On methods for proving lower bounds in propositional logic

Jan Krajíček*

Mathematical Institute of the Academy of Sciences
Žitná 25, Praha 1, 115 67, Czech Republic

This paper is based on my lecture [26]. It examines the problem of proving non-trivial lower bounds for the length of proofs in propositional logic from the perspective of methods available rather than surveying known partial results (i.e., lower bounds for weaker proof systems). We discuss neither motivations for proving lower bounds for propositional logic nor relations to other problems in logic or complexity theory. The reader is referred to [20] for the background information (as well as for all details missing in this paper). The paper is aimed at curious non-specialists. The style of our exposition is accordingly informal at places and we do not burden the text (especially in the introduction) with exhausting references not directly related to our main objective. The reader starving for details can find them, together with all original references, in [20] (see also expository articles [25, 32]).

Introduction

The language of propositional calculus contains constants 0 and 1 (false and true), connectives $\neg$, $\vee$ and $\wedge$ with their usual meaning, and atoms $p_0, p_1, \ldots$.

A propositional calculus is given by a finite number of axiom schemes (like $A \vee \neg A$) and schematic inference rules (like modus ponens: from A and $\neg A \vee B$ infer B). The only requirement is that the axioms and rules are sound and implicationally complete (i.e., if B is a tautological consequence of $A_1, \ldots A_k$ then B is provable from $A_1, \ldots, A_k$). Calculi of this type are called *Frege systems* after [9]. Fix one of them and call it F.

The complexity of a proof (tacitly a proof in F) is measured by two important functions: the number of proof steps and the size, i.e., the total number of symbols in the proof. These functions yield two measures of complexity of a tautology τ, namely $k_F(\tau)$ and $s_F(\tau)$, the minimal number of steps in a proof

*Partially supported by the *US - Czechoslovak Science and Technology Program* grant # 93025, and by the grant #119107 of the *AV ČR*.

of τ and the minimal size of a proof of τ respectively. Important observation is that if we augment F by the substitution rule (allowing to infer any substitution instance of an already proved formula in one step) then these two measures become essentially equal. The same effect has the extension rule (allowing to abbreviate formulas in a proof). None of these rules is schematic in the same sense as is modus ponens.

Now we are in a position to state the main problem.[1]

> **Problem:** Show that there is no polynomial $p(x)$ such that for a Frege system F it holds $k_F(\tau) \leq p(n)$, for every n and every tautology τ of size at most n.

The set of tautologies $TAUT$ is $coNP$-complete and a proof of τ with k steps can be coded by a string of size $O(k + |\tau|)$ (this is non-trivial, cf. [20, Lemmas 4.5.3 and 4.5.7]). Hence a Frege system can be thought of as a non-deterministic acceptor of $TAUT$ and the existence of a polynomial bounding the number of steps in proofs would imply that $TAUT \in NP$. Thus, unless the generally accepted conjecture that $NP \neq coNP$ fails, indeed no such polynomial $p(x)$ exists.

The problem is quite robust as it is stated. It does not depend on a particular language (any complete language is good) or on particular axioms schemes and rules. We may add even the substitution and the extension rules. It also does not depend on a particular format of proofs we require (tree-like or sequence-like). In fact, it also does not matter whether we confine to Frege systems or whether we use Gentzen's sequent calculus (with cut) or natural deduction, or extended resolution. The phrase *does not matter* means that proofs in one system can be translated into proofs in another system with just a polynomial increase in the number of steps.

No non-trivial lower bounds for $k_F(\tau)$ are known at present. For some provably less efficient systems superpolynomial lower bounds are known. These systems include, in particular, resolution, constant-depth subsystems of a Frege system and their extensions by some counting principles, and cutting planes proof system.

The methods used in the proofs of these lower bounds include counting arguments, an adaptation of the method of random restrictions from Boolean complexity (that can be cast also as forcing in non-standard models of bounded arithmetic), and effective interpolation theorems. We shall discuss these methods later.

Finally we should mention the tautology that was used in one or other form in all lower bounds mentioned earlier. It is the *pigeonhole principle* PHP^m_n,

[1]Experts among readers should note now, and keep in mind throughout the paper, that we are concerned with the measure k_F rather than with s_F.

$m > n$,

$$\bigwedge_{i<m} \bigvee_{j<n} p_{ij} \ \rightarrow \ \bigvee_{i_1<i_2<m} \ \bigvee_{j<n} (p_{i_1 j} \wedge p_{i_2 j})$$

formalizing that no map from $\{0,\ldots,m-1\}$ to $\{0,\ldots,n-1\}$ can be injective. In retrospect we can see that it was a crucial step taken by [9] to put this tautology forward as a candidate for being hard (i.e., without short proofs) for usual proof systems. One particular difficulty in approaching the problem stated earlier is that we lack such good candidates for F.

In next three sections we describe and compare three universal frameworks for lower bounds to k_F. In section 4 we consider some related mathematical structures. Section 5 discusses limitations of particular methods used so far for subsystems of F. In section 6 we discuss new candidates of hard tautologies.

1 Partial Boolean valuations

A partial Boolean algebra $\mathcal{B}$ is a set together with distinguished constants $0_{\mathcal{B}}$, $1_{\mathcal{B}}$ and partial functions $\neg, \wedge, \vee$ such that any instance $t = s$ of any identity of some fixed equational axiomatization (e.g., [14]) of the theory of Boolean algebras, in which both terms t, s are defined, is actually valid in $\mathcal{B}$. The following notion was defined in [23].

Let Γ be a finite set of formulas closed under subformulas. A *partial Boolean valuation* of Γ is a map

$$\nu : \Gamma \rightarrow \mathcal{B}$$

of Γ into a partial Boolean algebra $\mathcal{B}$ such that

1. $\nu(0) = 0_{\mathcal{B}}$ and $\nu(1) = 1_{\mathcal{B}}$, whenever 0 and 1 are in Γ
2. $\neg\nu(A)$ is defined and equal to $\nu(\neg A)$, whenever $A, \neg A$ are in Γ
3. $\nu(A) \wedge \nu(B)$ is defined and equal to $\nu(A \wedge B)$, if all $A, B, A \wedge B$ are in Γ. Analogously for $\vee$.

Theorem 1.1 ([23]) *Let τ be a tautology and let Γ range over sets of formulas containing τ and closed under subformulas.*

(a) Assume that every set Γ with $\leq k$ formulas admits a partial Boolean valuation $\nu : \Gamma \rightarrow \mathcal{B}$ in which $\nu(\tau) \neq 1_{\mathcal{B}}$. Then:

$$k_F(\tau) > \epsilon \cdot k$$

(b) Assume that $k_F(\tau) > k^c$. Then every set Γ of $\leq k$ formulas admits a partial Boolean valuation ν in which $\nu(\tau) \neq 1_{\mathcal{B}}$.

Constants ϵ, c depend only on the particular formulation of the Frege system.

Part (a) says that partial Boolean valuations can be used to prove a lower bound to $k_F(\tau)$. Part (b) complements this by showing that at least a lower bound of the form $k_F(\tau)^{\Omega(1)}$ can be proved, in principle, by a construction of suitable partial Boolean valuations.

Let us illustrate the method on an example. Consider the tautology $(\neg)^{(2k)}(1)$, $2k$ negation signs in front of 1. It was proved in [21] that $k_F((\neg)^{(2k)}(1)) = \Omega(k)$. We show this by constructing a suitable partial Boolean valuation for every set Γ of at most $2k$ formulas and containing $(\neg)^{(2k)}(1)$. As $\Gamma \leq 2k$, Γ does not contain some formula $(\neg)^{(i)}(1)$, for $i < 2k$. Define map ν_i in two stages:

1. For $j < i$ give to $(\neg)^{(j)}(1)$ the value $1_{\mathcal{B}}$ if j is even and the value $0_{\mathcal{B}}$ if j is odd.

   For $j \geq i$ give to $(\neg)^{(j)}(1)$ the value $0_{\mathcal{B}}$ if j is even and the value $1_{\mathcal{B}}$ if j is odd.

2. For any formula $A(\overline{p})$ evaluate first atoms $\overline{p}$ by $0_{\mathcal{B}}$, maximal subformulas of the form $(\neg)^{(j)}(1)$ according to 1., and then evaluate A using ordinary truth-tables of $\neg, \vee, \wedge$.

It is easy to see that this defines a partial Boolean valuation of Γ in $\{0_{\mathcal{B}}, 1_{\mathcal{B}}\}$ in which $\nu_i((\neg)^{(2k)}(1)) = 0_{\mathcal{B}}$. Hence a lower bound $k_F((\neg)^{(2k)}(1)) = \Omega(k)$ follows by Theorem 1.1.

Admittedly the tautology $(\neg)^{(2k)}(1)$ is rather primitive. Sadly enough, this is essentially the best lower bound for any $k_F(\tau)$ known at present.

2 Local Boolean valuations

Another form of a Boolean-type valuation was used in [28] and formalized into a universal framework in [8, 32].

Let Γ be a set of formulas. A *local Boolean valuation* is a map η assigning to every subset $\Delta \subseteq \Gamma$ of at most c formulas an ordinary total Boolean algebra $\mathcal{B}_\Delta$ and a map $\eta_\Delta : \Delta \to \mathcal{B}_\Delta$ preserving all connectives for formulas in Δ satisfying the following compatibility condition. Whenever $\Delta_1 \subseteq \Delta_2 \subseteq \Gamma$ are two sets of size at most c then there is a homomorphism ρ from $\mathcal{B}_{\Delta_1}$ into $\mathcal{B}_{\Delta_2}$ such that $\rho(\eta_{\Delta_1}(A)) = \eta_{\Delta_2}(A)$ holds for all $A \in \Delta_1$. The constant c depends only on the particular Frege system F.

It was proved in [20, Chpt.13] that any set Γ with a local Boolean valuation in which $\eta_{\{\tau\}}(\tau) \neq 1_{\mathcal{B}_{\{\tau\}}}$ admits a partial Boolean valuation $\nu : \Gamma \to \mathcal{B}$ in which $\nu(\tau) \neq 1_{\mathcal{B}}$ (assuming that c is large enough). This shows that if we can find a local Boolean valuation with this property for any Γ of size $\leq k$, then $k_F(\tau) = \Omega(k)$.

In the other direction consider the following construction. From Γ form a new set $\Gamma' \supseteq \Gamma$ as follows. Let $\mathcal{B}_c$ be the finite total Boolean algebra (of size 2^{2^c}) freely generated by $b_1, \ldots, b_c$, let $t_1, t_2, \ldots$ be 2^{2^c} terms (formed from $\overline{b}$)

expressing all elements of $\mathcal{B}_c$, and let $s_1, s_2, \ldots$ be all terms occurring in some fixed derivations (from the identities defining Boolean algebras) of all identities of the form $\neg t_i = t_j$, $t_i \vee t_j = t_k$ and $t_i \wedge t_j = t_k$ valid in $\mathcal{B}_c$.

Given set Δ of at most c formulas $A_1, \ldots, A_d$, $d \leq c$, form the set Δ^+ of all formulas $s_1(b_1/A_1, \ldots, b_d/A_d, b_{d+1}/1, \ldots, b_c/1), \ldots$. Define $\Gamma' \supseteq \Gamma$ to be the minimal set closed under subformulas and containing $\bigcup_{\Delta \subseteq \Gamma, |\Delta| \leq c} \Delta^+$. Note that $|\Gamma'| = |\Gamma|^{O(1)}$.

Obviously, a partial Boolean valuation ν of Γ' yields a local Boolean valuation of Γ as the images of Δ^+ in ν are total Boolean algebras. Hence part (b) of Theorem 1.1 implies part (b) of the next theorem.

Theorem 2.1 *Let τ be a tautology and let Γ range over sets of formulas containing τ and closed under subformulas.*

(a) [8, 32] Assume that every set Γ with $\leq k$ formulas admits a local Boolean valuation η in which $\eta_{\{\tau\}}(\tau) \neq 1_{\mathcal{B}_{\{\tau\}}}$. Then $k_F(\tau) = \Omega(k)$.

(b) On the other hand, any set Γ, $\Gamma \leq k_F(\tau)^\epsilon$, admits a local Boolean valuation η in which $\eta_{\{\tau\}}(\tau) \neq 1_{\mathcal{B}_{\{\tau\}}}$.

Constant ϵ depends only on the particular formulation of the Frege system.

3 A Prover - Adversary game

The following game played by two players, *Prover* and *Adversary*, was defined in [8, 32]. In every round Prover asks about the truth-value of a formula and Adversary replies with a value. When aiming at proving τ, Prover asks in the first round about the truth-value of τ and Adversary is obliged to reply with 0. The game ends when the answers of Adversary contain an elementary contradiction, i.e., 0 gets value 1 or vice versa, or formulas $A, \neg A$ get the same value, or formulas $A, B, A \wedge B$ (resp. $A \vee B$) get values contradicting the truth-tables of $\wedge$ (resp. of $\vee$). The following theorem was proved in [8, 32] by induction on t and $k_F(\tau)$.

Theorem 3.1 ([8, 32]) *Let t be the minimal number such that there is a Prover forcing the end of the game on τ in t rounds against any Adversary. Then t is proportional to* $\log_2(k_F(\tau))$.

The theorem can be also seen as a corollary (in fact, an equivalent version) of the fact that every proof can be rewritten into a form of a balanced tree with only a polynomial increase in the number of steps.

Let us illustrate the method on the same example as in section 1 (following [8]). Adversary may use partial Boolean valuations ν_i defined in section 1 as follows. In every round s, being asked about a formula A, he takes the collection X_s of all ν_i such that all his answers in rounds $1, \ldots, s-1$ were consistent with

ν_i. Then he answers 1 if at least half of valuations from X_s give to A value $1_{\mathcal{B}}$, otherwise he answers 0. Clearly $|X_s| \geq \frac{2k}{2^{s-1}}$ and Prover cannot force an elementary contradiction if $|X_s| \geq 2$. Hence Adversary using this strategy survives at least $\log_2(2k)$ rounds with any prover.

This construction of a strategy for Adversary from partial Boolean valuations can be generalized to any τ. Fix t such that $k_F(\tau) > 2^{O(t)}$, the constant in the exponent to be determined later. For any prover P take the binary tree of depth $t-1$ corresponding to all possible plays P can have against some adversary. Put Γ_P to be the smallest set closed under subformulas and containing all $2^t - 1$ conjunctions of answers of an adversary (determining a path in the tree) in first $i = 1, \ldots, t$ rounds. In particular, $\neg\tau \in \Gamma_P$. A crucial technical fact is that if there would be a prover P forcing the end of a game in t rounds against any adversary then, in fact, there would be such prover yielding the set Γ_P of size $O(2^t + |\tau|)$, and such that it is a priori sufficient to restrict to finitely many of such provers. This follows from Theorem 3.1 and [20, Lemmas 4.4.4 and 4.4.6]. Consider only such provers P.

Assume that $k_F(\tau) > |\Gamma_P|^c$, c the constant from Theorem 1.1. Then there is a partial Boolean valuation $\nu_P : \Gamma_P \to \mathcal{B}_P$ in which $\nu_P(\tau) \neq 1_{\mathcal{B}_P}$, i.e., $\nu_P(\neg\tau) \neq 0_{\mathcal{B}_P}$. Put X_1 to be the set of all these valuations. At round s Adversary has the set X_s of those ν_P for which $\nu_P(\psi_1 \wedge \ldots \wedge \psi_{s-1}) \neq 0_{\mathcal{B}_P}$, where $\psi_1(= \neg\tau), \ldots, \psi_{s-1}$ are his answers in the first $s-1$ rounds. Enquired about the truth-value of ψ he computes the ν_P-values of the conjunctions $\psi_1 \wedge \ldots \wedge \psi_{s-1} \wedge \psi$ and $\psi_1 \wedge \ldots \wedge \psi_{s-1} \wedge \neg\psi$ (both are in Γ_P) and answers in such a way that the new conjunction has still the ν_P-value different from $O_{\mathcal{B}_P}$.

4 Related structures

We shall digress at this point and consider four different mathematical structures related to the methods described earlier. In particular, we shall discuss non-standard models of bounded arithmetic, the approximation method from Boolean complexity, logical structures arising in quantum mechanics, and partial algebraic structures.

4.1 Non-standard models of bounded arithmetic

Let N be a countable non-standard model of a sufficiently strong fragment of true arithmetic, say of Peano arithmetic. Let $\tau \in N$ be a non-standard propositional formula of size $n = |\tau|$, built from non-standardly many atoms $p_0, \ldots, p_m$. Assume that N thinks that τ is a tautology that $k_F(\tau) > n^\ell$, all standard ℓ. By compactness argument this is a consistent situation if k_F cannot be bounded by a polynomial. Consider the following construction.

Let $M \subseteq_e N$ be the initial part of N consisting of numbers with at most n^ℓ bits, $\ell < \omega$. Let $Flas^M$ be all elements of M coding in N and M a formula built from atoms $p_0, \ldots, p_m$. Assume that we find a map $\nu : Flas^M \to \mathcal{B}$, where $\mathcal{B}$ is a total Boolean algebra, and such that $\nu(\tau) \neq 1_{\mathcal{B}}$.

Take an ultrafilter $\mathcal{U} \subseteq \mathcal{B}$ such that $\nu(\tau) \notin \mathcal{U}$ and define the map

$$\eta : A \in Flas^M \to \nu(\tau)/\mathcal{U} \in \{0, 1\}$$

In particular, $\eta(\tau) = 0$ and, in a sense, we may think of the tuple $\eta(p_0), \ldots, \eta(p_m)$ as of a truth-assignment satisfying $\neg\tau$. A problem with this interpretation is that we cannot define the assignment neither in N (as we do not assume $\mathcal{U}$ to be definable in N) nor in the standard model (as both τ and the assignment are nonstandard). This suggest to consider the set of all tuples of bits $\langle \eta(A_1), \ldots, \eta(A_t) \rangle$ formed from all tuples $A_1, \ldots, A_t$ of elements of $Flas^M$ that are coded in M. These tuples of bits can be identified via dyadic encoding with numbers. The set of these numbers M^* is, in fact, a structure extending M and with a suitable choice of $\mathcal{U}$ it is a model of bounded arithmetic theory S^1_2, see [23]. Moreover, in M^* τ is not a tautology anymore.

On the other hand, having an extension M' of M in which $\neg\tau$ is satisfied by a truth-assignment $\overline{a} \in \{0, 1\}^{m+1}$ allows to evaluate in M' any $A \in Flas^M$ under $\overline{a}$, obtaining a Boolean valuation in which τ gets value 0.

We note that the valuation ν of $Flas^M$ is really only a partial Boolean valuation from the point of view of N, as $Flas^M$ is not closed even under all conjunctions (in N).

In this way Boolean valuations of sets of propositional formulas correspond to extensions of models of bounded arithmetic. The particular theory S^1_2 appears as we consider Frege systems; other proof system correspond to other theories of bounded arithmetic.

4.2 The approximation method

[36] formalized [34, 35] into a universal framework for proving lower bounds on the size of general circuits. A particular presentation is as follows, cf. [36, 16].

Let $f : \{0, 1\}^n \to \{0, 1\}$ be a Boolean function about which we want to prove that it cannot be computed by a small circuit. Let C be a Boolean circuit (over the base $0, 1, \neg, \vee, \wedge$) with inputs $x_1, \ldots, x_n$. Every node (i.e., a subcircuit) y of C determines a function C_y of $x_1, \ldots, x_n$ computed by the subcircuit y. Take the set $X := f^{(-1)}(0)$ and assign to every node y a subset $||y||$ of X of those inputs accepted by C_y. We may think of the map $|| \ldots ||$ as a map from C into the Boolean algebra $\exp(X)$ of the subsets of X preserving the connectives.

We assign to nodes of C a value in $\{0, 1\}$ as follows. Pick $U \subseteq \exp(X)$ and assign to y the value $\eta_U(y) := 1$ if $||y|| \in U$ and $\eta_U(y) := 0$ otherwise. Assume that C computes f. Then $\eta_U(C) = 0$ iff $\emptyset \notin U$. U defines a vector $w_U \in \{0, 1\}^n$ whose i^{th} coordinate is $\eta_U(x_i)$. Thus if we find U not containing $\emptyset$ such that $f(w_U) = 1$ and η_U preserves the connectives in C we, in fact, demonstrate that $C(w_U) \neq f(w_U)$ and so C does not compute f. This method is universal in the sense that such U exists whenever the size of C is at most k^ϵ, k being the circuit-size of f (and ϵ an independent constant), cf. [36, 16]).

Note that the map η_U is only a partial Boolean valuation unless U is an ultrafilter. Thus partial Boolean valuations are inevitable as on the finite Boolean algebra $\exp(X)$ the only ultrafilters are principal and thus always $w_U \in X$.

For the approximation method in the particular form as in [34, 35, 38] a partial Boolean valuation of the subcircuits of C can be described directly. Let y^* be the approximating function assigned to y and let E be the set of all inputs that are erroneously computed by y^* at some y. Then define the value of y to be the collection of all subcircuits y such that $y^* = z^*$ holds outside the set E. By the definition of E this map preserves all connectives of C. The point then is to show that C^* and f do not agree outside E.

Now assume that f is the characteristic function of an NP-predicate. Form a formula τ of the form

$$\alpha(x_1, \ldots, x_n, z_1, \ldots, z_{n^{O(1)}}) \rightarrow \beta(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

where α is a formula formalizing that $f(x_1, \ldots, x_n) = 1$ as witnessed by $\overline{z}$, and β formalizes that circuit C defined by $\overline{y}$ accepts $\overline{x}$. Hence τ is a tautology iff C accepts all inputs accepted by f. Now assume also that we have a partial Boolean valuation ν of the set of subformulas of τ in which $\nu(\tau) = 0_{\mathcal{B}}$. Hence

$$\nu(\alpha(x_1, \ldots, x_n, z_1, \ldots, z_{n^{O(1)}})) = \alpha(\nu(x_1), \ldots, \nu(x_n), \nu(z_1), \ldots, \nu(z_{n^{O(1)}})) = 1_{\mathcal{B}}$$

and

$$\nu(\beta(x_1, \ldots, x_n, y_1, \ldots, y_m)) = \beta(\nu(x_1), \ldots, \nu(x_n), \nu(y_1), \ldots, \nu(y_m)) = 0_{\mathcal{B}}$$

so we may think of the tuple $\nu(x_1), \ldots, \nu(x_n)$ as an input from $\mathcal{B}^n$ accepted by f but not by C. In fact, the model-extension construction from the previous section can made the intuition precise (and, in particular, yield a new 0-1 input in M^*).

4.3 Logical structures arising in quantum mechanics

Important object arising in quantum mechanics is the lattice of closed linear subspaces of a Hilbert space. This object is called also a lattice of (quantum mechanical) propositions, see [5, 15]. It is not a Boolean algebra.

The sublattices of the lattice of propositions that are Boolean algebras play an important role in defining compatible propositions; propositions are compatible if the sublattice they generate is a Boolean algebra. The sublattices that are complete Boolean algebras correspond to reference frames of observations, see [42]. Another way of approaching a logic in which not all propositions are compatible is by formalizing the informal notion of logic with partial propositions, see [39, 18]. These were studied in a connection with the hidden variables problem, see [17, 19].

A third logical object arising in quantum mechanics are formal dialogs, used as a form of semantic for quantum logic (see [30, 40]).

These three structures, the lattice of propositions, reference frames and formal dialogs, appear to be analogous to partial Boolean valuations, local Boolean valuations and the Prover-Adversary game. For the latter structures sections 1-3 explain why they occur simultaneously, while for the former structures this seem to be a matter of discussion, see [3].

While we are at pointing informal relations we may as well add one more. Note that the construction from section 4.1 is somewhat analogous to a construction of a Quantum set theory, see [41]. This is a theory constructed as Boolean-valued set theory with formulas taking their truth-values in the lattice of propositions defined earlier rather than in a complete Boolean algebra.

4.4 Partial algebraic structures

A partial algebraic structure is a set together with a collection of partial operations. A variety of algebraic structures of a given signature axiomatized by identities T (call the variety also T) gives rise to an associated class T^p of partial algebras in the same signature. Namely, a partial algebra is in T^p iff instances $t = s$ of all identities of T that are actually defined in the partial algebra are also valid in it. (Occasionally few more technical conditions are added, see [10, 11].) An interesting problem associated with T^p is the embeddability problem: given a finite partial structure from T^p decide whether it can be embedded into a total (possible infinite) structure from T. Important theorem of [10] says that the embeddability problem is decidable iff the word problem associated to T is decidable. It follows that if all partial algebras from T^p can be embedded into total ones then the word problem for T is decidable. It is instructive to compare the following proof-sketch of this corollary with the proof of Theorem 1.1 in [23]. Let $\overline{a}$ be generators of an algebra $\mathcal{A}$ from T, $r_i(\overline{a}) = s_i(\overline{a})$ its finite presentation and $w_1(\overline{a}), w_2(\overline{a})$ two words. For every subterm t occurring in one of r_i, s_i, w_1, w_2 introduce new unknown b_t and rewrite the identities $r_i = s_i$ into the set of indentities the form $b_i = b_j$ and $f(b_{i_1}, \ldots, b_{i_k}) = b_j$. From these identities derive, using T, all possible identities of the same form, possible identifying new pairs $b_i = b_j$. This process yields a partial algebra $\mathcal{A}^p$ from T^p. If $b_{w_1} = b_{w_2}$ in $\mathcal{A}^p$ then $w_1 = w_2$ in $\mathcal{A}$. Otherwise $\mathcal{A}^p$ can be embedded into a total algebra $\mathcal{A}'$ and hence $w_1 \neq w_2$ in its subalgebra generated by the image of $\mathcal{A}^p$. Hence $w_1 \neq w_2$ in $\mathcal{A}$ as well.

Partial Boolean algebras arising in section 1 can be never embedded in a total one. This is because every tautology must get value 1 in every total Boolean algebra (otherwise a suitable ultrafilter would define a truth-assignment not satisfying the tautology). It is an interesting problem whether we can get any quantitative information about the structure of partial Boolean valuations. Specifically, assume that $\nu : \Gamma \to \mathcal{B}$ is a partial Boolean valuation in which a tautology gets a value different from $1_{\mathcal{B}}$, and let $|\mathcal{B}| = \ell$. The tables of operations $\neg, \vee, \wedge$ of $\mathcal{B}$ have $2\ell^2 + \ell$ potential entries.

Can we show that, say, at most 99% of entries of the tables of a partial Boolean algebra are filled? This would hold if the fact that more than 99% of the entries are filled would imply that $\mathcal{B}$ is embeddable in a total Boolean algebra (something similar holds for partial groups, see [29]).

5 Limitations of particular methods

In this section we want to examine why methods used for lower bounds for subsystems of a Frege system mentioned in the introduction do not work for F as well. First we should frankly admit that the word *methods* is not appropriate. This is because we are able to prove lower bounds only for very few tautologies and we are definitely not able to determine the minimal number of steps needed in a proof of an arbitrary tautology.

Secondly there seems to be a popular opinion that a lower bound for a proof system is essentially a corollary of a Boolean complexity lower bound for the class of formulas occurring in proofs in the particular proof system. This is, unfortunately or fortunately, not the case. (A sceptical reader may try to adapt [35, 38] to a lower bound for tautologies $Count_{q,1}$ - defined below - in a natural proof system working with constant-depth formulas with counting-mod-p gates, p, q different primes, see [20, 4] for a definition of such a system.) One reason perhaps is that formulas or circuits represent deterministic computations while proof systems are non-deterministic.

A counting argument used originally by [12] to prove a lower bound for resolution works as follows. There is a large set X of truth assignments (to atoms of PHP_n^{n+1} - see the introduction) with the following property. Any refutation of the clauses representing $\neg PHP_n^{n+1}$ determines a map from X to the clauses occurring in the refutation such that the preimage of any clause is small. As X is large, the number of clauses must be large too.

There is no a priori reason why similar approach cannot work for F. Indeed, [13] succeeded in reproving an exponential lower bounds for monotone circuits ([34, 2]) in this way. However, the structure of F-proofs appears to be much more complex than that of resolution refutations (the difference between the two proof systems may be also documented by a big difference between bounded arithmetic theories corresponding to them, see [20]) to allow a direct construction of a suitable map.

The method of random restrictions in Boolean complexity works as follows. Given a constant-depth and not too big circuit one shows (by a probabilistic argument) that there is an assignment of 0 and 1 to some inputs simplifying the circuit substantially. This means that the Boolean function computed by the restricted circuit on the unassigned inputs can be, in fact, computed by a circuit of a very simple form. Then one shows that the function the original circuit supposedly computed does not have this property.

In lower bounds for constant-depth subsystems of a Frege system a related approach is used (e.g., [1, 22, 28, 31]). First partially evaluate atoms so that all formulas in a fixed and not too big proof of a tautology (e.g., PHP_n^{n+1}) get simplified. Then argue that there cannot be a proof of the restricted tautology involving only simple formulas. As the restrictions must not simplify the tautology too much they must be of a special form. In the case of the formula PHP_n^{n+1} the restrictions correspond to partial injective maps from $\{0, \ldots, n\}$ into $\{0, \ldots, n-1\}$. The second step is then achieved in [28] by a form of a local Boolean valuation (of the set of simplified formulas occurring in the restricted proof), in [22, 31] it is an argument in the spirit of the Prover-Adversary game.

A principal reason why this does not work for F is that a general formula or a circuit do not simplify much after a restriction (but see [20, Chpt.13]). We may at least try to learn a lesson of how partial Boolean valuations implicitly occurring in proofs of lower bounds for PHP_n^{n+1} are constructed and used, and think about how to extend such an approach to F. The reader may find this in detail in [20, Chpt.12] and here we add only few general observations (we shall assume a familiarity with [28, 23] for the next paragraph).

Important objects in [28] are complete systems. A disjunction of maps (map-conjuctions precisely) from a complete system is shortly provably equivalent to 1, assuming $\neg PHP_n^{n+1}$ as an axiom. *Shortly provably equivalent* means that we take a set Γ of not too many formulas and any proof may use only formulas from Γ, cf. [23]. Thus, assuming $\neg PHP_n^{n+1}$, complete systems are just new disjunctive normal forms of 1. In terms of a partial Boolean valuation $\nu : \Gamma \to \mathcal{B}$ this means that ν-values of maps from a complete system form a partition of unity in $\mathcal{B}$. To restrict the proof means to augment $\neg PHP_n^{n+1}$ by a new axiom, a map-conjunction. Under this new axiom all formulas in Γ have (shortly provably equivalent) new disjunctive normal forms. In proving this a crucial step is an application of a switching lemma. In the language of ν this corresponds to refining a subset of $\mathcal{B}$ into an antichain.

Let us now turn to the method of effective interpolation. It was first explicitly proposed in [22] and put to work in [37, 24], implicitly in [6], and in [33]. (This development is not much covered in [20] so we add references.)

We say that a proof system admits effective interpolation if every implication

$$A(\overline{p}, \overline{q}) \to B(\overline{p}, \overline{r})$$

provable in k steps has an interpolant $I(\overline{p})$ whose circuit-size is $k^{O(1)}$. An effective monotone interpolation asserts the same for implications without negative occurrences of p_i in A and B, and requires $I(\overline{p})$ to define a Boolean function computable by a monotone circuit of size $k^{O(1)}$. These effective versions of interpolation are valid for resolution, cut-free sequent calculus, a version of the depth 2 subsystem of the sequent calculus, linear equational logic and cutting planes (see the references above).

The idea of using effective interpolation for lower bounds is as follows. Assume that a proof system P admits effective (monotone) interpolation and that $A_n(\overline{p}, \overline{q}) \to B_n(\overline{p}, \overline{r})$ is a family of implications with atoms $\overline{p} = p_1, \ldots, p_n$ and of size $n^{O(1)}$ that do not have (monotone) interpolants of polynomial size. Then the implications necessarily do not have P-proofs with $n^{O(1)}$ steps.

It is an important open problem to decide which proof systems do admit effective interpolation. There are some limitations to effective monotone interpolation (see [24]) showing that the known positive results are almost best possible. However, for the non-monotone version similar statement is open. [27] show that unless a standard cryptographical conjecture about the security of the RSA encryption scheme fails, Frege systems do not admit effective interpolation.

For constant-depth subsystems we do not have similar result but we may note that a theorem of [4] implies that a version of effective interpolation valid for proof systems mentioned earlier does not hold for extensions of constant-depth systems by modular counting principles. This version implies, in particular, that if formulas A and B have no common atoms and $A \vee B$ is provable in k steps then one of A, B is provable in $k^{O(1)}$ steps.

Consider formulas $\neg Count^n_{q,i}(\overline{r})$ formalizing that the atoms $\overline{r}$ define a q-partition of n, where $n \equiv i \pmod q$. In particular, there is one atom r_e for each q-element subset e of $\{0, \ldots, n-1\}$ and the formula formalizes the fact that $\{e \mid r_e = 1\}$ is not a total partition of $\{0, \ldots, n-1\}$. Define:

$$A := Count^{6a+1}_{2,1}(\overline{r}) \quad \text{and} \quad B := Count^{6b+1}_{3,1}(\overline{s})$$

From $\overline{r}$ and $\overline{s}$ we can define constant-depth formulas $\overline{C}$ such that $\neg A \wedge \neg B$ imply by a short constant-depth proof

$$\neg Count^{(6a+1)(6b+1)}_{6,1}(\overline{C})$$

(think of the rectangle $(6a+1) \times (6b+1)$ partitioned into rectangles of size 2×3 defined by $\overline{r}, \overline{s}$). Hence a constant-depth Frege system augmented by instances of $Count_{6,1}$ proves $A \vee B$ by a poly-size proof. However, by the main theorem (Thm 1.2) of [4] none of $Count_{2,1}$ or $Count_{3,1}$ admits poly-size proofs from $Count_{6,1}$.

It is not known whether $min(k_F(A), k_F(B)) = k_F(A \vee B)^{O(1)}$ for A, B without common atoms. The reader may contemplate difficulties encountered while trying to prove such an inequality using one of Theorems 1.1, 2.1 or 3.1.

6 Hard tautologies ?

It is apparently rather difficult to come up with tautologies τ that would be reasonable candidates to have large $k_F(\tau)$. A heuristic reason for that is that

Frege systems can count and hence combinatorial principles derivable by counting arguments (like the pigeonhole principle) cannot be hard for F (even when measuring the complexity of proofs by $s_F(\tau)$ rather than by $k_F(\tau)$, see [7]).

In [27] the following tautologies τ_p were defined. It is not known whether they have Frege proofs with polynomially many steps.

Fix p a prime with n bits. The tautology τ_p is formed from atoms $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ and $z_1, \ldots, z_{n^{O(1)}}$. Atoms $\overline{x}, \overline{y}$ represent bits of two integers and $\overline{z}$ stand for bits of the table of a computation of the product $\overline{x} \cdot \overline{y}$. The formula τ_p asserts that if both $\overline{x}, \overline{y}$ are bigger than 1 and $\overline{z}$ is indeed a computation of $\overline{x} \cdot \overline{y}$ then the output of the computation (as encoded in $\overline{z}$) is not equal to p.

Currently no lower bounds for these tautologies are known in any proof system. On the other hand, we also do not know an infinite set of primes p for which there would be Frege proofs with polynomially many steps. It would be very interesting to prove a superpolynomial lower bound to $k_F(\tau_p)$ even under some unproved but plausible conjecture from computational complexity theory.

Acknowledgement: I thank P. Pudlák and A. A. Razborov for comments on the draft of this paper.

References

[1] M. Ajtai: The complexity of the pigeonhole principle, in: Proc. IEEE 29^{th} Annual *Symp. on Foundation of Computer Science*, (1988), pp. 346-355.

[2] A. E. Andreev : On a method for obtaining lower bounds for the complexity of individual monotone functions (in Russian), *Doklady AN SSSR*, **282(5)**, (1985), pp.1033-1037.

[3] *Current issues in quantum logic*, Eds. E.G.Beltrametti and B.van Fraasen, Plenum Press, New York-London, Ettore Majorana International Science Series, Vol.8, Proc. of the Workshop on Quantum Logic held Dec.2-9, 1979 in Erice, Sicily. (1981).

[4] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi and P.Pudlák : Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proceedings of the London Mathematical Society*, to appear.

[5] G. Birkhoff and J. von Neumann: The logic of quantum mechanics, *Annals of Mathematics*, **37**, (1936), pp.823-843.

Reprinted in *The logico-algebraic approach to quantum mechanics*, Vol.I., Ed. C.A.Hooker, D.Reidel Publ.Co., Dordrecht-Boston, (1975).

[6] M. L. Bonet, T. Pitassi, and R. Raz : Lower bounds for cutting planes proofs with small coefficients, preprint, (1994).

[7] S. Buss : The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic* **52**, (1987), pp. 916-927.

[8] S. Buss and P. Pudlák: How to lie without being (easily) convicted and the length of proofs in propositional calculus, in: Proceedings of the meeting *Computer Science Logic*, Kazimierz 1994, Eds. L.Pacholski and J.Tiuryn, LNCS **933**, Springer-Verlag, (1995), pp.151-162.

[9] S.A. Cook and A.R. Reckhow: The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**, (1979), pp. 36-50.

[10] T. Evans: Word problems, *Bulletin of the AMS*, **84(5)**, (1978), pp.789-802.

[11] G. Gratzer : *Universal algebra* (2nd ed.), Springer - Verlag, (1979), 581 p.

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

[13] —— : Counting bottlenecks to show monotone $P \neq NP$, preprint, (1995).

[14] E.V. Huntington: Sets of independent postulates for the algebra of logic, *Transaction of the AMS*, **5**, (1904), pp.288-309.

[15] J.M. Jauch: *Foundations of quantum mechanics*, Addison-Wesley, Reading-Menlo Park-London-Don Mills, Series in Advanced Physics, (1968).

[16] M. Karchmer : On proving lower bounds for circuit size, in : *Proc. Structure in Complexity*, 8^{th} Annual Conference, *IEEE* Computer Science Press, (1993), pp. 112-119.

[17] S. Kochen and E. Specker: Logical structures arising in quantum theory, in: *The theory of models*, Eds. J. Addison, L. Henkin and A. Tarski, North-Holland, Amsterdam, (1956).

Reprinted in *The logico-algebraic approach to quantum mechanics*, Vol.I., Ed. C.A.Hooker, D.Reidel Publ.Co., Dordrecht-Boston, (1975).

[18] —— : The calculus of partial propositional functions, in: *Logic, Methodology and Philosophy Science*, Ed. Y. Bar-Hillel, North-Holland, Amsterdam, (1965).

Reprinted in *The logico-algebraic approach to quantum mechanics*, Vol.I., Ed. C.A.Hooker, D.Reidel Publ.Co., Dordrecht-Boston, (1975).

[19] —— : The problem of hidden variables in quantum mechanics, *J. of Mathematics and Mechanics*, **17**, (1967), pp.59-67.

Reprinted in *The logico-algebraic approach to quantum mechanics*, Vol.I., Ed. C.A.Hooker, D.Reidel Publ.Co., Dordrecht-Boston, (1975).

[20] J. Krajíček : *Bounded arithmetic, propositional logic and complexity theory*, Cambridge University Press, in print.

[21] —— : Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universitas Carolinae*, **30(1)**, (1989), pp.137-140.

[22] —— : Lower bounds to the size of constant-depth propositional proofs, *J. of Symbolic Logic*, **59(1)**, (1994), pp.73-86.

[23] —— : On Frege and extended Frege proof systems, in: *Feasible Mathematics II*, Eds. P. Clote and J. Remmel, Birkhauser, (1995), pp. 284-319.

[24] —— : Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. of Symbolic Logic*, (1995), to appear.

[25] —— : A fundamental problem of mathematical logic, *Annals of Kurt Gödel Society*, Springer Verlag, (1995), to appear.

[26] —— : Valuations of Boolean formulae in partial algebras, in: Volume of Abstracts of the Tenth International Congress *Logic, Methodology and Philosophy of Science*, International Union of History and Philosophy of Science, Florence (August 19-25, 1995), (1995), pp.6-7.

[27] J. Krajíček and P. Pudlák: Some consequences of cryptographical conjectures for S^1_2 and EF, Proc. of the meeting *Logic and Computational Complexity*, (Indianapolis, October 1994), Ed. D. Leivant, (1995), to appear.

[28] J. Krajíček, P. Pudlák and A. Woods: An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, *Random Structures and Algorithms*, **7(1)**, (1995), pp.15-39.

[29] A. Lewenberg : On elementary pairs of O-minimal structures, PhD.Thesis, University of Illinois at Champaign-Urbana, (1995).

[30] P. Mittelstaedt : *Quantum logic*, D. Reidel Publ.Co., Dordrecht, Synthese Library, Vol. 126, (1978).

[31] T. Pitassi, P. Beame and R. Impagliazzo: Exponential lower bounds for the pigeonhole principle, *Computational Complexity*, **3**, (1993), pp.97-308.

[32] P. Pudlák : The lengths of proofs, in: *Handbook of Proof Theory*, Ed. S. Buss, to appear.

[33] —— : Lower bounds for resolution and cutting planes proofs and monotone computations, preprint, (1995).

[34] A. A. Razborov : Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathem. Doklady*, **31**, (1985), pp.354-357.

[35] ——— : Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, (1987), pp.598-607.

[36] ——— : On the method of approximations, in: *Proc. 21th Annual ACM Symp. on Theory of Computing*, (1989), pp. 168-176. ACM Press.

[37] ——— : Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**, (1995), pp.201-224.

[38] R. Smolensky : Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in: *Proc. 19th Ann. ACM Symp. on Th. of Computing*, (1987), pp. 77-82.

[39] E. P. Specker: The logic of propositions which are not simultaneously decidable, *Dialectica*, **14**, (1960), pp.239-246.

Reprinted in *The logico-algebraic approach to quantum mechanics*, Vol.I., Ed. C.A.Hooker, D.Reidel Publ.Co., Dordrecht-Boston, (1975).

[40] E.-W. Stachow: Completeness of quantum logic, *J. Phil. Logic*, **5**, (1976), pp.237-280.

[41] G. Takeuti: Quantum set theory, in: [3], pp.303-322.

[42] ——— : Quantum logic and quantization, in; *Proc. Int. Symp. Foundations of Quantum Mechanics*, Tokyo, (1983), pp.256-260.