Lower Bounds for Propositional Proofs and Independence Results in Bounded Arithmetic

Alexander A. Razborov*

Steklov Mathematical Institute
Vavilova 42, 117966, GSP–1, Moscow, RUSSIA

Abstract. We begin with a highly informal discussion of the role played by Bounded Arithmetic and propositional proof systems in the reasoning about the world of feasible computations. Then we survey some known lower bounds on the complexity of proofs in various propositional proof systems, paying special attention to recent attempts on reducing such bounds to some purely complexity results or assumptions. As one of the main motivations for this research we discuss provability of extremely important propositional formulae that express hardness of explicit Boolean functions with respect to various non-uniform computational models.

1. Propositional proofs as feasible proofs of plain statements

Interesting and viable logical theories do not appear as result of sheer speculation. Conversely, they attempt to summarize and capture a certain amount of reasoning of a certain style about a certain class of objects that had existed in the math community before the mathematical logics entered the stage. For example, the set theory ZF was developed to distill those partial cases of the comprehension scheme (contradictory in full generality) that are really used in the common day work of a "practical mathematician". The aim of Peano Arithmetic PA was to capture that part of reasoning about integers which involves only finite objects, or at least can be in principle reduced to this form like some deep results using trigonometrical sums.

For many computer scientists, however, the world is usually even more restricted. Namely if we perform certain computation with an input binary string a, then all objects viewed during this computation not only are finite, but usually are required to have the bit length bounded a priori in terms of the length of a by some simple function like a polynomial or a quasipolynomial. Respectively, as a logical basis for the reasoning about this bounded world we would like to have a formal theory capable exactly of formalizing "common" arguments that may involve only those finite objects whose length is bounded in the length of a, and that, moreover, can be efficiently computed from this parameter. The exact

* Supported by the grant # 96-01-01222 of the Russian Foundation for Fundamental Research

meaning of efficient computability is determined by the class of computations we are trying to emulate in the context of Proof Theory.

A large variety of such theories appeared in the literature, most of them under the generic name *Bounded Arithmetic*. Naturally, the theories corresponding to (supposedly) different complexity classes are (also supposedly) different. One important empiric observation is that, vice versa, theories differently defined to capture the same class of computations tend to be isomorphic. For example, theories corresponding to the most basic world of time-bounded computations were independently defined in at least three different forms: Cook's equational theory PV [13], first order theories S^1_k and second order theories V^1_k [10]. It turned out, however, that PV is in some sense equivalent to S^1_2 [10, Chapter 6], and that S^1_k is simply isomorphic to (an inessential modification of) V^1_{k-1} [41, 29]. This robustness additionally suggests that we are on the right track in our quest for the theories of "feasible reasoning about feasible objects".

It is a common place in the Proof Theory that when we are interested in the provability of some formulae, the first question to ask is what is their logical complexity. This parameter typically measures the number of alternations of connectives or quantifiers and usually dictates which kind of techniques we should look for in our proof-theoretical studies. In the case of the theories of Bounded Arithmetic this helps us to draw a rather clear and natural distinction between what we are and what we are not going to do in this paper. Namely, there exists a rich and powerful *witnessing technique* for studying the provability of formulae that contain non-trivial bounded quantifiers, non-triviality meaning that they quantify over the full domain of objects whose length is comparable to the length of initial parameters. This technique is *not* considered in this paper, and the interested reader is referred e.g. to the monographs [10, 17, 22].

The only formulae we are dealing with in this paper are Σ^b_0-formulae. These are essentially the formulae in which all quantifiers are *sharply bounded* i.e., quantify over some domain whose *size* is comparable to the length of initial parameters.

The bad news about these formulae is that the previously known witnessing technique can not distinguish between their truth and provability and hence can be hardly used for studying them proof-theoretically. The good news is that the provability of Σ^b_0-formulae in theories of Bounded Arithmetic is closely related to the existence of short propositional proofs for certain propositional tautologies associated with the formula.

We do not give here exact definitions or details, they can be found e.g. in [22]. The best way for a complexity-oriented reader to imagine this correspondence is to invoke the familiar analogy with uniform vs. non-uniform computational models. A Σ^b_0-formula corresponds to a language, provability in Bounded Arithmetic is analogous to computability within specified amount of computational resources in some uniform model, and the length of propositional proofs for associated tautologies corresponds to the size of circuits computing restrictions of our language onto words of prescribed length.

The main purpose of the introductory part above was to convey to nonspecialists at least some feeling about the theory of feasible provability, and about the role played in this area by propositional proofs. We are not going to return to this topic (with a few minor exceptions). In comparison with first or second order formal theories, the model of propositional proof systems is much simpler to formulate and much cleaner combinatorially. Hence, similarly to Boolean circuits in the context of Computational Complexity, propositional proof systems provide a convenient and elegant framework for contemplating over lower bounds arguments, and explaining to a sufficiently broad audience the main ideas of what has been done. The latter task is exactly what we will try to do in the rest of the paper. Once again, the reader should bear in mind that our original motivation is to study the provability of plain ($= \Sigma_0^b$) statements by the amount of reasoning allowed in the world of feasibly computed objects (= in certain fragments of Bounded Arithmetic), and that this is basically equivalent to the study of complexity of propositional proofs.

2. Some concrete propositional proof systems

The most general definition of a propositional proof system was given in [14]:

Definition 1. Let $\mathcal{C}$ be a certain class of propositional formulae in variables $p_1, \ldots, p_n, \ldots$, and $\mathrm{TAUT}_{\mathcal{C}}$ be the set of all tautologies from the class $\mathcal{C}$ (if $\mathcal{C}$ is not specified, we assume by default that it consists of all bounded-fanin formulae in the standard language $\{0, 1, \neg, \vee, \wedge\}$ and abbreviate $\mathrm{TAUT}_{\mathcal{C}}$ to TAUT). A *propositional proof system* (p.p.s.) for the class $\mathcal{C}$ is a poly-time computable function P from $\{0,1\}^*$ *onto* $\mathrm{TAUT}_{\mathcal{C}}$. For a tautology $\phi \in \mathrm{TAUT}_{\mathcal{C}}$, any string w such that $P(w) = \phi$ is called a *P-proof of ϕ*.

Let $s_P(\phi)$ be the minimal possible length $|w|$ of a P-proof w of ϕ. A p.p.s. P is called *optimal* if $s_P(\phi)$ is bounded from above by a polynomial in $|\phi|$, uniformly for $\phi \in \mathrm{TAUT}_{\mathcal{C}}$. The following easy result, also from [14], indicates that in its full generality this definition is just a reformulation of the standard characterization of $co-\mathbf{NP}$ and has only little to do with the "real" proof theory:

Theorem 2. $\mathbf{NP} = co-\mathbf{NP}$ *if and only if there exists an optimal propositional proof system.*

In this paper, however, we will consider only natural proof systems, and we are primarily interested in proving their non-optimality. This is equivalent to obtaining lower bounds on $s_P(\phi_n)$ for *some* sequence of tautologies $\{\phi_n\}$. As we will see many times throughout this paper, there is a striking analogy between this task (and approaches to it) and the similar task of obtaining lower bounds on the complexity of Boolean functions. Here is one place where this analogy fails: for propositional proofs there does not seem to exist any analogue of the statement that almost all Boolean functions are hard, and the question whether the sequence ϕ_n should consist of "explicit" or arbitrary tautologies does not seem to be too relevant.

The following definition allows us to compare different p.p.s. by their strength:

Definition 3. Let P_0, P_1 be propositional proof systems for some classes $\mathcal{C}_0, \mathcal{C}_1$ of formulae respectively, and assume that $\mathcal{C}_0 \subseteq \mathcal{C}_1$. We say that P_1 *polynomially simulates* P_0 if there is a poly-time computable function $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ such that $P_0(w) = P_1(f(w))$ for all $w \in \{0,1\}^*$. Two proof systems for the same class of formulae are *polynomially equivalent* if they polynomially simulate each other.

Notice that if P_0 is polynomially simulated by P_1 then it has a *polynomial speed-up* over P_1, that is $s_{P_1}(\phi) \leq s_{P_0}(\phi)^{O(1)}$, $\phi \in \mathrm{TAUT}_{\mathcal{C}_0}$. Vice versa, in all known cases when one natural p.p.s. has a polynomial speed-up over another p.p.s., this is due to the existence of some (also natural) polynomial simulation.

As the most basic example of a p.p.s. take the ordinary Hilbert-style propositional calculus from your favourite textbook in mathematical logics. It is based upon some finite number of axiom schemes and inference rules like modus ponens and can be easily converted into a p.p.s. F in the sense of Definition 1 as follows. Let $F(w)$ be the final tautology in w if w is some (encoding of) legal inference in our calculus. If w is a meaningless word, we let $F(w) \rightleftharpoons 1$. This p.p.s. F is called *Frege proof system.*

At the first sight, this definition is somewhat ambiguous as there are several variants of the propositional calculus (almost as many as textbooks). However, the following theorem [35] shows that the differences between them are actually inessential:

Theorem 4. *If the language of some Frege system F_1 contains the language of another Frege system F_0, then F_1 polynomially simulates F_0. In particular, every two Frege systems in the same language are equivalent.*

Coming back for a moment to the discussion from the previous section, Frege proofs correspond to (non-uniform) class $\mathbf{NC}^1$ in the sense that they allow plain reasoning about $\mathbf{NC}^1$-predicates (= predicates expressible by small propositional formulae). All p.p.s. considered in this paper follow the same pattern for different complexity classes, and always allow straight-line proofs (that is, every deduced formula can be used more than once in forthcoming inferences). Missing details of definitions as well as more information about these p.p.s. and their modifications can be found e.g. in [22, 44].

Resolution. This proof system was introduced in [8] and further developed in [16, 38]. Let $\mathcal{C}$ be the class of all disjunctive normal forms. A *resolution proof* of a tautology $\phi = (K_1 \vee \ldots \vee K_m)$ from $\mathrm{TAUT}_{\mathcal{C}}$ is actually a resolution refutation of the set $\{D_1, \ldots, D_m\}$, where D_i is the *clause* (elementary disjunction) that is the negation of the elementary conjunction K_i. In turn, a *resolution refutation* of a set of clauses is an inference of the empty clause 0 from this set in the calculus with the only *resolution rule*

$$\frac{D \vee p \qquad E \vee (\neg p)}{D \vee E}.$$

We denote this proof system by R.

Bounded depth Frege systems. Let $d \geq 2$ be a fixed constant. F_d is the p.p.s. defined similarly to the ordinary Frege system F with the exception that it operates with (unbounded fan-in) formulae of depth at most d over the standard basis $\{0, 1, \neg, \vee, \wedge\}$. Axioms and inference rules are modified in a natural way so that they take care of unbounded fan-in.

We will also consider extensions of F_d with axiom schemes $Count_m$, where m is some fixed integer, expressing that no universe of cardinality not divisible by m can be partitioned into m-sets. An even stronger system is obtained if we append to our language the connective MOD_m of counting modulo m, along with natural axioms and inference rules expressing its basic properties. This system will be denoted by $F_d(MOD_m)$.

Cutting planes ([15]). These generalize resolutions and are defined similarly with the exception that this time K_i (and hence D_i) have the form of arbitrary inequalities of the form $a_1p_1 + \cdots + a_np_n \geq T$, where the coefficients $a_1, \ldots, a_n, T$ are integer numbers, and p_i are treated as $(0,1)$-valued variables. This system has a number of obvious axioms and inference rules, and just one less straightforward *division rule*

$$\frac{a_1cp_1 + \cdots + a_ncp_n \geq T}{a_1p_1 + \cdots + a_np_n \geq \lceil T/c \rceil},$$

where $a_1, \ldots, a_n, c, T$ are integers and $c > 0$ (its non-triviality stems from rounding up rather than down). By analogy with threshold circuits (see e.g. [30]), cutting planes come in two different versions. Namely, we can write the coefficients $a_1, \ldots, a_n, T$ in unary (the case of *small weights*) or in binary (*arbitrary weights*). The corresponding p.p.s. will be denoted by CP^*, CP respectively.

Extended Frege system, denoted EF [13]. We enlarge the ordinary Frege system by allowing it to introduce *extension axioms* of the form $(p \equiv A)$, where A is a formula, and p is a new *extension atom* that did not occur previously in the proof. This is an extremely powerful and probably the most important propositional proof system. The reason is that it corresponds to the complexity class $\mathbf{P}/poly$: roughly speaking, what extension atoms and axioms do, they allow us to evaluate arbitrary Boolean circuits.

There are many polynomial simulations between natural propositional proof systems, their numerous modifications etc. For p.p.s. introduced above there are no real surprises on the map of known simulations between them: it completely mimics the map of known containments between underlying complexity classes, see Figure 1. [44, Figure 1] contains more remarkable landmarks in this neighborhood.

3. Algebraic and combinatorial machinery borrowed from Boolean complexity

When superpolynomial lower bounds are proved for some class of Boolean circuits, the machinery developed for that purpose usually conveys much more

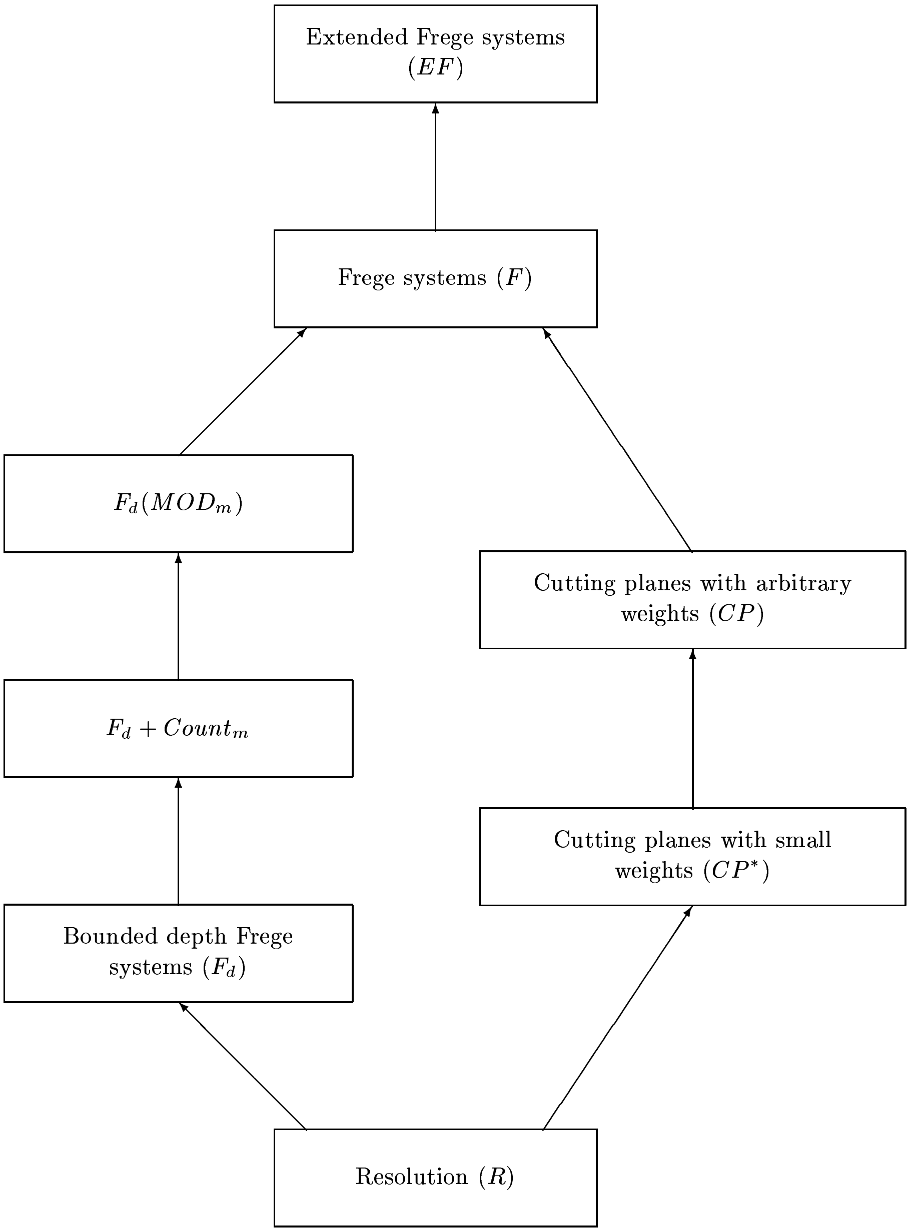

Fig. 1. Map of known simulations

information. In many cases this lead us to a rather clear understanding of what, how and why can or cannot be computed by small circuits from this class. Thus, it is natural to try to apply this or similar machinery to propositional proofs that operate with tautologies expressible by circuits already understood in this way.

In some cases this analogous approach to proving lower bounds on the complexity of propositional proofs turned out to be fruitful. Exponential lower bounds were consequently established for resolutions [42, 18, 43, 12], bounded depth Frege systems [1, 7, 21, 25, 26, 2, 6, 36] and their extensions $F_d + Count_m$ [3, 5, 37, 11].

We do not present here these important results in more details as this is already quite successfully done e.g. in [22, 44]. We only remark that our experience gathered in this field strictly suggests that the problem of proving lower bounds on the complexity of propositional proofs is usually much harder than the similar problem for the underlying circuit class, and there are no obvious generalizations to the case of p.p.s.

Lower bounds for resolutions are treated as deep and ingenious results, whereas lower bounds for DNF is something completely trivial. Even with Håstad Switching Lemma in hand [20] it took a lot of work to adopt it for constant-depth propositional proofs, and even more work to prove lower bounds for the extension $F_d + Count_m$. Moreover, looking closely at Figure 1, we might expect lower bounds for cutting planes and the system $F_d(MOD_p)$, p a prime, as such bounds are known for the corresponding circuit models.

Lower bounds for cutting planes will be presented in the next section, but they are based on ideas totally different from the machinery used in the theory of threshold circuits. No "combinatorial" proof of lower bounds for cutting planes is currently known. The situation with the system $F_d(MOD_p)$ is even worse: the question of its optimality is still open. In the recent paper [11] this question was reduced to lower bounds on the degree of coefficients in a certain "extended" version of one partial case of Hilbert's Nullstellensatz. This reduction emulates in the context of propositional proofs the main lemma from [28, 40] on approximating $ACC^0[p]$-circuits by low degree polynomials. The remaining step, however (proving lower bounds on the degrees for this algebraic problem) is still elusive.

We conclude this section with mentioning another recent paper [19] that provides one of the rare examples of influence in another direction. Namely, in that paper combinatorial ideas previously used for resolutions in [18] were successfully employed in Boolean complexity to provide a new elegant method of obtaining exponential lower bounds on the monotone circuits size of explicit Boolean functions.

4. Interpolation theorems and disjoint NP-pairs

Given our inability to prove superpolynomial lower bounds on the size of Boolean formulae or circuits computing explicit Boolean functions, and observations made in the previous section, we can hardly expect a "combinatorial" proof of non-optimality for strong p.p.s. like F or EF. In this section we present another approach that is more akin to the witnessing technique mentioned in Section 1 and looks more promising.

The general idea of this approach is not to try to analyze directly potential propositional proofs but rather to extract from them some unlikely algorithmic consequences in the real world. This, if successful, would give us *conditional* statements about non-optimality of p.p.s. modulo complexity assumptions saying that the consequences extracted from the proofs actually do not take place. Roughly speaking, if lower bounds for propositional proofs must necessarily be at least as hard as complexity lower bounds (and the latter are currently inaccessible), let us at least show that they are *just* as hard!

One successful scheme fulfilling this idea for substantially weaker p.p.s. appeared, implicitly and independently, in [32, 9]. More explicit and slightly different treatments of this scheme were later given in [23, 33], and in our presentation we follow an intermediate course between them.

Let $U, V \subseteq \{0,1\}^*$ be two disjoint $\mathbf{NP}$-sets, and let us arbitrarily fix their $\mathbf{NP}$-representations

$$\left.\begin{array}{l} x \in U \equiv \exists y \in \{0,1\}^{p(n)} A_n(x,y), \\ x \in V \equiv \exists z \in \{0,1\}^{p(n)} B_n(x,z), \end{array}\right\} \tag{1}$$

$n = |x|$, where $A_n(\mathbf{p}, \mathbf{q})$, $B_n(\mathbf{p}, \mathbf{r})$ are propositional formulae of polynomial in n size. Then $U \cap V = \emptyset$ implies that for every n, $\neg A_n(\mathbf{p}, \mathbf{q}) \vee \neg B_n(\mathbf{p}, \mathbf{r})$ is a tautology and hence provable in the propositional calculus. This tautology can be re-written in the form $B_n(\mathbf{p}, \mathbf{q}) \supset \neg A_n(\mathbf{p}, \mathbf{r})$, and Craig's Interpolation Lemma (which, although, amounts to something completely trivial in the propositional case) guarantees us the existence of a formula $C_n(\mathbf{p})$ called an *interpolant* that depends on $\mathbf{p}$-variables only and such that both $B_n(\mathbf{p}, \mathbf{q}) \supset C_n(\mathbf{p})$ and $C_n(\mathbf{p}) \supset \neg A_n(\mathbf{p}, \mathbf{r})$ are provable. Semantically this means that the set $L \rightleftharpoons \{x \mid C_n(x_1, \ldots, x_n), n = |x|\}$ has the property $U \cap L = \emptyset$, $V \subseteq L$, i.e., it *separates* U and V.

Suppose now we additionally know that the tautology $\neg A_n(\mathbf{p}, \mathbf{q}) \vee \neg B_n(\mathbf{p}, \mathbf{r})$ has a *short* proof in some p.p.s. P (informally speaking, this means that P can easily prove the disjointness of U and V). Then we might expect that in this case something could be additionally said about the *complexity* of the interpolant C_n, i.e., we would have some constructive form of the interpolation theorem. And then we could argue another way around: if U and V can *not* be separated by any set L of the complexity prescribed by the interpolation theorem, then the corresponding tautologies $\neg A_n(\mathbf{p}, \mathbf{q}) \vee \neg B_n(\mathbf{p}, \mathbf{r})$ do not have short P-proofs, and, thus, P is not optimal.

Lower bounds based upon this idea independently appeared in [32] (for the system R in the uniform framework), and in [9] (for CP^*). [27] established the interpolation theorem for cutting planes with arbitrary coefficients, and this is the strongest system for which it is currently known:

Theorem 5. *There exists a polynomial time algorithm which does the following. Given a CP-refutation of some set of clauses*

$$\{ A_i(\mathbf{p}, \mathbf{q}) \mid i \in I \} \cup \{ B_j(\mathbf{p}, \mathbf{r}) \mid j \in J \},$$

where all variables occurring in A_i, B_j are explicitly displayed, the algorithm produces a Boolean circuit $C(\mathbf{p})$ that computes an interpolant for $A(\mathbf{p}, \mathbf{q}) \rightleftharpoons \bigwedge_{i \in I} A_i(\mathbf{p}, \mathbf{q})$ and $B(\mathbf{p}, \mathbf{r}) \rightleftharpoons \bigwedge_{j \in J} B_j(\mathbf{p}, \mathbf{r})$ in the above sense.

In particular, if the size of the original CP-refutation is polynomial in the number n of variables in $\mathbf{p}$, the same is true for the size of $C(\mathbf{p})$. Therefore, if there exist two disjoint **NP**-sets U and V that can not be separated by any set in $\mathbf{P}/poly$, then the cutting planes system (and any forthcoming p.p.s. for which we might manage to prove a similar interpolation theorem) is not optimal. The sequence of hard tautologies would have the form $\neg A_n(\mathbf{p}, \mathbf{q}) \vee \neg B_n(\mathbf{p}, \mathbf{r})$, where A_n, B_n are arbitrary CNF of polynomial size representing U, V in the sense of (1).

The existence of such pairs (U, V) follows from either $\mathbf{NP} \cap co{-}\mathbf{NP} \not\subseteq \mathbf{P}/poly$ (for trivial reasons) or $\mathbf{UP} \not\subseteq \mathbf{P}/poly$ (see [39, Theorem 9]). In the next section we will discuss some concrete pairs that are likely to fulfill this assumption.

But the monotone analogue of this assumption *is* known, although the proof is rather hard [4]. Quite remarkably, a *monotone* version of Theorem 5 allows us to obtain *unconditional* lower bounds for cutting planes based upon this knowledge.

To be more specific, assume that the set U is an ideal w.r.t. the natural partial ordering on $\{0,1\}^*$ given by $x \leq y \rightleftharpoons (|x| = |y| \ \& \ \forall i \leq |x| (x_i \leq y_i))$, and V is a filter w.r.t. the same ordering. Assume also that the representation (1) witnesses these monotonicity properties in the sense that $A_n(\mathbf{p}, \mathbf{q})$ contains $\mathbf{p}$-variables only negatively, and $B_n(\mathbf{p}, \mathbf{r})$ contains them only positively. Then one might hope that the short circuit whose existence is guaranteed by Theorem 5 can be additionally guaranteed to be monotone.

This is indeed so for the restricted version CP^* of cutting planes [9] which immediately implied in that paper exponential lower bounds on $s_{CP^*}(\phi_n)$ for some tautologies ϕ_n. More specifically, let propositional variables p_{ij} $(1 \leq i < j \leq n)$ encode in a natural way an undirected graph on n vertices, and let $Colour_n(\mathbf{p}, \mathbf{q})$ be a poly-sized CNF that contains $\mathbf{p}$ only negatively and expresses that $\mathbf{q}$ is a proper $(m-1)$-colouring of this graph, $m \rightleftharpoons \lfloor \frac{1}{8}(n/\log n)^{2/3} \rfloor$. Similarly, let $Clique_n(\mathbf{p}, \mathbf{r})$ contain $\mathbf{p}$ only positively and say that $\mathbf{r}$ is an m-clique in the graph represented by $\mathbf{p}$. It is the main result of [4] that every monotone circuit separating the sets $\{ x \mid |x| = n \ \& \ \exists y \ Colour_n(x, y) \}$ and $\{ x \mid |x| = n \ \& \ \exists z \ Clique_n(x, z) \}$ must have size $2^{\Omega\left((n/\log n)^{1/3}\right)}$. Hence:

Theorem 6. *Every CP^*-proof of the tautology $\neg Clique_n(\mathbf{p}, \mathbf{q}) \vee \neg Colour_n(\mathbf{p}, \mathbf{r})$ must have size $2^{\Omega\left((n/\log n)^{1/3}\right)}$.*

The situation with cutting planes proofs having arbitrary coefficients is slightly more complicated. For this case it is not known whether there always exists an interpolant $C(\mathbf{p})$ computable by ordinary monotone circuits of polynomial size. However, Pudlák [27] introduced some natural generalization of Boolean monotone circuits which he called *monotone circuits over reals*, and showed that a poly-sized interpolant for CP-proofs can be constructed in this broader class. The second main result of [27] (which is also of independent interest in "pure" Complexity Theory) is a generalization of the Alon-Boppana bound to the case of monotone circuits over reals. Altogether this implies the extension of Theorem 6 to cutting planes with arbitrary coefficients. No "direct" combinatorial proof of non-optimality for CP, or even for CP^* is currently known.

5. Tautologies expressing hardness of Boolean functions

So far we were interested in general methods for showing lower bounds on the complexity of propositional proofs paying only little attention to the look of tautologies for which these bounds are attained. On the contrary, in this section we study the proof complexity for quite concrete and extremely important propositional formulae expressing major results and central open problems in Computational Complexity.

Fix some parameters n and $t = t(n) \leq 2^n$. Let $\mathbf{p} \rightleftharpoons (p_x \,|\, x \in \{0,1\}^n)$ be a vector of propositional variables of length 2^n encoding the truth-table of a Boolean function in n variables, and $Circuit_{t,n}(\mathbf{p},\mathbf{q})$ be a CNF of size $2^{O(n)}$ expressing that $\mathbf{q}$ encodes a Boolean circuit of size at most t that computes this function. As we require the size to be polynomial only in 2^n, not in n, constructing such a CNF presents no difficulties. For example, $\mathbf{q}$ can simply encode all instructions of the circuit as well as truth-tables of all intermediate results. Like in Computational Complexity, exact details of this encoding are unimportant for our purposes.

Now, $\mathbf{NP} \overset{?}{\subseteq} \mathbf{P}/poly$ is equivalent to the question if $\neg Circuit_{t(n),n}(s_n, \mathbf{q})$ are tautologically true for some function $t(n)$ not bounded by any polynomial, and an arbitrary $\mathbf{NP}$-complete function $\{s_n\}$ (for definiteness, SATISFIABILITY). Moreover, what Boolean complexity has been basically doing over last 30 years was trying to prove, with the help of the algebraic and combinatorial methods mentioned in Section 3, propositional formulae of the form $\neg Circuit^*_{t(n),n}(f_n, \mathbf{q})$ for explicit functions f_n, integer-valued $t(n)$ that are as large as possible, and $Circuit^*_{t,n}$ corresponding to some restricted class of Boolean circuits.

One more face of the already strong connections existing between propositional proofs and Boolean circuits was observed in [31], where I proposed the thesis that *in all known cases of success achieved in proving propositional formulae of the form* $\neg Circuit^*_{t(n),n}(f_n, \mathbf{q})$, *this proof is actually an EF-proof*[2] *of size* $2^{O(n)}$. This immediately gives raise to the following natural ques-

[2] Strictly speaking, [31] deals with some second order theories $V_1^0(\delta)$ of Bounded Arithmetic, but all considerations from there translate to propositional proof systems as sketched at the end of Section 1. In fact, only a few proofs in Boolean complexity use the full strength of the Extended Frege system: many major results already have

tion: since we are currently unable to prove things like $\neg Circuit_{n^2,n}(s_n, \mathbf{q})$ or $\neg Formula_{n^{10},n}(s_n, \mathbf{q})$, then perhaps we should think in another direction and try to show that these supposed tautologies significantly differ from their already proven restricted versions and do not possess short propositional proofs at all. And the first natural thing to wonder about this question: is there any hope to *prove* something intelligent about it provided we *believe* that in reality things like $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ take place but are extremely hard to prove?

The hope to show with a direct combinatorial or algebraic argument that $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ does not have short EF-proofs or F-proofs seems to be even more vain than the hope to prove non-optimality of these proof systems using arbitrary tautologies. Indeed, it finally may happen (although it seems more and more unlikely – see [34] for one possible explanation) that we significantly underestimate the potential of this machinery, and it will eventually prove $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ and then non-optimality of EF. But even in that case, given the main thesis from [31], the first step in this program would probably give a *short EF-proof* of $\mathbf{NP} \not\subseteq \mathbf{P}/poly$, and with all our nice machinery in hands we could not establish strong lower bounds on $s_{EF}(\neg Circuit_{t,n}(s_n, \mathbf{q}))$ simply for the reason these bounds are not true!

On the other hand, it seems that "witnessing" arguments from Section 4, if successful at all, tend to be perfectly applicable to supposed tautologies like $\neg Circuit_{t,n}(s_n, \mathbf{q})$ since the latter are of "universal" nature and have a lot of useful structure hidden inside. Let us show, for example, how to associate to these tautologies some natural pair of $\mathbf{NP}$-sets that presumably can not be separated by a set in $\mathbf{P}/poly$.

Fix any sufficiently constructive super-polynomially growing function $t(n)$, and let the $\mathbf{NP}$-set $SIMPLE_t$ consist of all truth-tables f_n of Boolean functions in n variables that are computable by a circuit of size at most $t(n)$. Then

$$f_n \in SIMPLE_t \equiv \exists y \in \{0,1\}^{p(n)} Circuit_{t(n),n}(f_n, y)$$

for some polynomial $p(n)$. Let $s = \{s_n \mid n \in \omega\}$ be a sufficiently constructive sequence of Boolean functions, and consider also the shifted version $SIMPLE_t^{\oplus s}$ given by

$$f_n \in SIMPLE_t^{\oplus s} \equiv \exists z \in \{0,1\}^{p(n)} Circuit_{t(n),n}(f_n \oplus s_n, z).$$

The following is an easy consequence of the main result from [34] observed in [32]:

Theorem 7. *If there exists a pseudorandom number generator $G_k : \{0,1\}^k \longrightarrow \{0,1\}^{2k}$ in $\mathbf{P}/poly$ that is secure against attack by 2^{k^ϵ}-sized circuits for some fixed $\epsilon > 0$, then $SIMPLE_t$ and $SIMPLE_t^{\oplus s}$ can not be separated by any set computable by circuits of quasipolynomial size.*

---

short F-proofs, and some of them even F_d-proofs for a fixed reasonable d.

In combination with Theorem 5, this implies lower bounds $2^{n^{\omega(1)}}$ on the length of any CP-proof of the formula

$$\neg Circuit_{t(n),n}(\mathbf{p},\mathbf{q}) \vee \neg Circuit_{t(n),n}(\mathbf{p}^{\oplus s_n},\mathbf{r}),$$

where $\mathbf{p}^{\oplus s_n}$ has the obvious meaning[3], modulo the same cryptographic assumption as in Theorem 7. This formula, however, has an easy propositional proof from an instance of $\neg Circuit_{4t(n)+3,n}(s_n,\mathbf{q})$ obtained by a formalization of the obvious construction that takes XOR of one $t(n)$-sized circuit $\mathbf{q}$ computing some function $\mathbf{p}$ with another such circuit computing $\mathbf{p}^{\oplus s_n}$ giving a $(4t(n)+3)$-sized circuit that computes s_n. Putting things together, and observing that our argument does not actually use the constructiveness of $t(n), s_n$, we get:

Theorem 8. *If there exists a pseudorandom number generator $G_k : \{0,1\}^k \longrightarrow \{0,1\}^{2k}$ in $\mathbf{P}/poly$ that is secure against attack by 2^{k^ϵ}-sized circuits for some fixed $\epsilon > 0$, then for every super-polynomially growing function $t(n)$ and every sequence of Boolean functions $\{s_n \mid n \in \omega\}$, the formulae $\neg Circuit_{t(n),n}(s_n,\mathbf{q})$ do not possess CP-proofs of size $2^{n^{O(1)}}$.*

This conditional lower bound is true for any sequence $\{s_n\}$. As observed by Avi Wigderson (in the context of Natural Proofs – see the journal version of [34]), for some specific s_n we can obtain *unconditional* results of this sort. Suppose for example that B_n is a hard bit of the discrete logarithm problem. Then for sufficiently large $t(n)$ (certainly, $t(n) = 2^{n^\epsilon}$ would do for any fixed $\epsilon > 0$) the formulae $\neg Circuit_{t(n),n}(B_n,\mathbf{q})$ do not possess quasipolynomial size CP-proofs, *without any unproven complexity assumptions.* The reason, roughly speaking, is that if the discrete logarithm function is hard, we apply Theorem 8 with G_k based on this function, and if it is easy then $\neg Circuit_{t(n),n}(B_n,\mathbf{q})$ are not tautologies and do not have any CP-proof at all. Of course, this argument is highly non-constructive, essentially uses the law of the excluded middle and does *not* imply non-optimality of CP since we do not know for sure whether $\neg Circuit_{t(n),n}(B_n,\mathbf{q})$ are really tautologies.

6. Some directions for future research

As we observed in Section 3, there still remains one natural p.p.s., namely $F_d(MOD_p)$, p a prime, for which the traditional algebraic and combinatorial machinery has very good chances to succeed in proving non-optimality. That would be very nice to obtain such a result as this would practically equalize the achievements of this machinery in Computational Complexity and in Proof Theory.

One bad news about the interpolation theorem is that its extension to the system EF turned out to be highly unlikely. Namely, [24] gave an example of

[3] Notice that if the function s_n is actually easy, then this formula has no CP-proof at all for the trivial reason it is not a tautology.

two disjoint **NP**-sets such that the fact of their disjointness *has* poly-size EF-proofs but which can not be separated by a set in $\mathbf{P}/poly$ if the cryptosystem RSA is secure. Hence, the analogue of Theorem 5 for EF could be used for a successful cryptoattack to break RSA. Despite this discouraging fact, the general approach of extracting some unlikely algorithmic consequences from potential propositional proofs still looks (in my opinion) promising.

For example, suppose we manage to show that every poly-size EF-proof (or F-proof) of any tautology of the form $\phi(\mathbf{q}) \vee \psi(\mathbf{r})$ implies the *existence* of a poly-size EF-proof for either $\phi(\mathbf{q})$ or $\psi(\mathbf{r})$ (but in general we can neither construct this proof efficiently nor even indicate for which of the two parts it exists). Notice that this is true if *exactly* one of the components $\phi(\mathbf{q})$, $\psi(\mathbf{r})$ is a tautology, simply by substituting into the original proof an arbitrary falsifying assignment for another component, and that at the moment this assumption does not seem to contradict any piece of our complexity intuition. Then the optimality of EF would imply, similarly to Section 4, that every two disjoint **NP**-sets can be separated by a disjoint pair of $co-\mathbf{NP}$ sets. This would have almost as striking consequences for the tautologies $\neg Circuit_{t,n}(f_n, \mathbf{q})$ discussed in Section 5 as the "strong" version of the interpolation theorem for EF.

References

1. M. Ajtai. The complexity of the pigeonhole principle. In *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, pages 346–355, 1988.
2. M. Ajtai. Parity and the pigeonhole principle. In S. R. Buss and P. J. Scott, editors, *Feasible Mathematics*, pages 1–24. Birkhauser, 1990.
3. M. Ajtai. The independence of the modulo p counting principle. In *Proceedings of the 26th ACM STOC*, pages 402–411, 1994.
4. N. Alon and R. Boppana. The monotone circuit complexity of Boolean functions. *Combinatorica*, 7(1):1–22, 1987.
5. P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. To appear in *Proc. of the London Math. Soc.*, 1994.
6. P. Beame and T. Pitassi. Exponential separation between the matching principles and the pigeonhole principle. Submitted to *Annals of Pure and Applied Logic*, 1993.
7. S. Bellantoni, T. Pitassi, and A. Urquhart. Approximation of small depth Frege proofs. *SIAM Journal on Computing*, 21(6):1161–1179, 1992.
8. A. Blake. *Canonical expressions in Boolean algebra.* PhD thesis, University of Chicago, 1937.
9. M. Bonet, T. Pitassi, and R. Raz. Lower bounds for cutting planes proofs with small coefficients. In *Proceedings of the 27th ACM STOC*, pages 575–584, 1995.
10. S. R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.
11. S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. Submitted to *Computational Complexity*, 1996.
12. V. Chvátal and E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35(4):759–768, 1988.

13. S. A. Cook. Feasibly constructive proofs and the propositional calculus. In *Proceedings of the 7th Annual ACM Symposium on the Theory of Computing*, pages 83–97, 1975.
14. S. A. Cook and A. R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.
15. W. Cook, C. R. Coullard, and G. Turán. On the complexity of cutting plane proofs. *Discrete Applied Mathematics*, 18:25–38, 1987.
16. M. Davis and H. Putnam. A computing procedure for quantification theory. *Journal of the ACM*, 7(3):210–215, 1960.
17. P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic.* Springer-Verlag, 1993.
18. A. Haken. The intractability or fesolution. *Theoretical Computer Science*, 39:297–308, 1985.
19. A. Haken. Counting bottlenecks to show monotone $\mathbf{P} \neq \mathbf{NP}$. In *Proceedings of the 36th IEEE FOCS*, 1995.
20. J. Håstad. *Computational limitations on Small Depth Circuits.* PhD thesis, Massachusetts Institute of Technology, 1986.
21. J. Krajíček. Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73–86, 1994.
22. J. Krajíček. *Bounded arithmetic, propositional logic and complexity theory.* Cambridge University Press, 1994.
23. J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. To appear in *Journal of Symbolic Logic*, 1994.
24. J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S_2^1 and EF. To appear in the Proceedings of the meeting *Logic and Computational Complexity*, Ed. D. Leivant, 1995.
25. J. Krajíček, P. Pudlák, and A. R. Woods. Exponential lower bounds to the size of bounded depth frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7(1):15–39, 1995.
26. T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993.
27. P. Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. Submitted to *Journal of Symbolic Logic*, 1995.
28. А. А. Разборов. Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения. *Матем. Зам.*, 41(4):598–607, 1987. A. A. Razborov, Lower bounds on the size of bounded-depth networks over a complete basis with logical addition, *Mathem. Notes of the Academy of Sci. of the USSR*, 41(4):333-338, 1987.
29. A. Razborov. An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 247–277. Oxford University Press, 1992.
30. A. Razborov. On small depth threshold circuits. In *Proceedings of the SWAT 92, Lecture Notes in Computer Science,* 621, pages 42–52, New York/Berlin, 1992. Springer-Verlag.
31. A. Razborov. Bounded Arithmetic and lower bounds in Boolean complexity. In P. Clote and J. Remmel, editors, *Feasible Mathematics II. Progress in Computer Science and Applied Logic, vol.* 13, pages 344–386. Birkhaüser, 1995.

32. A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic. *Изв. АН СССР, сер. матем.* (*Izvestiya of the RAN*), 59(1):201–222, 1995. See also *Izvestiya: Mathematics 59:1, 205-227.*
33. A. Razborov. On provably disjoint **NP**-pairs. Technical Report RS-94-36, Basic Research in Computer Science Center, Aarhus, Denmark, 1994.
34. A. Razborov and S. Rudich. Natural proofs. To appear in *Journal of Computer and System Sciences* (for the preliminary version see *Proceedings of the 26th ACM Symposium on Theory of Computing*, pp. 204-213), 1994.
35. R. A. Reckhow. On the lengths of proofs in the propositional calculus. Technical Report 87, University of Toronto, 1976.
36. S. Riis. *Independence in Bounded Arithmetic.* PhD thesis, Oxford University, 1993.
37. S. Riis. Count(q) does not imply Count(p). Technical Report RS-94-21, Basic Research in Computer Science Center, Aarhus, Denmark, 1994.
38. J. A. Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, 1965.
39. A. L. Selman. Complexity issues in cryptography. *Proceedings of Symposia in Applied Mathematics*, 38:92–107, 1989.
40. R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, pages 77–82, 1987.
41. G. Takeuti. *RSUV* isomorphisms. In P. Clote and J. Krajíček, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 364–386. Oxford University Press, 1992.
42. Г. С. Цейтин. О сложности вывода в исчислении высказываний. In А. О. Слисенко, editor, *Исследования по конструктивной математике и математической логике,* II*; Записки научных семинаров ЛОМИ, т. 8*, pages 234–259. Наука, Ленинград, 1968. Engl. translation: G. C. Tseitin, On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic, Part II*, ed. A. O. Slissenko, pp. 115-125.
43. A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.
44. A. Urquhart. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 1:425–467, 1995.

This article was processed using the LaTeX macro package with LLNCS style