 43]. Another example is provided by the famous Riemann hypothesis. Besides partial results in its directions, analogous statements were formulated and proved for (various curves over) a finite field, see [52].

The intended structure for the conjecture that $\mathcal{P} \neq \mathcal{NP}$ (or that $\mathcal{PH}$ does not collapse in general) is the set of natural numbers $\mathbf{N}$ and the structures where the involved notions make a very good sense are models of bounded arithmetic. Thus to show that $\mathcal{P} \neq \mathcal{NP}$ in a class of models of bounded arithmetic appears to be a major research task, complementing the program of Boolean complexity to prove lower bounds to circuit-size for various restricted circuit models. The problem to establish the conjecture that $\mathcal{PH}$ does not collapse for a class of models of S_2 is just the finite axiomatizability problem.

Further connections to Boolean complexity are provided by [47] who showed that methods used at present for circuit-size lower bounds can be formalized in a suitable systems of bounded arithmetic, see also [26, Chpt.15].

6 A Current Research

The following two problems, two sides of the same coin by section 4., were currently investigated ([24, 48, 49, 27, 31]) and are not yet fully settled.

1. Let P be a propositional proof system. Estimate the circuit-size of an interpolant of an implication from the minimum size of its P-proof.
2. Let T be a theory and assume that T proves that two $\mathcal{NP}$-sets (represented by Σ_1^b-formulas) U and V are disjoint. Estimate the complexity (circuit-size) of a set separating the two sets.

If T proves $U(x) \rightarrow \neg V(x)$, where $U(x)$ and $V(x)$ are two Σ_1^b-formulas, then the implications $\neg||\neg U||^n \rightarrow ||\neg V||^n$ have polynomial size P_T-proofs, and the interpolants I_n for them define the set:

$$W = \bigcup_n \{\epsilon \in \{0,1\}^n \mid I_n(\epsilon)\}$$

separating $U = \{x \mid U(x)\}$ and $V = \{x \mid V(x)\}$: $U \subseteq W \wedge W \cap V = \emptyset$. Hence an upper bound for the first problem for $P = P_T$ yields an upper bound for the second one. In the opposite direction a similar reduction works. Take $T \supseteq T_P$ in which the P-proofs of the implications $\phi_n(\overline{p},\overline{q}) \rightarrow \psi_n(\overline{p},\overline{r})$ are definable. Then T proves the disjointness of the sets $U = \bigcup_n \{\epsilon \in \{0,1\} \mid \exists\delta\phi_n(\epsilon,\delta)\}$ and $V = \bigcup_n \{\epsilon \in \{0,1\} \mid \exists\xi\neg\psi_n(\epsilon,\xi)\}$, and every set separating U from V yields interpolants for the implications.

The problem is relevant to the lower bound problem for propositional logic as follows ([24]). Assume that two $\mathcal{NP}$-sets cannot be separated by a set of small circuit-size complexity. Assume also that a proof system P admits a polynomial upper bound in the first problem. Then we have a lower bound for P. Namely, the implications determined by the two sets cannot have short P-proofs as otherwise the two sets could be separated by a low complexity set (by the assumption about the existence of a polynomial upper bound for problem 1.) contradicting the assumption about the inseparability of U and V.

This problem is, to a large extent, still open. The reader may consult [27] for up-to-day (January 1995) information.

Acknowledgement: I thank V. Švejdar for comments on the manuscript of this paper.

References

1. Ajtai, M. (1983) Σ_1^1 - formulae on finite structures, *Annals of Pure and Applied Logic*, **24** : 1-48.
2. ——— (1988) The complexity of the pigeonhole principle, in: *Proc. IEEE 29th Annual Symp. on Foundation of Computer Science*, pp. 346-355.
3. ——— (1990) Parity and the pigeonhole principle, in: *Feasible Mathematics*, Eds. S.R.Buss and P.J.Scott, pp.1-24. Birkhauser.
4. ——— (1994) The independence of the modulo p counting principles, in: *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pp.402-411. ACM Press.
5. Alon, N., and Boppana, R. (1987) The monotone circuit complexity of boolean functions, *Combinatorica*, **7(1)** : 1-22.
6. Andreev, A. E. (1985) On a method for obtaining lower bounds for the complexity of individual monotone functions (in Russian), *Doklady AN SSSR*, **282(5)** : 1033-1037.
7. Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., and Pudlák, P. (1994) Lower bounds on Hilbert's Nullstellensatz and propositional proofs, submitted.
8. Beame, P., and Pitassi, T. (1993) Exponential separation between the matching principles and the pigeonhole principle, preprint.
9. Boppana, R., and Sipser, M. (1990) Complexity of finite functions. in:*Handbook of Theoretical Computer Science*, ed.J. van Leeuwen, pp.758-804.
10. Buss, S. R. (1986) Bounded Arithmetic. Naples, Bibliopolis. (Revision of 1985 Princeton University Ph.D. thesis.)
11. ——— (1987) The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic*, **52**: 916-927.
12. ——— (1993) Relating the bounded arithmetic and polynomial time hierarchies, manuscript.

13. Clote, P., and Krajíček, J. (1993) Open problems, in: *Arithmetic, Proof Theory and Computational Complexity*, eds.P. Clote and J. Krajíček, pp.1-19, Oxford Press.
14. Cobham, A. (1965) The intrinsic computational difficulty of functions, in : *Proc. Logic, Methodology and Philosophy of Science*, ed. Y. Bar-Hillel, North-Holland. Pp. 24-30.
15. Cook, S A. (1971) The complexity of theorem proving procedures, in: *Proc. 3^{rd} Annual ACM Symp. on Theory of Computing*, pp. 151-158. ACM Press.
16. ——— (1975) Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.
17. Cook, S. A., and Reckhow, A. R. (1979) The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**:36-50.
18. Furst, M., Saxe, J., B., and Sipser, M. (1984) Parity, circuits and the polynomial-time hierarchy, *Math. Systems Theory*, **17**: 13-27.
19. Garey, M.R., and Johnson, D. S. (1979) Computers and intractability. New York, W.H.Freeman and Co..
20. Haken,A. (1985) The intractability of resolution, *Theoretical Computer Science*, **39**:297-308.
21. Hastad, J. (1989) Almost optimal lower bounds for small depth circuits. in: *Randomness and Computation*, ed. S.Micali, Ser.Adv.Comp.Res. **5**: 143-170. JAI Pres.
22. Krajíček, J. (1989) Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universitas Carolinae*, **30(1)**:137-140.
23. ——— (1993) Fragments of bounded arithmetic and bounded query classes, *Transactions of the A.M.S.*, **338(2)** : 587-598.
24. ——— (1994) Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**, pp.73-86.
25. ——— (1995) On Frege and Extended Frege proof systems, in: *Feasible Mathematics II*, eds. P. Clote and J. Remmel, Birkhauser, pp.284-319.
26. ——— (1994) *Bounded arithmetic, propositional logic and complexity theory*, Cambridge University Press, in print.
27. ——— (1995) Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic, preprint.
28. Krajíček, J. and Pudlák, P. (1989) Propositional proof systems, the consistency of first order theories and the complexity of computations, *J. Symbolic Logic*, **54(3)**:1063-1079
29. ——— (1990) Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**:29-46.
30. ——— (1990) Propositional provability in models of weak arithmetic, in: *Computer Science Logic (Kaiserlautern, Oct. '89)*, eds.E.Boerger, H.Kleine-Bunning and M.M. Richter, LNCS 440, pp.193-210. Springer-Verlag.
31. ——— (1995) Some consequences of cryptographical conjectures for S_2^1 and EF, submitted.
32. Krajíček, J, Pudlák, P, and Takeuti, G. (1991) Bounded arithmetic and the polynomial hierarchy, *Annals of Pure and Applied Logic*, **52**: 143-153.
33. Krajíček, J.,Pudlák, P. and Woods, A. (1991) Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, submitted.
34. Krajíček, J., and Takeuti, G. (1990) On bounded $\sum_1^1$-polynomial induction, in: *Feasible Mathematics*, eds. S.R. Buss and P.J. Scott, pp.259-280. Birkhauser.
35. ——— (1992) On induction-free provability, *Annals of Mathematics and Artificial Intelligence*, **6**: 107-126.

36. Matijasevic, Y. (1970) Enumerable sets are Diophantine, *Doklady AN SSSR*, **191**, pp.279-282.
37. Meyer, A., and Stockmeyer, L. (1973) The equivalence problem for regular expressions with squaring requires exponential time, in: *Proc. IEEE* 13^{th} *Symp. on Switching and Automata Theory*, pp. 125-129.
38. Parikh, R. (1971) Existence and feasibility in arithmetic, *Journal of Symbolic Logic*, **36**, pp.494-508.
39. Paris, J., and Wilkie, A. J. (1981) Δ_0 sets and induction, in: Proc. of the Jadwisin Logic Conf., Poland, pp.237-248. Leeds University Press.
40. ——— (1985) Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic*, LNM 1130, pp.317-340.Springer.
41. ——— (1987) On the scheme of induction for bounded arithmetic formulas, *Annals of Pure and Applied Logic*, **35**, pp.261-302.
42. Pheidas, T. (1991) Hilbert's tenth problem for fields of rational functions over finite fields, *Inventiones Mathematicae*, **103**, pp.1-8.
43. ——— (1994) Extensions of Hilbert's tenth problem, *Journal of Symbolic Logic*, **59(2)**, pp.372-397.
44. Pitassi, T., Beame, P., and Impagliazzo, R. (1993) Exponential lower bounds for the pigeonhole principle, *Computational complexity*, **3**, pp.97-308.
45. Razborov, A. A. (1985) Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathem. Doklady*, **31**, pp.354-357.
46. ——— (1987) Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)** : 598-607.
47. ——— (1994) Bounded arithmetic and lower bounds in Boolean complexity, in : Feasible Mathematics II, eds. P. Clote and J. Remmel, Birkhauser, pp.344-386.
48. ——— (1994) Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, to appear.
49. ——— (1994) On provably disjoint NP-pairs, preprint.
50. Riis, S. (1993) Independence in bounded arithmetic, PhD. Thesis, Oxford University.
51. ——— (1994) $Count(q)$ does not imply $Count(p)$, preprint.
52. Shafarevich, I. R. (1974) Basic algebraic geometry, Springer-Verlag, N.York, Heidelberg, Berlin.
53. Smale, S. (1992) Theory of computation, in: *Mathematical Research Today and Tomorrow*, eds. C. Casacuberta and M. Castellat, Spring-Verlag, Berlin, Heidelberg, pp.59-69.
54. Smolensky, R (1987) Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in: *Proc. 19th Ann. ACM Symp. on Th. of Computing*, pp. 77-82.
55. Yao, Y. (1985) Separating the polynomial-time hierarchy by oracles, in: *Proc. 26th Ann. IEEE Symp. on Found. of Comp. Sci.*, pp. 1-10.
56. Zambella, D. (1994) Notes on polynomially bounded arithmetic, *preprint*.