On the complexity of the propositional calculus

Pavel Pudlák*
Mathematical Institute, Prague

November 25, 1998

Abstract

We show that research into the complexity of propositional proofs is related to various problems in other branches of mathematics. A nondeterministic procedure for a $co\mathcal{NP}$-complete can be viewed as a propositional proof system. We survey several proof systems which were proposed for problems in integer linear programing, algebra and graph theory. Then we consider a general method of proving lower bounds on the lengths of propositional proofs which is based on a property of some systems called *effective interpolation*. This means that the circuit complexity of interpolating boolean functions $f(x)$ of an implication $\phi(x,y) \rightarrow \psi(x,z)$ can be bounded by a polynomial in the length of a proof of the implication. We shall prove such a theorem for a system for integer linear programing proposed by Lovász and Schrijver [34] and show a relation between a problem on the complexity of linear programing and a problem of proving lower bounds on the lengths of proofs in this system. We shall consider the lengths of proofs in nonclassical logics, in particular monotone and intuitionistic logics, and, in a similar way, show a relation to the complexity of sorting networks.

1 Introduction

It is well-known that the theory of $\mathcal{NP}$-completeness and the problem $\mathcal{P} = \mathcal{NP}$? originated in the research of the complexity of propositional calculus. The computational content of the concept of a proof is a nondeterministic computation. Also, the satisfiability of a boolean formula has this nature. Thus the question $co\mathcal{NP} = \mathcal{NP}$?, closely related to the famous problem $\mathcal{P} = \mathcal{NP}$?, can be stated as a problem on the lengths of proofs in propositional calculus. To be more precise, we shall talk about propositional *proof systems*. In the general definition of

*pudlak@math.cas.cz, this work was partially supported by grant A1019602 of AV ČR and by cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic)

a proof system (equivalent to the one of [14]), a proof can be any object, we only require that the relation *"x is a proof of y"* in the proof system is checkable in polynomial time. Of course, we also assume that the provable propositions are just tautologies. In this definition we do not specify the class of formulas from which we take the tautologies. It is assumed that it is sufficiently universal in the sense that it is possible to code in this class all formulas in some complete basis of connectives. In this setting the problem $co\mathcal{NP} = \mathcal{NP}$? is equivalent to the question whether there is a polynomially bounded proof system, ie., a system in which every tautology has a proof of polynomial length.

The usual textbook proof systems are the so-called *Frege systems* or *sequent calculi*. One may naively expect that they are not particularly efficient and it would be easy to prove that they are not polynomially bounded, but the contrary is true. At present this problem seems hopelessly difficult. In order to get some experience with proving lower bounds on the lengths of proofs in propositional calculus we have to consider weaker proof systems. In practice there is a demand for solving even $\mathcal{NP}$-hard problems; in some cases a solution is considered satisfactory even if the algorithm is nondeterministic and gives short "proofs" for a large subset of instances. Such systems fall under the general concept of the propositional proof system, if we think of the objects as a suitable class of formulas. So a proof system is just a nondeterministic algorithm for a $co\mathcal{NP}$-complete problem. Several such procedures have been investigated mainly in combinatorial optimization, algebra and graph theory. We shall survey some systems in section 2.

The $co\mathcal{NP} = \mathcal{NP}$? and practical proof systems are not the only motivation for the research into the lengths of proofs in propositional calculus. It has been shown that superpolynomial lower bounds for certain proof systems can be used to prove the independence of true sentences from first order theories. In this way one could get explicit independent Π_1 sentences different from Gödel sentences. The theories for which these relations have been studied are weak subsystems of Peano arithmetic with the generic name *Bounded Arithmetic*. In some special cases independence results have been achieved. Theoretically this approach to independence results can work for any theory (containing a fragment of arithmetic such as Robinson's Q). However, for strong theories this leads to combinatorial problems of such complexity that there is little hope of making any progress in this way. We shall not survey this connection here and refer the reader to Krajíček's book [25].

Several methods of proving lower bounds on the lengths of proofs have been developed. In section 3 we shall explain the most appealing one, which is based on the well-known Craig interpolation theorem. The idea is to bound the complexity of the interpolant in terms of the complexity of the proof of the implication. In this way the lower bound problem on the length of proofs is reduced to a lower bound problem on the circuit size of particular circuits. Methods of complexity theory can then be applied directly. We shall prove such an interpolation theorem for one of the systems for integer linear programing.

Very little is known about the lengths of proofs in proof systems for nonclassical logics. Some nonclassical calculi are important for Artificial Intelligence, thus the question of the efficiency is of a practical interest. Here we show in section 4 that some restricted systems for *classical* propositional logic can be viewed as parts of systems for some *nonclassical* logics. In particular the resolution system is a part of the monotone sequent calculus which in turn is included in the intuitionistic sequent calculus.

The interesting feature of the research of such "practical" proof systems is that it connects with important mathematical problems. In particular our Problems 1 to 3 are related to two important subjects in theoretical computer science: the complexity of linear programing and the complexity of sorting.

The reader interested in the subject treated here can learn more in the book [25] and surveys [5, 28, 30, 38].

2 Mathematical proof systems

In this section we shall review some systems from mathematical practice. This means that they were proposed to give an explicit or efficient solution of a mathematical problem, or are motivated by such a result. We start, however, with one which is rather logical.

2.1 Resolution System

This is the propositional part of Robinson's resolution procedure for first order logic. We can view it as a refutation system for sets of disjunctions of *literals,* which are propositional variables and their negations. We think of disjunctions of literals as *sets* of literals, hence we do not need any structural rules. The only rule is the *resolution rule,* or the *cut,*

$$\frac{\bigvee A, \quad \bigvee B}{\bigvee (A \cup B) \setminus \{p, \neg p\}},$$

provided that $p \in A$ and $\neg p \in B$. A set of disjunctions is refuted by deriving the empty disjunction. We can look at it also dually; a resolution proof is then a proof of a formula in DNF. The complexity of a proof is measured by the number of disjunctions in the proof. A more restricted version is when one thinks of proofs as trees and counts the number of nodes. Exponential lower bounds are known for the unrestricted resolution system [19].

2.2 Proof systems for integer linear programing

An integer linear programing problem is given by a set of linear inequalities with real coefficients. In order to be able to consider the complexity of this problem, we shall assume that the coefficients are rational. The problem is to find integers satisfying these inequalities. The problem is known to be $\mathcal{NP}$-complete. A restricted version, where we look only for 0–1 solutions, is equally hard. In this case we can think of the variables as being propositional variables and inequalities as being a special kind of formulas, *threshold formulas*. Several proof systems have been proposed for this problem. Though they can also be used to derive inequalities from a given set of inequalities, it is more convenient to treat them as refutation systems, in a similar manner as resolution. Thus a proof starts with a given set of inequalities, proceeds with deriving new ones and ends with deriving a contradiction which is a false inequality, such as $0 \geq 1$.

Since we consider only 0–1 solutions, we shall assume that for each propositional variable x, the two inequalities $x \leq 1$ and $x \geq 0$ are among the initial ones. All systems contain rules making linear combinations from derived inequalities. We shall also assume that $1 \geq 0$ is given for free. Recall that we allow only rational coefficients in the inequalities.

2.2.1 Cutting Planes

The additional rule in this system is the *rounding rule:*

$$\frac{a_1x_1 + \ldots + a_nx_n + b \geq 0}{a_1x_1 + \ldots + a_nx_n + \lfloor b \rfloor \geq 0}$$

provided that $a_1, \ldots, a_n$ are integers. The completeness was proved by Gomory [17]; for 0–1 solutions it can be proved by simulating resolution. Exponential lower bounds for this system have been proved [21, 37].

2.2.2 Lovász and Schrijver [34]

The idea here is to allow also quadratic inequalities. The new rule is

$$\frac{F \geq 0}{xF \geq 0, \quad (1-x)F \geq 0}$$

where F is a linear term and x is a variable. This rule is sound for $0 \leq x \leq 1$. Note that we can apply this rule only to linear inequalities, thus in order to be able to apply it again, we have to eliminate the quadratic terms using linear combinations of the quadratic inequalities. Furthermore one can use the inequality $x^2 - x \geq 0$, for every variable, which gives, using the rule, $x^2 - x = 0$. The completeness can again be proved by simulating resolution.

Let us prove the following lemma as an example of a proof in this calculus.

Lemma 1 *The inequality $x + y + z \leq 1$ is derivable from $x + y \leq 1$, $x + z \leq 1$ and $y + z \leq 1$.*

Proof. By multiplying $x+y \leq 1$ by x and using $x^2 = x$ we get $xy \leq 0$. In the same way we get also $xz \leq 0$ and $yz \leq 0$. Adding $x+y \leq 1$ and $y+z \leq 1$, we get $x+2y+z \leq 2$. Multiplying it by $1-x$ and using $x^2 = x$, we get $2x+2y+z-2xy-xz \leq 2$. Using $xy \leq 0$ and $xz \leq 0$ it reduces to $2x+2y+z \leq 2$. Multiplying by $1-z$ and using $z^2 = z$ we get $2x+2y+2z-2xz-2yz \leq 2$, which reduces to $2x+2y+2z \leq 2$. This gives the conclusion by dividing it by 2. □

The following proposition implies that the calculus is stronger than resolution, as the *Pigeon Hole Principle* tautologies PHP do not have subexponential proofs in resolution.

Proposition 1 *The PHP tautologies have polynomial size proofs in the Lovasz-Schrijver calculus.*

Proof. The n-th PHP tautology is stated as the unsatisfiability of the following system of equations:

$$\begin{array}{ll} \sum_j x_{ij} \geq 1, & \text{for } i = 1, \ldots, n+1, \\ x_{ij} + x_{i'j} \leq 1, & \text{for } i, i' = 1, \ldots, n+1, \ i \neq i' \text{ and } j = 1, \ldots n. \end{array}$$

By adding the first set of inequalities, we get $\sum_{ij} x_{ij} \geq n+1$. To get a contradiction, we shall derive $\sum_{ij} x_{ij} \leq n$ from the second set of inequalities. For each j we shall show, gradually for all $r = 1, \ldots, n$, $\sum_{t=i}^{i+r} x_{t,j} \leq 1$, for all $i \leq n+1-r$. For $r = 1$, these are just inequalities contained in the initial ones. To go from r to $r+1$, take $\sum_{t=i}^{i+r} x_{t,j} \leq 1$ and $\sum_{t=i+1}^{i+r+1} x_{t,j} \leq 1$ and apply the lemma to $x = x_{i,j}$, $y = \sum_{t=i+1}^{i+r} x_{t,j}$ and $z = x_{i+r+1,j}$. This gives $\sum_{t=i}^{i+r+1} x_{t,j} \leq 1$. The number of inequalities that we have to consider in this proof is, clearly, polynomial. □

Furthermore Lovász and Schrijver considered extensions of this system obtained by adding the *multiplication rule* (multiplying two linear inequalities) and the axiom schema $F^2 \geq 0$ for every F linear.

2.2.3 Chvátal [unpublished]

This system resembles natural deduction, as one works with assumptions. In a proof we can pick an arbitrary linear inequality $F \geq a$ with *integer coefficients* and we branch the proof according to the two possibilities $F \geq a$ and $F \leq a-1$ (since we consider only integral solutions, we do not have to consider the values between $a-1$ and a). Such assumptions can be nested arbitrarily many times. Otherwise we use only linear combinations. Formally we can represent such a proof as a rooted binary tree, where the edges are labelled by linear inequalities in such a way that for each node the two edges have labels $F \geq a$ and $F \leq a-1$.

At each leaf there is a linear combination of the initial inequalities and those on the branch which leads to that leaf which produces a contradiction. In passing, note that the contradictory linear combinations can be found using polynomial time algorithms for linear programming, thus the proof is determined by the branching inequalities. It is an easy exercise to simulate Cutting Planes in this system. The relation to the previous system is not known.

Chvátal proposed also an apparently stronger version where the proofs have the structure of general DAGs. An exponential lower bound has been obtained for this system with the restriction that the coefficients are integers bounded by a polynomial in the input length [29].

2.3 Ideal generation systems

Let us now consider general algebraic equations

$$f_1 = 0, \ldots, f_n = 0$$

over some field. Again, the existence of a solution in the field is $\mathcal{NP}$-hard (and $\mathcal{NP}$-complete, if the field is finite). A well-known general criterion on unsolvability is the Hilbert Nullstellensatz. It says that the system is unsolvable in the algebraic closure of the field iff 1 is in the ideal generated by the polynomials of the equations. This leads to the following two systems. In both systems we assume that the set of equations includes $x^2 - x = 0$ for every variable, which ensures that solutions can be only 0–1. (In this case the Nullstellensatz has an easy proof by induction on the number of variables.)

2.3.1 Nullstellensatz proof system

A proof in this system is a sequence of polynomials $g_1, \ldots, g_n$ such that

$$g_1 f_1 + \ldots + g_n f_n = 1$$

(in the ring of polynomials). A natural measure of complexity of such a proof is the sum of the numbers of monomials in the polynomials $g_1, \ldots, g_n$, as this is roughly the length of a sequence encoding them. Another natural measure is the maximal degree of the polynomials $g_1, \ldots, g_n$. Clearly, if the degree is bounded by a constant, then the number of monomials is bounded by a polynomial. The converse is, of course, not true, but at least for some nice sets of polynomials $f_1, \ldots, f_n$, one can obtain a constant degree proof from a polynomial size proof by applying a random restriction. The restricted proof uses a "similar" set of polynomials. An example of such a set of polynomials are polynomials expressing the pigeon hole principle.

In general (when the equations $x^2 = x$ are not present) the minimal degree of the polynomials $g_1, \ldots, g_n$ can be exponential. Here, it can be at most the number of variables plus 1, as the equations $x^2 - x = 0$ ensure that multilinear polynomials are sufficient.

This system was investigated in connection with another proof system [2, 6] (the so called *bounded depth Frege system.*). An exponential lower bound on the lengths of proofs of some particular tautologies in that system was shown by reducing the question to a nonconstant lower bound on the degree of Nullstellensatz proofs.

An interesting feature of this system is that for a constant degree the proof search is easy; namely, a proof can be found in polynomial time by solving linear equations for the coefficients of the polynomials $g_1, \ldots, g_n$.

2.3.2 Polynomial calculus (also: Groebner proof system)[9]

Here we generate members of the ideal sequentially, using the basic closure conditions. Thus a proof is a sequence of polynomials $h_1, \ldots, h_m$ where each polynomial either belongs to the initial ones, or is obtained by the addition of two previously derived polynomials, or by multiplying a previously derived polynomial by an arbitrary one. Again, the most interesting parameter is the maximal degree of the polynomials $h_1, \ldots, h_m$. Proving lower bounds on the degree is harder than for the previous system; the first nonconstant lower bounds were found only recently ([24] for the field of reals, [43] for all fields, [27] for finite fields).

The proof search problem is in $\mathcal{P}$ also for polynomial proofs of constant degree. This follows from the Groebner basis algorithm [9].

2.3.3 Ideals in graph theory

Given a graph G on $\{1, \ldots, n\}$, we associate to it the polynomial

$$f_G = \prod_{i<j \text{ adjacent}} (x_i - x_j).$$

Some monotone families of graphs can be determined by ideals. E.g. the independence number of a graph is less than k iff f_G belongs to the ideal $I(k,n)$ of the polynomials which vanish whenever k variables are set equal. In some cases it is possible to find a set of generators such that the membership in this set can be decided in polynomial time. In the example above such a set of generators consists of f_H where H ranges over graphs which are unions of k vertex disjoint complete graphs [33]. Hence, for a graph G with independence number $\leq k$, the polynomial f_G can be expressed as

$$f_G = \sum_H g_H f_H,$$

where H are unions of k vertex disjoint complete graphs and g_H are some polynomials. As in the Nullstellensatz proof system, we can think of this expression as a proof (of G having the independence number $\leq K$). The natural measures of complexity are the size of this expression and the number of generators used. We do not know about any bounds on the complexity of such proofs.

2.4 Hajós calculus

This is a calculus for proving that a given graph G is not three-colorable. The initial axiom is the graph K_4, the complete graph on four vertices. The rules are: *edge/vertex introduction,* which allows to add vertices and edges arbitrarily, *contraction,* which allows to contract two nonadjacent vertices into one, and the following *join rule.* Suppose two constructed graphs share a vertex a and suppose (a, b) is an edge in one graph and (a, c) is in the other one. Then we deduce that the graph obtained from them by deleting $(a, b), (a, c)$ and adding (b, c) is also not three-colorable. Hájos introduced this system and proved its completeness [18].

The problem of proving lower bounds seems very hard, as this system simulates even *extended Frege systems* [36]. Surprisingly, for the version with proof trees an exponential lower bound was found [32].[1]

3 Lower bounds based on effective interpolation

Craig's interpolation theorem, restricted to propositional calculus, states that for a true implication $\phi(\bar{u}, \bar{x}) \to \psi(\bar{u}, \bar{y})$ where $\bar{u}, \bar{x}, \bar{y}$ are disjoint sets of variables, there exists a formula $\chi(\bar{u})$ containing only the common variables of the antecedent and succedent such that both $\phi(\bar{u}, \bar{x}) \to \chi(\bar{u})$ and $\chi(\bar{u}) \to \psi(\bar{u}, \bar{y})$ are true [15, 16]. Let

$$X = \{\bar{a};\ \exists \bar{b}\ \phi(\bar{a}, \bar{b})\}, \quad Y = \{\bar{a};\ \exists \bar{c}\ \neg\psi(\bar{a}, \bar{c})\}, \quad Z = \{\bar{a};\ \chi(\bar{a})\}.$$

Then the validity of the implication $\phi(\bar{u}, \bar{x}) \to \psi(\bar{u}, \bar{y})$ means that $X \cap Y = \emptyset$. The interpolation property of $\chi(\bar{u})$ means that $X \subseteq Z$ and $Z \cap Y = \emptyset$, ie., Z separates the sets X and Y. It was first observed by Mundici [35] that the question of how small interpolants χ can one find for given ϕ and ψ is essentially the question, how difficult is to separate two disjoint $\mathcal{NP}$ sets. It is a generally accepted conjecture, very important for cryptography, that the separating set cannot be in $\mathcal{P}$ for some $\mathcal{NP}$ disjoint pairs. This conjecture implies that for the corresponding implication there is no polynomial size interpolant formula.

The idea of proving a lower bound on the lengths of proofs using interpolation, as proposed by Krajíček [26], is to show a bound on the complexity of the interpolant not in terms of the complexity of ϕ and ψ, but in terms of the complexity of the *proof* of $\phi(\bar{u}, \bar{x}) \to \psi(\bar{u}, \bar{y})$. Then, if we succeed to show that for some implication of this form the interpolant cannot be simple, we can conclude that the proof of $\phi(\bar{u}, \bar{x}) \to \psi(\bar{u}, \bar{y})$ cannot be simple either. Such a relation between the size of a proof of $\phi(\bar{u}, \bar{x}) \to \psi(\bar{u}, \bar{y})$ and the complexity

[1] In the case of the extended Frege system the versions with trees and DAGs are equivalent, so this shows that the tree structure is not preserved in the simulation of the Hájos calculus.

of an interpolant is known for some systems, eg. for Resolution and Cutting Planes [26, 37]. Namely, the set Z can be computed by a boolean circuit whose size is polynomial in the size of the proof. This property of a proof system is called *effective interpolation.* An effective interpolation does not suffice for proving superpolynomial lower bounds on the lengths of proofs. We can derive such bounds only using some conjectures from cryptography. These conjectures are quite strong, thus one may wonder what do we gain by proving an effective interpolation theorem. Isn't it better to use just the conjecture $\mathcal{NP} \neq co\mathcal{NP}$? But we do get more. Firstly, $\mathcal{NP} \neq co\mathcal{NP}$ is not known to be comparable with such conjectures, however strong they seem. Secondly, using effective interpolation and an assumption that a particular function is one way, we get explicit tautologies which should not have short proofs. Furthermore, having effective interpolation may be the first step to get an unconditional lower bound, as it was the case eg. for Cutting Planes.

3.1 Interpolation for the calculus of Lovász and Schrijver

Here we prove such effective interpolation for the calculus of Lovász and Schrijver described above. Our proof actually gives a stronger result – effective interpolation for the union of Cutting Planes and the Lovász – Schrijver calculus with the general multiplication rule. As we have to use the rounding rule anyway, we shall consider this stronger calculus. (Actually, we do not know if the following lemma holds for the Lovász – Schrijver calculus alone.)

Lemma 2 *Let $\bar{x}$ and $\bar{y}$ be two disjoint sets of variables and $E_{\bar{x}}$ and $E_{\bar{y}}$ sets of linear inequalities containing only the corresponding variables. Suppose we have a proof of contradiction from the union of the two sets, then we can construct in polynomial time a proof of contradiction from one of the sets.*

Proof. We shall use an idea of some previous proofs of effective interpolation [37]: we will split the proof into two proofs each using only one kind of variables, either $\bar{x}$, or $\bar{y}$. An inequality in the original proof is the sum of the corresponding pair of the new inequalities except that the constant term may be larger in the original proof than the sum of the constant terms in the new inequalities. Hence the new inequalities are at least as strong as the original one. Thus at least one of the proofs must contain a contradiction.

First we redefine the concept of a proof. A line in a proof will be only a *linear* inequality. To get a new linear inequality we may use a more complicated construction, namely, take some positive linear combinations of the given inequalities, multiply some of them by variables and take their sum. This is allowed only if all quadratic terms cancel in the sum. In other words, we do not consider the intermediate quadratic inequalities as separate steps. Furthermore we shall use only inequalities with integer coefficients. Thus the rounding rule will be interpreted as taking a linear combination and rounding in one step.

An inequality $F_1(\bar{x})+F_2(\bar{y})+c \geq 0$, with F_1, F_2 linear forms and constant c, of the original proof will correspond to inequalities $F_1(\bar{x})+c_1 \geq 0$ and $F_2(\bar{y})+c_2 \geq 0$ in the two new proofs. We shall prove by induction that $c_1+c_2 \leq c$, so the two inequalities are at least as strong as the original one.

It is trivial to show that the rounding rule, if done in parallel in the two proofs, preserves this property. Thus it remains to show this for the multiplication rule of the Lovász – Schrijver calculus. An inequality derived by this rule has the following general form

$$\begin{gathered} L^{(1)}(\bar{x})+L^{(2)}(\bar{y})+ \\ \sum_i a_i(x_i^2-x_i)+\sum_k L_k^{(3)}(\bar{x})L_k^{(4)}(\bar{x})+ \\ \sum_j b_j(y_j^2-y_j)+\sum_l L_l^{(5)}(\bar{y})L_l^{(6)}(\bar{y})+ \\ \sum_m L_m^{(7)}(\bar{x})L_m^{(8)}(\bar{y}) \geq 0 \end{gathered}$$

where $L^{(1)}(\bar{x}), L^{(2)}(\bar{y}), L_k^{(3)}(\bar{x}) \geq 0, \ldots, L_m^{(8)}(\bar{y}) \geq 0$ are some linear inequalities derived before. Let us note that in each of the following expressions

$$\begin{gathered} L^{(1)}(\bar{x}), \quad L^{(2)}(\bar{y}), \\ \sum_i a_i(x_i^2-x_i)+\sum_k L_k^{(3)}(\bar{x})L_k^{(4)}(\bar{x}), \\ \sum_j b_j(y_j^2-y_j)+\sum_l L_l^{(5)}(\bar{y})L_l^{(6)}(\bar{y}), \\ \sum_m L_m^{(7)}(\bar{x})L_m^{(8)}(\bar{y}), \end{gathered}$$

all quadratic terms cancel. So we can assume w.l.o.g. that we actually first derive the inequalities with these linear terms and then we sum them. The first four are all right as they use only one type of variable, so we only need to consider the last one. Let us write it as $F_1(\bar{x})+F_2(\bar{y})+c \geq 0$, with F_1, F_2 linear forms and a constant c. The crucial observation is that this inequality follows from $L_m^{(7)}(\bar{x}) \geq 0$, $L_m^{(8)}(\bar{y}) \geq 0$ without using the assumption that x_i and y_j are integers. (Recall that $x_i^2-x_i \geq 0$ and $y_j^2-y_j \geq 0$ are the only axioms which express that fact and we do not use them here.) Hence $F_1(\bar{x})+F_2(\bar{y})+c \geq 0$ must be a linear combination of these inequalities. Taking separately the parts of this linear combination with $\bar{x}$ resp. $\bar{y}$ we get inequalities $F_1(\bar{x})+c_1 \geq 0$ and $F_2(\bar{y})+c_2 \geq 0$ with $c_1+c_2=c$ as consequences of the previous inequalities. The constants c_1, c_2 need not be integers, so we round them down.

Now, we have to find the constants c_1, c_2 in polynomial time. This is done using a polynomial time algorithm for linear programming. To find $-c_k$, for $k = 1, 2$, we maximize F_k using the inequalities above as constraints.

In the two new proofs the coefficients of the variables come from the original proof, thus we only have to watch if the constant terms are not too small (they are always less than or equal to the original ones). But if the constant is less than the negative of the sum of the coefficients of the variables, the inequality cannot be satisfied and we can stop. $\square$

Theorem 2 *The calculus of Lovász and Schrijver combined with Cutting Planes has effective interpolation.*

Proof. Suppose we have a proof of contradiction from the union of the two sets of linear inequalities $E_{\bar{u},\bar{x}}$ and $E_{\bar{u},\bar{y}}$, with $\bar{x}$ and $\bar{y}$ two disjoint sets of variables. We want to construct a polynomial size circuit which for a given input $\bar{a}$ tells which of the two sets $E_{\bar{a},\bar{x}}$, $E_{\bar{a},\bar{y}}$ is inconsistent. It is enough to have a polynomial algorithm, as it can be turned into a polynomial size circuit using standard methods. Such an algorithm was shown in the previous lemma. $\square$

We do not know if effective interpolation holds for stronger versions of the calculus, in particular, if it holds when inequalities $F^2 \geq 0$ are added for all linear functions F.

An interesting observation, due to J. Sgall, is that *interpolating functions for this system are as hard as solving an instance of linear programing* (the one with arbitrary rationals). Namely, take $\sum_i -a_{ij}x_i + d_j \geq 0$, $\sum_i c_i x_i \geq u$ and $\sum_j a_{ij}y_j + c_i \geq 0$, $\sum_j d_j y_j \geq -u + \varepsilon$ for a small $\epsilon > 0$. Here u is the single common variable. To determine for which u which part is contradictory, means to locate the minimax e with ε precision. (Here we take u to be an arbitrary real, but instead we can take several 0–1 variables multiplied by powers of 2 to approximate it.) Similar characterizations of the complexity of the interpolation are known for other systems: interpolants for Resolution are characterized by boolean circuits [26], interpolants for Nullstellensatz by span programs [39].

3.2 Monotone interpolation

As we have observed above, an effective interpolation does not suffice to prove a superpolynomial lower bound on the lengths of proofs. However, in some cases (Resolution, Cutting Planes, Nullstellensatz) it is possible to get a reduction to some monotone circuits for which it is possible to prove exponential lower bounds. In particular for Cutting Planes, assuming that the coefficients with the variables $\bar{x}$ are all positive, an interpolant can be computed by a *monotone real circuit.* Such circuits are generalizations of monotone boolean circuits in the sense that they are allowed to use arbitrary reals in computations and the gates are arbitrary binary nondecreasing real functions. The lower bound techniques for monotone boolean circuits can be easily extended to this kind of circuits [21, 37].

In order to prove a lower bound by a reduction to monotone real circuits for the calculus of Lovász and Schrijver, we need to show that a suitably presented versions of linear programing can be computed by monotone real circuits, namely:

Problem 1 *Let a matrix $\{a_{ij}\}$ and a vector $\vec{d}$ of rational numbers be fixed. Does there exist a polynomial size monotone real circuit which for given input vector $\vec{c}$ of rational numbers computes*

$$\max\{\sum_j d_j y_j;\ \forall i\ \sum_j a_{ij} y_j \le c_i\}\ ?$$

Note that the maximum as a function of the variables c_i is nondecreasing, since by increasing a c_i we increase the set over which we maximize. This problem is interesting independently of its application to the bounds on the length of proofs. A negative answer would show that all polynomial algorithms for linear programing must be, in some sense, indirect. Namely, any polynomial size arithmetic circuit for linear programing would have to compute some values which do not depend on the input in a monotone way. For the negative solution to this problem, it suffices to find a counterexample to the monotone version of the interpolation theorem above, namely a short proof of a "monotone" tautology for which we know that it does not have an interpolant computable by small monotone real circuits. We know, for instance, that there is no subexponential size real monotone circuit which separates graphs with m cliques from $m-1$-colorable graphs [37]. Thus, if one can solve negatively the above problem by finding subexponential size proofs of the following tautology expressing that for every graph (coded by the variables p_{ij}) either it does not have a clique of size m (coded by the variables q_{ki}), or it is not $m-1$-colorable (the coloring coded by the variables r_{il}).

$$\sum_i q_{ki} \ge 1, \quad \text{for } k = 1, \dots, m;$$

$$\sum_k q_{ki} \le 1, \quad \text{for } i = 1, \dots, n;$$

$$\sum_l r_{il} \ge 1, \quad \text{for } i = 1, \dots, n;$$

$$q_{ki} + q_{k'j} - p_{ij} \le 1 \quad \text{for } 1 \le i < j \le n,\ 1 \le k, k' \le m,\ k \ne k';$$

$$p_{ij} + r_{il} + r_{jl} \le 2, \quad \text{for } 1 \le i < j \le n, l = 1, \dots, m-1.$$

Let us note that these are the tautologies for which exponential lower bounds were shown in [37], so it would also show that Cutting Planes are weaker than Lovász and Schrijver. By adding corresponding inequalities in the last two sets we can eliminate the variables p_{ij} and get a stronger system where the last two sets are replaced by

$$q_{ki} + q_{k'i} + r_{il} + r_{jl} \leq 3$$

$$\text{for } 1 \leq i < j \leq n,\ 1 \leq k, k' \leq m,\ k \neq k',\ 1 \leq i < j \leq n,\ l = 1, \dots, m-1.$$

These equations express that there are two mappings, one defined on an m element set, the other having domain an $m-1$ element set, such that the composition of the two is a one-to-one mapping. The unsatisfiability of this set is a sort of a stronger pigeon hole principle.

3.3 Existential interpolation

It has been shown that effective interpolation is unlikely for some strong systems [31]. Therefore one has to look for other methods or one has to generalize the concept of effective interpolation. There is one particularly natural generalization, called *existential interpolation*. We say that a proof system P has this property, if there exists a polynomial p such that the following holds. If $\phi(\bar{x}) \vee \psi(\bar{y})$, with $\bar{x}$ and $\bar{y}$ disjoint sets of variables, has a proof of length n in P, then either $\phi(\bar{x})$ or $\psi(\bar{y})$ has a proof of length at most $p(n)$ in P. (In a more general version we allow the latter proof to be in some stronger proof system P'.) All the systems for which we know that effective interpolation holds, satisfy also this condition. On the other hand, there is a proof system for which only existential interpolation has been shown. This is the system of Chvátal described above (with proofs as trees), see [22]. However, for this system a slightly less effective interpolation theorem has been shown where the circuits are of size $n^{O(\log n)}$ [22] and effective interpolation was proved for the case of polynomially bounded integer coefficients [29] (the last result is actually stronger: it works for proofs as DAGs and there is a monotone version of it).

For using existential interpolation to prove superpolynomial lower bounds we need two disjoint $\mathcal{NP}$ sets A, B which cannot be separated using a pair of disjoint $co\mathcal{NP}$ sets A', B' in such a way that $A \subseteq A'$ and $B \subseteq B'$. Let us note that the pairs of disjoint $\mathcal{NP}$ sets A, B which one gets from the functions used in cryptography do not satisfy this condition, since they are actually complements.

4 The lengths of proofs in nonclassical logics

In artificial intelligence we need to automate logical deduction and quite often nonclassical logics seem the better alternative. Hence one should study the lengths of proofs also for nonclassical calculi. But even if we stick to classical logic (say, we are interested in the complexity theory and aim at $co\mathcal{NP} \neq \mathcal{NP}$), proof systems for some nonclassical logics may help. The aim of this section is to show that.

The basic observation is: *Propositional Resolution system is the sequent system restricted to propositional variables.* In more detail, we represent the disjunction $\neg x_1 \vee \ldots \vee \neg x_m \vee y_1 \vee \ldots \vee y_n$ by the sequent $x_1, \ldots, x_m \longrightarrow y_1, \ldots, y_m$. If we use only propositional variables as formulas, the only rules that can be used in the classical sequent calculus LK are structural rules and *cut*. The structural rules correspond to the fact that in resolution we think of disjunctions as sets, the cut is the resolution rule.

4.1 Monotone sequent calculus

Now we can embed Resolution in other calculi by relaxing the condition on the formulas used in proofs. One of such calculae is the *monotone sequent calculus.* This is LK restricted to formulas in the monotone basis $\wedge, \vee$. The only monotone tautological *formula* is the constant for truth $\top$, thus we are rather interested in proving tautological *sequents.* The interpretation of monotone sequents is an implication $\phi \rightarrow \psi$ with ϕ and ψ monotone formulas. Tautologies of the monotone sequent calculus are all classical tautologies which are implications of monotone formulas. Such a fragment of classical logic is also known as *geometric logic.*

While for monotone boolean circuits exponential lower bounds were proved long ago, we do not have any nontrivial lower bounds on the lengths of proofs in the monotone sequent calculus.

There is a trivial and useless interpolation theorem here; namely, for a monotone sequent $\Phi(\bar{u}, \bar{x}) \longrightarrow \Psi(\bar{u}, \bar{y})$, we have interpolants $\Phi(\bar{u}, \top, \ldots, \top)$ and $\Psi(\bar{u}, \bot, \ldots, \bot)$. Note that this is different from the translation of the interpolation theorem for Resolution. The form we get in this way is the following. Two *sets* of sequents are given, one in variables $\bar{u}, \bar{x}$ and the other in variables $\bar{u}, \bar{y}$. Furthermore we have a proof of contradiction from the union of the two sets. In the case of Resolution, formulas occurring in the sequents are only propositional variables. Then, there exists a polynomial size circuit which for a given assignment $\bar{a}$ for the variables $\bar{u}$ decides which of the sets is contradictory. It is rather unlikely that this generalizes to sets of sequents with arbitrary monotone formulas, as it would imply effective interpolation for classical (ie., with negations) Frege systems.

In several cases the first sequence of tautologies for which an exponential lower bound was shown was the Pigeon Hole Principle (PHP). Also here it is important as several other tautologies (eg. those used for exponential lower bounds for cutting planes) can be reduced to PHP. Note that PHP is a monotone tautology ("every pigeon sits in a hole $\longrightarrow$ there is a hole with two pigeons"). We do not know if PHP has polynomial proofs in the monotone sequent calculus. This is, a bit surprisingly, related to the question on the complexity of sorting networks. The usual proofs of PHP go by induction counting the pigeons assigned to a segment of holes. To construct such a proof in monotone calculus we need to formalize the concept of counting. There are constructions of polynomial size monotone counting formulas. The first is a probabilistic construction of Valiant [44], the second follows from the famous sorting network of Ajtai, Komlós and Szemeredi [1]. However, having small monotone counting formulas does not suffice for simulating the inductive proof of the PHP; we need also short proofs of the basic properties of the counting formulas. There is little hope to get it for the first kind of monotone formulas, as they are not explicit, their existence is shown by a probabilistic argument. In the case of the formulas obtained from the sorting network the problem is that the proof of the properties of the circuit is highly nontrivial and, moreover, relies on the construction of expander graphs. All the proofs of the expanding properties of the known explicit constructions of expanders are nonelementary. Thus the following seems to be a difficult problem:

Problem 2 *Are there polynomial size monotone counting formulas with polynomial size proofs of the basic properties?*

The counting formulas are formulas which are true iff exactly k variables are true; k ranges from 1 to the number of variables; the basic properties express that if exactly k variables are true and we flip a false variable, we get $k+1$ true variables. A negative solution to the problem would be an explanation why there are no "simple" monotone counting formulas, hence no simple sorting networks of logarithmic depth. Let us also state the related problem on PHP explicitly.

Problem 3 *Does PHP have proofs of polynomial length in the monotone sequent calculus?*

4.2 Intuitionistic propositional calculus

This is the most famous among nonclassical calculi. We arrive at it by observing that monotone sequents which are classical tautologies are also intuitionistic tautologies. Striclty speaking the monotone sequent calculus is not a subsystem of the intuitionistic sequent system, as in the intuitionistic sequent calculus only sequents with the empty or one-element consequents are allowed, but there is a simple simulation. Consequents with more than one formulas are simulated by disjunctions of the formulas.

No superpolynomial lower bounds are known on the lengths of intuitionistic sequent proofs. This problem is not necessarily harder than the same for the monotone sequent calculus, since the language is richer. It seems to be easier than proving superpolynomial lower bounds for the classical sequent calculus, since the set of intuitionistically valid tautologies is $\mathcal{PSPACE}$-complete. We do not have a proof of a superpolynomial lower bound for proofs in the intuitionistic propositional calculus, but we can at least prove an effective interpolation theorem. This follows from a recent result of Buss and Mints, which answers a problem posed in an earlier version of this paper.

Theorem 3 **([7])** *There is a polynomial time algorithm which for every proof of* $\longrightarrow \phi \vee \psi$ *in the intuitionistic propositional sequent calculus constructs a proof, in the same calculus, of* $\longrightarrow \phi$ *or* $\longrightarrow \psi$*?*

Note that we do not assume that the formulas have disjoint sets of variables here. This theorem is a computationally efficient version of the well-known theorem on intuitionistically derivable disjunctions in the propositional calculus.

Corollary 4 *Let a proof* D *of* $\chi(\bar{u}) \longrightarrow \phi(\bar{u},\bar{x}) \vee \psi(\bar{u},\bar{y})$ *in the intuitionistic propositional calculus be given. Then it is possible to construct a circuit* C *whose size is polynomial in the size of* D *and which, for every vector* $\bar{a}$ *of 0's and 1's which satisfies* $\chi(\bar{a})$*, tells one of the formulas* $\phi(\bar{a},\bar{x})$*,* $\psi(\bar{a},\bar{y})$ *which is a tautology.*

Proof. Let $\bar{a}$ be given. Think of $\bar{a}$ as a vector of symbols for the truth and the falsehood and substitute it for the variables $\bar{u}$ in the proof D. If $\chi(\bar{a})$ is true, then it is derivable by a proof whose size is polynomial in the size of χ since the formula does not contain variables. Thus we get a proof of $\longrightarrow \phi(\bar{a},\bar{x}) \vee \psi(\bar{a},\bar{y})$. Then we apply the algorithm of the theorem above to get a proof of $\phi(\bar{a},\bar{x})$ or $\psi(\bar{a},\bar{y})$. □

Corollary 5 *Suppose two disjoint sets* $X, Y \in \mathcal{NP}$ *are given such that* X *and* Y *cannot be separated by a set in* $\mathcal{P}/poly$*. Then it is possible to construct a sequence of propositional intuitionistic tautologies which do not have polynomial size proofs.*

Proof. Let X and Y be given. Furthermore, let a natural number n be given. The disjoint sets $X \cap \{0,1\}^n$ and $Y \cap \{0,1\}^n$ can be defined by $\{\bar{a};\ \exists\bar{b}\ \neg\phi(\bar{a},\bar{b})\}$ and $\{\bar{a};\ \exists\bar{c}\ \neg\psi(\bar{a},\bar{c})\}$ with ψ,ϕ propositional formulas of polynomial size in n. Hence $\phi(\bar{u},\bar{x}) \vee \psi(\bar{u},\bar{y})$ is a classical tautology. Let $\chi(\bar{u})$ be $(u_1 \vee \neg u_1) \wedge \ldots \wedge (u_n \vee \neg u_n)$. Consider the following formula.

$$\chi(\bar{u}) \longrightarrow \neg\neg\phi(\bar{u},\bar{x}) \vee \neg\neg\psi(\bar{u},\bar{y}). \tag{1}$$

If it had a polynomial size proof, then, by the previous corollary, we could construct a polynomial size circuit which separates the sets $X \cap \{0,1\}^n$ and $Y \cap \{0,1\}^n$. That would be a contradiction with the assumption about the sets X and Y. Hence it remains to show that the formula (1) is an intuitionistic tautology. The reason is that we have *excluded middle* for the common variables, thus we can prove it "by cases". Each case reduces to a classical formula.

Arguing more precisely, first we observe that $\chi(\bar{u})$ is equivalent to $\bigvee_{\bar{a}}(u_1^{a_1} \wedge \ldots \wedge u_n^{a_n})$, where the superscript indicates whether we take the variable or its negation. Thus we only need to show that, for every $\bar{a}$, either

$$u_1^{a_1} \wedge \ldots \wedge u_n^{a_n} \longrightarrow \neg\neg\phi(\bar{u}, \bar{x}) \tag{2}$$

or

$$u_1^{a_1} \wedge \ldots \wedge u_n^{a_n} \longrightarrow \neg\neg\psi(\bar{u}, \bar{y}) \tag{3}$$

is intuitionistically valid. To this end we first prove by induction on subformulas α of ϕ and ψ that

$$u_1^{a_1} \wedge \ldots \wedge u_n^{a_n} \longrightarrow \alpha(\bar{u}) \equiv \alpha(\bar{a}) \tag{4}$$

Since either $\phi(\bar{a}, \bar{x})$ or $\psi(\bar{a}, \bar{y})$ is a classical tautology, we have that either $\neg\neg\phi(\bar{a}, \bar{x})$ or $\neg\neg\psi(\bar{a}, \bar{y})$ is an intuitionistic tautology. Thus (4) gives (2) or (3), hence (1) is an intuitionistic tautology. □

In order to get an unconditional lower bound, one may try to prove a monotone version of the effective interpolation for the intuitionistic calculus. This should give a monotone circuit C in Corollary 4 for suitable formulas ϕ, ψ, χ. Thus we might get an exponential lower bound on the lengths of proofs of the tautologies on cliques and colorings of graphs, as we did in case of Resolution and Cutting Plane proofs.

The clique-coloring tautology says that it is not possible to have two mappings, one is from an m element set in the graph such that the image of the m element set is a clique, the other is a mapping from the graph such that no two vertices connected by an edge are mapped to the same element. Hence the composition of the two alleged mappings violates the PHP. Though the composition is definable in the intuitionistic calculus by a polynomial size formula and the properties of the two mappings ensure that it is one-to-one, it seems that the clique-coloring tautologies, in the form required by the interpolation theorem above, are not derivable from PHP tautologies using polynomial size intuitionistic proofs. If that was possible we could reduce proving a lower bound on PHP in the monotone sequent calculus to a lower bound on the clique-coloring tautologies in the intuitionistic propositional calculus.

Problem 4 *Does PHP have proofs of polynomial size in the intuitionistic sequent calculus?*

It is well-known that PHP has polynomial size proofs in the classical sequent calculus [8].

There are many more logics that are interesting from the point of view of the complexity of proofs. For instance, there is a calculus called *Positive Logic*, which is between monotone and intuitionistic logic. It uses the connectives $\wedge, \vee, \rightarrow$, thus it generalizes the monotone calculus by allowing more than one implication in a formula; see [40] for more information.

Acknowledgment

This paper resulted to a large extent from discussions with Vašek Chvátal, Jan Krajíček, László Lovász, Jiří Sgall and Gaisi Takeuti, which I appreciate very much. I am also grateful to Sam Buss for reading the manuscript and pointing out several corrections.

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, *An $O(n \log n)$ sorting network,* Proc. 15-th ACM Symp. on Theory of Computing, 1983

[2] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi and P. Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs,* Proc. London Math. Soc. (3) 73, 1996, 1-26

[3] Bonet, M., Pitassi, T. and Raz, R., *Lower bounds for Cutting Planes proofs with small coefficients,* Proc. 27-th STOC, 1995, 575-584.

[4] Bonet, M., Pitassi, T. and Raz, R., *No feasible interpolation for TC^0-Frege proofs,* Proc. 38-th FOCS, 1997, 254-263

[5] S. R. Buss, *Propositional proof complexity*, preprint, 1997

[6] S. Buss, R. Impagliazzo, J.Krajíček, P. Pudlák, A.A. Razborov and J. Sgall, *Proof complexity in algebraic systems and constant depth Frege systems with modular counting,* Computational Complexity 6, (1996/1997), 256-298

[7] S.R. Buss, G. Mints, *The complexity of the disjunction end existence properties in intuitionistic logic*, preprint, 1997

[8] S.R. Buss, *The propositional pigeonhole principle has polynomial size Frege proofs,* JSL 52, 916-27

[9] M. Clegg, J. Edmonds, R. Impagliazzo, *Using the Groebner basis algorithm to find proofs of unsatisfiability,* Proc. 28-th ACM STOC, 1996, 174-183

[10] V. Chvátal, *Edmonds polytopes and a hierarchy of combinatorial problems,* Discrete Math., 4 (1973), 305-337.

[11] V. Chvátal, *Some linear programing aspects of combinatorics,* in Proc. of the Conf. on Algebraic Aspects of Combinatorics, Toronto 1975, Utilitas Math. Publishing Inc., Winnipeg, 2-30.

[12] V. Chvátal, W. Cook, M. Hartmann, *On cutting plane proofs in combinatorial optimization,* Linear Algebra and Its Applications 114/115 (1989), 455-499.

[13] W. Cook, C.R. Coullard, and Gy. Turán, *On the complexity of Cutting Plane proofs*, Discrete Applied Mathematics 18, (1987), 25-38

[14] S.A.Cook and R.A. Reckhow, *The relative efficiency of propositional proof systems,* JSL 44, 1987, 25-38

[15] W. Craig, *Linear reasoning: A new form of the Herbrand-Gentzen theorem,* Journ. of Symb. Logic 22(3), (1957), 250-287

[16] W. Craig, *Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory,* Journ. of Symb. Logic 22(3), (1957), 269-285

[17] R.E. Gomory, *An algorithm for integer solutions of linear programs,* in Recent Advances in Mathematical Programming, eds. R.L. Graves and P. Wolfe, McGraw-Hill, 1963, 269-302

[18] G. Hajós, *Über eine Konstruktion nicht n-färbener Graphen,* Wiss. Zeitschr. M. Luther Univ. Halle-Wittenberg, A 10, 1961, 116-117

[19] A. Haken, *The intractability of resolution,* Theoretical Computer Science, 39, (1985), 297-308

[20] A. Haken, *Counting bottlenecks to show monotone $P \neq NP$,* Proc. 36-th Annual IEEE Symp. on Foundations of Computer Science, Milwaukee, 1995, 36-40

[21] A. Haken and S.A.Cook, *An exponential lower bound for the size of monotone real circuits*, J. of Computer and System Sciences, to appear

[22] R. Impagliazzo, T. Pitassi, *Interpolation for generalized cutting planes system,* preprint, 1996

[23] R. Impagliazzo, T. Pitassi, A. Urquhart, *Upper and lower bounds for tree-like cutting planes proofs,* Proc. 9-th Annual IEEE Symp. on Logic in Computer Science, 1994, 220-228

[24] R. Impagliazzo, P. Pudlák and J. Sgall, *Simplified lower bounds for the polynomial calculus,* Computational Complexity, to appear

[25] J. Krajíček, *Bounded Arithmetic, Propositional Logic and Complexity Theory,* Cambridge University Press 1995.

[26] J. Krajíček, *Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic,* Journ. of Symb. Logic 62/2, 1997, 457-486

[27] J. Krajíček, *On the degree of ideal membership proofs from uniform families of polynomials over a finite field,* submitted, 1997

[28] J. Krajíček, *A fundamental problem of mathematical logic,* Collegium Logicum, Annals of Kurt Gödel Society Vol. 2, 1996, 56-64

[29] J. Krajíček, *Discretely ordered modules as a first-order extension of the cutting planes proof system,* JSL, to appear

[30] J. Krajíček, *On methods for proving lower bounds in propositional logic,* M.L. Dalla Chiara et al. (eds.), Logic and Scientific Methods, Kluwer Acad. Publ., 69-83

[31] J. Krajíček and P. Pudlák, *Some consequences of cryptographical conjectures for S_2^1 and EF,* Information and Computation 140, 1998, 82-94.

[32] K. Iwama and T. Pitassi, *Exponential lower bound for the Tree-like Hajós Calculus,* 1997, preprint

[33] S-Y. R. Li and W-C. W. Li, *Independence numbers of graphs and generators of ideals,* Combinatorica 1,1981, 55-61

[34] L. Lovász and A. Schrijver, *Cones of matrices and set-functions and 0-1 optimization,* SIAM J. Optimization 1(2), 166-190

[35] D. Mundici, *NP and Craig's interpolation theorem,* Logic Colloquium 1982, North-Holland, 345-358

[36] T. Pitassi and A. Urquhart, *The complexity of the Hajós calculus,* Proc. 33-th Symp. on Foundations of Computer Science, IEEE, 1992, 187-196

[37] P. Pudlák, *Lower bounds for resolution and cutting planes proofs and monotone computations,* JSL 62/3, 1997, 981-998

[38] P. Pudlák, *The lengths of proofs,* in *Handbook of Proof Theory,* S. Buss ed., North-Holland, 1998, 547-637

[39] P. Pudlák and J. Sgall, *Algebraic models of computation and interpolation for algebraic proof systems,* in Proof Complexity and Feasible Arithmetics, P.W. Beame and S.R. Buss eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Science 39, 279-295

[40] H. Rasiowa, *An algebraic approach to non-classical logics,* PWN-Polish Scientific Publishers and North-Holland Publishing Company, 1974

[41] A.A. Razborov, *Lower bounds on the monotone complexity of some boolean functions,* Doklady Akad. Nauk SSSR 282, (1985), 1033-1037

[42] A.A. Razborov, *Unprovability of lower bounds on the circuit size in certain fragments of Bounded Arithmetic,* Izvestiya of the R.A.N. 59(1), (1995), 201-222; see also Izvestiya: Mathematics 59:1, 205-227.

[43] A.A. Razborov, *Lower bound for the polynomial calculus,* Computational Complexity, to appear

[44] L.G. Valiant, *Short monotone formulae for the majority function,* J. of Algorithms 5, 1984, 363-366