On Frege and Extended Frege Proof Systems

JAN KRAJÍČEK

Abstract

We propose a framework for proving lower bounds to the size of EF-proofs (equivalently, to the number of proof-steps in F-proofs) in terms of *boolean valuations* . The concept is motivated by properties of propositional provability in models of bounded arithmetic and it is a finitisation of a particular forcing construction explained also in the paper. It reduces the question of proving a lower bound to the question of constructing a partial boolean algebra and a map of formulas into that algebra with particular properties. We show that in principle one can obtain via this method optimal lower bounds (up to a polynomial increase).

Introduction

A *propositional proof system* is any polynomial time function P whose range is exactly the set of tautologies TAUT, cf. [17]. For τ a tautology any string π such that $P(\pi) = \tau$ is called a *P-proof of τ*. Any usual propositional calculus, be it resolution or extended resolution, a Hilbert style system based on finitely many axiom schemes and inference rules (called a *Frege system* in [17]), Gentzen's sequent calculus or natural deduction system, is a propositional proof system in this sense, as they are all complete (resolution and extended resolution after a suitable encoding of formulas in DNF forms) and as it is decidable in polynomial time whether a string is a proof in the system or not.

The length (equivalently, *the size*) of a string δ will be denoted $|\delta|$. Thus the length of a proof is the total number of occurrences of symbols in it.

With a proof system P we associate two functions measuring the efficiency of P:

$$s^0_P(\tau) := \min\{|\pi| \mid \pi \text{ is an } P - \text{proof of } \tau\}$$

and

$$s_P(n) := \max\{s^0_p(\tau) \mid \tau \in TAUT, |\tau| \le n\} \ .$$

It is a *fundamental open problem* of mathematical logic and complexity theory to determine the growth rate of function $s_P(n)$ for "optimal" system P.

For example, the statement that there is a system P with $s_P(n)$ bounded by a power of n is equivalent to the statement that $NP = coNP$, cf [17].

For general system P nothing except trivial inequalities $s_P(n) = \Omega(n)$ and (for P containing resolution or cut-free system) $s_P(n) = \exp(O(n))$ is known. It is even unknown whether there is an optimal system P, where *optimal* means that $s_P(n)$ is bounded by a power of any other $s_Q(n)$, cf. [28]. For a small number of particular systems however, strong lower bounds of the form $\exp(n^{\Omega(1)})$ were established [43, 22, 26, 31, 36]. The strongest among these systems are the *constant-depth Frege systems,* see [26, 31, 36].

In this paper we consider the problem of proving non-trivial lower bounds to $s_F(n)$ and $s_{EF}(n)$, with F being a *Frege system* and EF being an *Extended Frege system,* cf. [17]. Presently only $s_F(n) = \Omega(n^2)$ is known.

Considerably more is understood about the mutual relations of the systems above regarding their efficiency. A partial quasiordering of proof systems, called *p-simulation,* was defined in [17]. In particular, if system P majorizes Q in this quasiordering then some power of $s_Q(n)$ majorizes $s_P(n)$. It is shown in [17] that in the induced equivalence relation Frege systems, the sequent calculus and the natural deduction system are equivalent (and are stronger than the resolution system by [22, 8]) and that the extended Frege system and extended resolution are also equivalent, and by [28, 19] these are equivalent also to a Frege system with the *substitution rule.* Moreover, various choices of axiom schemes and inference rules "of the same type" keep a system in the same equivalence class. Hence while studying function $s_P(n)$ of any of these systems we are quite free to choose its language and axiomatization, and the rules (for details see [17]).

It is known that if P is not optimal then one can find a polynomial-time set of tautologies expressing finitistic consistency statements which do not have polynomial size P-proofs, cf. [28]. However, it is difficult to work with such tautologies as they lack a direct combinatorial meaning and are instead related to delicate questions about the finitistic Gödel theorem. Thus one looks rather for a first order combinatorial principle valid over all finite structures where the combinatorial complexity of the principle would guarantee that tautologies τ_n, expressing that the principle holds in all structures with the universe of cardinality n, must have long P-proofs. This was successful in the cases of resolution and constant-depth Frege systems where the most frequently used principle is *the pigeonhole principle.* However, no example of a combinatorial statement which would make a plausible candidate for being hard for F or EF is known at present.[1]

[1] See [6]. In that paper and in [3] are also constructed polynomial-size Frege proofs of the Bondy theorem [4] which we suggested in [14] as a possible candidate of a principle hard for F.

It is conceivable that a direct combinatorial approach is not sufficient or that it is too difficult - similarly as it failed so far to produce any interesting lower bounds for general formulas or circuits - and that more subtle properties of F and EF will have to be explored.

A dominant property of these systems is their close relation to various systems of bounded arithmetic. In the present paper we study what this relation offers for the problem of establishing superpolynomial lower bounds for $s_F(n)$ or $s_{EF}(n)$. Our main result is a formulation of a framework suitable for proving such lower bounds. In the framework, called *boolean valuations*, the task to show lower bound m to the size of EF-proofs of tautology τ, $|\tau| \leq m$, is reduced to the problem of constructing for every set Γ of $O(m)$ formulas a partial boolean algebra $\mathcal{B}$ and a valuation $\nu : \Gamma \rightarrow \mathcal{B}$ with certain properties. We show that if such a valuation exists for each set Γ of $O(m)$ formulas then the lower bound m is valid and, on the other hand, if the lower bound m holds then such valuations exist for all sets of $m^{\Omega(1)}$ formulas. The concept of *boolean valuation* is motivated by properties of propositional provability in non-standard models of the theory V_1^1 and a particular forcing construction explained earlier in the paper.

The paper is organized as follows. Systems F and EF are defined in section 1 where we recall some of their combinatorial properties. In section 2 we recall the bounded arithmetic theories U_1^1 and V_1^1 and state some of their main properties. We also show in section 2 that the soundness of F (resp. of EF) is provable in U_1^1 (resp. in V_1^1) and we define a translation of $\Sigma_0^{1,b}$-formulas into propositional formulas.

In section 3 we give a proof that system EF polynomially simulates proofs in theory V_1^1 and obtain as a corollary of the proof the quasipolynomial simulation of U_1^1 by F and the polynomial simulation of $I\Delta_0(\alpha)$ by the constant-depth systems. The simulation implies, in particular, that if a combinatorial statement has a proof in V_1^1 (in a theory) then it has a short proof in EF (in the corresponding system).

The relations between EF and V_1^1 formulated in sections 2 and 3 show that a way to prove a superpolynomial lower bound to $s_{EF}(n)$ is to construct suitable extensions of models of V_1^1. In section 4 we define the notion of *a sequence of tautologies hard for a proof system* and restate using this notion some results from [28]. This suggests a type of tautology which might be hard for EF and a type of extension of models of V_1^1 whose construction is sought. In section 5 we consider a forcing construction of the relevant extension, albeit under the assumption that it does exist. This forcing construction motivates the *boolean valuations* framework defined in section 6. We also prove there that, in principle, one can obtain optimal lower bounds by this method.

The translation of an arithmetic proof into a family of polynomial-size propositional proofs was considered in [16, 37]. In particular, the relations between theory V_1^1 and proof system EF follows using known techniques from the relation of theory PV to EF established in [16]. The same techniques would give, however, only partial results about U_1^1 and F. The relation of $I\Delta_0(\alpha)$ and constant-depth Frege systems was proved in [37]. We give one proof implying all these relations. These issues are discussed more in the last section. We mention there also a communication complexity problem associated with an F-proof of a tautology. An upper bound to the communication complexity of the problem expressed in terms of the size of an F-proof implies a lower bound to the size of an F-proof of the tautology. For example, the lower bound of [22] can be presented in this form.

1 Frege and Extended Frege Proof Systems

For the sake of definiteness we shall adopt the following particular language for a *Frege system* F: the constants 0 (FALSE), 1 (TRUE), the connectives: $\neg, \wedge, \vee$ with their usual meaning, and atoms $p, q, \dots$. System F has a finite number of axiom schemes and inference rules which are sound and implicationally complete, cf. [17]. An *axiom* is any substitution instance of an axiom scheme. For example, F often has several axiom schemes and only one inference rule (e.g. the modus ponens).

Extended Frege system EF may be constructed as follows. An *EF-sequence* is a sequence of formulas $\psi_1, \dots, \psi_k$ such that each ψ_i is either an axiom of F, inferred from some previous ψ_u's by an inference rule or of the form $q \equiv \varphi$, where q is an atom occurring neither in φ nor in any of $\psi_1, \dots, \psi_{i-1}$. Such $q \equiv \varphi$ is called an *extension axiom* and q a new *extension atom* ($\equiv$ is an abbreviation). An *EF-proof* is any EF-sequence whose last formula does not contain any extension atom.

Frege system with the substitution rule SF is F augmented by the rule: from $A(p_1, \dots, p_k)$ infer $A(B_1, \dots, B_k)$, with B_i simultaneously substituted for p_i.

The next two theorems give some information about a mutual relation between these systems.

Theorem 1.1 ([28, 19]) *Systems EF and SF mutually p-simulate each other. In particular:*

$$s_{EF}(n) = (s_{SF}(n))^{O(1)} \text{ and } s_{SF}(n) = (s_{EF}(n))^{O(1)}.$$

■

Define function $k_P(n)$ for $P = F, EF$ and SF by first putting:

$$k_P^0(\tau) := \min\{k |\ \exists\ P\text{-proof of } \tau \text{ with } k \text{ proof steps}\},$$

and then:

$$k_P(n) := \max\{k_P^0(\tau) \mid \tau \in TAUT\ ,\ |\tau| \leq n\}.$$

This function is analogous to $s_P(n)$ measuring the number of proof steps instead of the size.

Theorem 1.2 ([17, 44, 24]) *(a)* $k_{EF}(n) \leq s_{EF}(n) = O(k_{EF}(n) + n)$

(b) $k_{EF}(n) \leq k_F(n) \leq O(k_{EF}(n))$

(c) there is $\varepsilon > 0$ *such that there are arbitrarily large tautologies* τ *for which it holds:*

$$\exp(\varepsilon \cdot k_{SF}^0(\tau)) < k_{EF}^0(\tau).$$

■

A particular corollary is that the task of establishing a superpolynomial lower bound for $s_{EF}(n)$ is equivalent to the task of establishing such a bound for $k_F(n)$.

We shall give another characterization of measures $k_F(n)$ and $s_{EF}(n)$ (Lemma 1.4) but first we need a technical result from [23]. The *logical depth* of a formula ϕ, $\ell dp(\phi)$, is the maximal length of a chain of subformulas of ϕ. It is inductively defined as follows:

1. $\ell dp(0) = \ell dp(1) = \ell dp(p_i) = 0$
2. $\ell dp(\neg\phi) = \ell dp(\phi) + 1$
3. $\ell dp(\phi \circ \psi) = max(\ell dp(\phi), \ell dp(\psi)) + 1$, for $\circ = \vee, \wedge$.

The following lemma is a corollary of a more general result for predicate calculus, cf. [23][2].

Lemma 1.3 *There exists constant c depending only on the particular definition of F such that whenever* $\phi_1, \ldots, \phi_k$ *is an F-proof then there is another F-proof* $\psi_1, \ldots, \psi_k$ *such that:*

1. $\ell dp(\psi_i) \leq c \cdot k$, *all i.*
2. *there is a substitution* δ *such that:*

$$\delta(\psi_i) = \phi_i$$

all i.

[2] A worse bound for the logical depth of formulas in a predicate calculus proof in terms of the number of proof steps appeared first in [35].

■

Define $\ell_F^0(\tau)$ to be the minimal ℓ such that there is an F-proof π of τ in which at most ℓ distinct formulas occur as subformulas, and put:

$$\ell_F(n) := \max\{\ell_F^0(\tau) \mid \tau \in TAUT\ , \ |\tau| \leq n\}.$$

Lemma 1.4 *For every tautology τ:*

$$k_F^0(\tau) \leq \ell_F^0(\tau) \leq c \cdot k_F^0(\tau) + |\tau|$$

where c is a constant depending on F only.

In particular, numbers $k_F(n) + n$ and $\ell_F(n) + n$ are proportional to each other.

Proof :

Let $\phi_1, \ldots, \phi_k$ be an F-proof of τ and constant c and formulas $\psi_1, \ldots, \psi_k$ those from Lemma 1.3. Let δ be a *minimal* substitution such that $\delta(\psi_k) = \phi_k = \tau$. Then sequence $\delta(\psi_1), \ldots, \delta(\psi_k)$ is a proof of τ and it contains at most $c \cdot k + |\tau|$ distinct formulas, as any subformula in it must occur in the depth at most c of the original proof or as a subformula of τ.

This proves the second inequality. The first one is trivial.

q.e.d.

We conclude this section by sketching a proof of a folklore theorem, essentially the only known lower bound to $s_F(n)$. The particular example $(\neg)^{(2m)}(1)$ was suggested by Buss; also [5, 24] relate to this result.

Theorem 1.5

$$s_F(n) = \Omega(n^2).$$

Sketch of proof:

Consider formula $\varphi := (\neg)^{(2m)}(1)$ and let π be its F-proof. As there is no tautology ψ whose substitution instance is φ and which satisfies $|\psi| < |\varphi|$, by Lemma 1.3 π must have $\Omega(m)$ proof steps and in fact, every subformula of φ must occur in some step of π in depth at most c (c the constant from Lemma 1.3). Hence the sum of the sizes of steps in π, i.e. $|\pi|$, must be at least $2m + (2m - c) + \ldots = \Omega(m^2) = \Omega(|\varphi|^2)$.

q.e.d.

Note that similar lower bound holds for any tautology φ for which there is no tautology ψ of smaller size $|\psi| < |\varphi|$ whose substitution instance would be φ.

2 Theories U_1^1 and V_1^1

Second order bounded arithmetic theories U_j^i and V_j^i were introduced in [7]. In this section we briefly recall the definition of U_1^1 and V_1^1 and obtain some basic information about their strength.

L is a second order language with first order functions and relations: $0, 1, x+y, x \cdot y, \lfloor \frac{x}{2} \rfloor, |x|, x \leq y, x = y$ (with the same meaning as in [7]), with second order variables $\alpha^t, \beta^s, \ldots$, where $t, s, \ldots$ are first order terms, ranging over finite sets of numbers, and with a membership relation $x \in \alpha^t$. Superscript t in α^t is introduced for technical reasons as an explicit upper bound to elements in α^t; we will mostly omit the superscript as such upper bounds are implicit in (proofs of) bounded formulas and we shall display it only to simplify the presentation.

Bounded formulas are formulas of L all of whose first order quantifiers are bounded. $\Sigma_0^{1,b}$-formulas are bounded formulas without second order quantifiers. $\Sigma_1^{1,b}$-formulas are bounded formulas in which all second order existential (resp. universal) quantifiers appear positively (resp. negatively). $\Pi_1^{1,b}$-formulas are defined dually and are logically equivalent to negations of $\Sigma_1^{1,b}$-formulas. A $\Sigma_1^{1,b}$ formula is $\Delta_1^{1,b}$ (resp. $\Delta_1^{1,b}$ in theory T) if it is equivalent to a $\Pi_1^{1,b}$-formula (resp. equivalent to it in T). In particular, all $\Sigma_0^{1,b}$-formulas are $\Delta_1^{1,b}$.

Theory $I\Sigma_0^{1,b}$ is a theory in language L with axioms: parts of axioms BASIC which do not involve function $x\#y$ (cf. [7]), the extensionality axiom, axioms stating that all sets are bounded:

$$\forall \alpha^{t(\overline{x})} \forall \overline{x}, y; y \in \alpha^t \rightarrow y \leq t(\overline{x}) \ ,$$

and the $\Sigma_0^{1,b}$-IND scheme:

$$A(0) \wedge \forall x (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)$$

for $A \in \Sigma_0^{1,b}$, and the *bounded* $\Sigma_0^{1,b} - CA$ scheme

$$\forall x \exists \psi \forall y < x; y \in \psi \equiv A(y),$$

again with $A \in \Sigma_0^{1,b}$.

Theory U_1^1 extends $I\Sigma_0^{1,b}$ by the $\Sigma_1^{1,b}$-LIND scheme:

$$A(0) \wedge \forall x \, (A(x) \rightarrow A(x+1)) \rightarrow \forall x A(|x|),$$

for $A \in \Sigma_1^{1,b}$.

Theory V_1^1 extends $I\Sigma_0^{1,b}$ by adopting the IND scheme for all $\Sigma_1^{1,b}$ formulas.[3]

[3] In accordance with the notation of [7] we should call these theories $\tilde{U}_1^1(BD)$ or $\tilde{V}_1^1(BD)$ but we choose to abuse the notation slightly to keep it simple as in all formulations these theories prove the same bounded formulas and there is no danger of confusion.

Theory V_1^1 contains U_1^1 and it is unknown whether this inclusion is proper or whether V_1^1 is somehow conservative over U_1^1. By [32] U_1^1 proves the $\Pi_1^{1,b}$-SEP scheme:

$$(\forall x, \neg A(x) \vee \neg B(x)) \rightarrow \forall x \exists \psi \forall y < x, (A(y) \rightarrow y \in \psi) \wedge (y \in \psi \rightarrow \neg B(y)),$$

with $A, B \in \Pi_1^{1,b}$, and hence also the $\Delta_1^{1,b}$-CA scheme:

$$(\forall x, A(x) \equiv B(x)) \rightarrow \forall x \exists \psi \forall y < x; y \in \psi \equiv A(y),$$

with $A \in \Sigma_1^{1,b}$ and $B \in \Pi_1^{1,b}$.

$\Delta_1^{1,b}$-CA over $I\Sigma_0^{1,b}$ readily gives the $\Delta_1^{1,b}$-IND scheme:

$$(\forall x, A(x) \equiv B(x)) \rightarrow (A(0) \wedge \forall x(A(x) \rightarrow A(x+1)) \rightarrow \forall x A(x)),$$

with $A \in \Sigma_1^{1,b}$ and $B \in \Pi_1^{1,b}$.

U_1^1 also proves the *choice scheme* $\Sigma_1^{1,b}$-AC:

$$\forall x < a \exists \psi A(x, \psi) \rightarrow \exists \varphi \forall x < a, A(x, (\varphi)_x),$$

with $A \in \Sigma_1^{1,b}$ and $y \in (\varphi)_x$ defined as $[x, y] \in \varphi$, $[x, y]$ being a pairing function.

Unfortunately, it appears unlikely that the useful scheme of *dependent choice* $\Sigma_1^{1,b}$-DC:

$$\forall x < a \forall \varphi \exists \psi A(x, \varphi, \psi) \rightarrow \forall \varphi \exists \theta, (\theta)_0 = \varphi \wedge \forall x < a, A(x, (\theta)_x, (\theta)_{x+1}),$$

(with $A \in \Sigma_1^{1,b}$) is available in U_1^1 as it is equivalent (over $I\Sigma_0^{1,b}$) to V_1^1.

From all these set-theoretic principles we shall need two particular closure properties, namely the counting functions and the evaluations of propositional formulas. Let $\Sigma_0^{1,b}$- formula $Enum(f, u, \alpha)$ denotes "f is an increasing bijection from u onto α".

Lemma 2.1 *U_1^1 proves that every set can be enumerated in increasing order:*

$$\forall \alpha \exists u \exists f; Enum(f, u, \alpha)$$

Proof :

Let a bound all elements of α and consider the formula

$$A(t) := \forall x, y \leq a \exists \beta \exists f, u; y \leq x + 2^t \rightarrow$$
$$\rightarrow (\beta = \{z \in \alpha | x \leq z \leq y\} \wedge Enum(f, u, \beta)).$$

This is a $\Sigma_1^{1,b}$-formula clearly satisfying induction assumptions $A(0)$ and $\forall t, A(t) \rightarrow A(t+1)$, and hence by $\Sigma_1^{1,b} - LIND$ $A(|a|)$ holds, i.e. f, u witnessing $A(|a|)$ for $x = 0$ and $y = a$ enumerate α in increasing order.

q.e.d.

The lemma implies that in U^1_1 one can $\Delta^{1,b}_1$-define the cardinality of a set:

$$|\alpha| := (\text{the unique } u \text{ s.t. } \exists f, Enum(f,u,\alpha)) \ ,$$

and hence also all combinatorial principles provable by elementary counting, e.g. the pigeonhole principle, are provable in U^1_1.

Propositional formulas, proofs and truth evaluations are coded as finite sets. *Formulas* are labelled binary trees with leaves labelled by $0,1$ or atoms and other nodes labelled by connectives (of appropriate arity). *Binary trees* are coded as finite partial orders with one maximal element (the root), no two incomparable elements majorizing a common element, and with every element having at most two successors.

Proofs are coded as particular finite sequences of formulas. A *truth evaluation of atoms* is a map of atoms into $\{0,1\}$. A *truth evaluation of formula* φ over evaluation α of its atoms is a labelling of nodes of φ by $0,1$ agreeing with α on atoms and fulfilling the usual truth table rules.

Clearly there are $\Sigma^{1,b}_0$-formulas $Fla(\varphi), Prf_P(\pi,\varphi), AtomEval(\varphi,\alpha)$ and $Eval(\eta,\varphi,\alpha)$ expressing that "φ is a formula", "π is a P-proof of φ" for $P = F$ or $P = EF$, "α evaluates atoms of φ" and "η is an evaluation of φ over evaluation of atoms α".

Lemma 2.2 *U^1_1 proves that every formula can be evaluated:*

$$\forall\varphi,\alpha;(Fla(\varphi)\wedge AtomEval(\varphi,\alpha)\rightarrow \exists\eta; Eval(\eta,\varphi,\alpha))$$

Proof :

Let φ be a formula and α evaluation of its atoms. Assume a is a bound to all nodes in φ and for $x < a$ let φ_x denote the subformula of φ with the root x. For ψ a subformula of φ and δ a set of some mutually incomparable nodes of φ, let $\psi\downarrow\delta$ denote the formula consisting of those nodes of ψ not majorized by any node of δ, with $y\in\delta$ being a leaf of $\varphi\downarrow\delta$ labelled by new atom q_y. Thus $\psi\downarrow\delta$ has at most $|\delta|$ new atoms not occurring in φ.

Consider formula:

$$(A(u) := \forall x < a\forall\delta(|\delta| \geq |a| - u), Fla(\varphi_x\downarrow\delta)\wedge|\varphi_x\downarrow\delta| \leq (3/2)^u \rightarrow$$

$$\rightarrow \forall\beta, AtomEval(\varphi\downarrow\delta,\alpha\cup\beta)\rightarrow\exists\eta; Eval(\eta,\varphi_x\downarrow\delta,\alpha\cup\beta).$$

As the size of δ is bounded by $|a|, \beta$ can be coded by a number bounded by a and hence $A(u)\in\Sigma^{1,b}_1$.

For $u = 0, |\varphi_x\downarrow\delta| = 1$ so $\varphi_x\downarrow\delta$ is just an atom or a constant and $A(0)$ clearly holds. The idea of the proof of implication $A(u)\rightarrow A(u+1)$ comes from [40] where Spira observed a

Claim: *Any formula* ψ_1 *has a subformula* ψ_2 *such that* $|\psi_2| \leq \frac{2}{3}|\psi_1|$ *and also* $|\psi_1| - |\psi_2| \leq \frac{2}{3}|\psi_1|$,

which is easy to formalize and prove in U_1^1.

Assume $A(u)$ and let $\varphi_x \downarrow \delta$ fulfill the hypotheses of $A(u+1)$. From Spira's claim follows that there is a node y in $\varphi_x \downarrow \delta (= \psi_1)$ s.t. both $\varphi_y \downarrow \delta (= \psi_2)$ and $\varphi_x \downarrow (\delta \cup \{y\})$ have size at most $(\frac{3}{2})^u$. By $A(u)$ then there is evaluation η' of $\varphi_y \downarrow \delta$ over any $\alpha \cup \beta$ and evaluation η'' of $\varphi_x \downarrow (\delta \cup \{y\})$ over $\alpha \cup \beta \cup \gamma$, where γ assigns to q_y the value computed by η'. Clearly then there is $\eta, \Sigma_0^{1,b}$- definable from η', η'', an evaluation of $\varphi_x \downarrow \delta$ over $\alpha \cup \beta$. This proves $A(u+1)$.

By $\Sigma_1^{1,b}$ - LIND then $A(\log_{3/2}(a))$ holds, i.e. there is an evaluation η of φ over α.

q.e.d.

Lemma 2.3 *There is a* $\Delta_1^{1,b}$ *in* U_1^1 *truth definition for propositional formulas, i.e. formula* $Tr(\varphi, \alpha)$ *formalizing "*φ *is true on evaluation* α *of its atoms" which is* $\Delta_1^{1,b}$ *in* U_1^1 *and about which* U_1^1 *proves the usual Tarski conditions.*

Proof :

Take $Tr(\varphi, \alpha) := \exists \eta; Eval(\eta, \varphi, \alpha) \wedge$ "η *gives* φ *value* 1". This is $\Delta_1^{1,b}$ as η is unique (in U_1^1).

q.e.d.

Now we formally define a translation of instances of $\Sigma_0^{1,b}$-formulas into propositional formulas mentioned in the introduction.

Let $A(\overline{x})$ be in $\Sigma_0^{1,b}$ and $\overline{n}$ be a tuple of numbers of the same length as $\overline{x}$ (as vectors). Then by induction on the logical complexity of A we define a propositional formula $\langle A(\overline{x}) \rangle_{\overline{n}}$:

(i) $\langle A(\overline{x}) \rangle_{\overline{n}} := 1$ (resp. $:= 0$) if $A(\overline{n})$ is a first order true (resp. false) atomic sentence,

(ii) $\langle A(\overline{x}) \rangle_{\overline{n}} := p_m^\alpha$, if $A(\overline{x})$ is of the form $t(\overline{x}) \in \alpha$ and m is the value of $t(\overline{n})$,

(iii) $\langle A(\overline{x}) \rangle_{\overline{n}} := \bigwedge_{i \leq m} p_i^{\alpha^t} \equiv p_i^{\beta^s}$ if $A(\overline{x})$ is of the form $\alpha^{t(\overline{x})} = \beta^{s(\overline{x})}$ and m is the larger of values $t(\overline{n}), s(\overline{n})$

(iv) $\langle \neg A \rangle_{\overline{n}} := \neg \langle A \rangle_{\overline{n}}$

(v) $\langle A \circ B \rangle_{\overline{n}} := \langle A \rangle_{\overline{n}} \circ \langle B \rangle_{\overline{n}}$, for $\circ = \wedge, \vee, \rightarrow$,

(vi) $\langle \exists y \leq t(\overline{x}) A(\overline{x}, y) \rangle_{\overline{n}} := \bigvee_{i \leq m} \langle A(\overline{x}, y) \rangle_{\overline{n}, i}$, if $t(\overline{n}) = m$,

(vii) $\langle \forall y \leq t(\overline{x}) A(\overline{x}, y) \rangle_{\overline{n}} := \bigwedge_{i \leq m} \langle A(\overline{x}, y) \rangle_{\overline{n}, i}$, if $t(\overline{n}) = m$.

In (iii),(vi) and (vii) $\bigwedge$ resp. $\bigvee$ denote conjunctions resp. disjunctions of $m+1$ formulae $\langle A(\overline{x}, y) \rangle_{\overline{n}, i}$ with brackets associated, for example, to the left.

Theorem 2.4 *U_1^1 proves that F is a sound proof system, i.e.*

$$\forall \varphi, \alpha, \pi; Prf_F(\pi, \varphi) \wedge AtomEval(\varphi, \alpha) \wedge Fla(\varphi) \rightarrow Tr(\varphi, \alpha).$$

In particular, if $A(x)$ is $\Sigma_0^{1,b}$ then U_1^1 proves:

$$\forall \pi \forall u, Prf_F(\pi, \langle A(x) \rangle_u) \rightarrow A(u).$$

Proof :

As truth definition $Tr(\varphi, \alpha)$ is $\Delta_1^{1,b}$, by $\Delta_1^{1,b}$-IND available in U_1^1 we prove that every step in an F-proof π is true under any fixed evaluation α of atoms.

If φ is $\langle A(x) \rangle_u$, where $A(x)$ is a $\Sigma_0^{1,b}$-formula with set variable α, $A(u)$ follows from $Tr(\varphi, \tilde{\alpha})$ by Tarski's conditions where by definition $\tilde{\alpha}$ evaluates atoms p_i^α to 1 iff $i \in \alpha$.

q.e.d.

Theorem 2.5 *V_1^1 proves that EF is a sound proof system:*

$$\forall \varphi, \alpha, \pi; Prf_{EF}(\pi, \varphi) \wedge AtomEval(\varphi, \alpha) \wedge Fla(\varphi) \rightarrow Tr(\varphi, \alpha).$$

In particular, if $A(x)$ is $\Sigma_0^{1,b}$ then V_1^1 proves:

$$\forall u, \pi; Prf_{EF}(\pi, \langle A(x) \rangle_u) \rightarrow A(u).$$

Proof :

By induction on the number of steps in π show that there is evaluation β of the extension atoms of π such that all steps in π are true under evaluation $\alpha \cup \beta$ of atoms occurring in π. The existence of β follows by $\Sigma_1^{1,b}$-IND.

q.e.d.

Now we reformulate Theorems 2.4 and 2.5 contrapositively, similarly to a theorem in [2], in a form suggesting that a way how to prove a lower bound on $s_F(n)$ or $s_{EF}(n)$ is to construct a particular model of theory U_1^1 or V_1^1 respectively.

A model of $I\Sigma_0^{1,b}$ has the form $M = (N_M, X_M)$, where N_M is the first order part (numbers) and X_M is the second order part (sets). To distinguish between set variables $\alpha, \beta, \ldots$ and elements of X_M we shall use $\sim$: hence $\tilde{\alpha}, \tilde{\beta}, \ldots$ are elements of a model.

Model M' is an *extension* of model M iff $N_M \subseteq N_{M'}$ and $X_M \subseteq X_{M'}$, and the extension is $\Sigma_0^{1,b}$-*elementary* iff $\Sigma_0^{1,b}$-sentences with parameters from M have the same truth value in M and M'.

Theorem 2.6 *Let $A(x,\alpha)$ be a $\Sigma_0^{1,b}$-formula with only free variables x and α. Let M be a non-standard model of true arithmetic $Th(\omega)$ and $n \in M\backslash\omega$ be a non-standard element.*

Assume that for every $k < \omega$ and every set $\tilde{\pi} \subseteq n^k$ coded in M there is a family $X \subseteq \bigcup_{k<\omega} P(n^k)$ and $\tilde{\alpha} \in X$ such that:

(i) $\tilde{\pi} \in X$

(ii) $(\bigcup_{k<\omega} n^k, X) \models U_1^1$

(iii) $(\bigcup_{k<\omega} n^k, X) \models \neg A(n,\tilde{\alpha})$.

Then formulas $\langle A(x)\rangle_m, m < \omega$, do not have polynomial size F-proofs. If the model in (ii) satisfies V_1^1 then formulas $\langle A(x)\rangle_m$ do not have polynomial size EF-proofs.

Proof :

Assume that formulas $\langle A(x)\rangle_m, m < \omega$, do have polynomial size F-proofs. As M satisfies true arithmetic there is $k < \omega$ such that for every element $n \in M$, M codes an F-proof of $\langle A(x)\rangle_n$ of size at most n^k. Let $\tilde{\pi} \subseteq n^k$ be such a proof.

Take X and $\tilde{\alpha} \in X$ satisfying conditions (i)-(iii). Then $(\bigcup_{k<\omega} n^k, X)$ is a model of U_1^1 in which the propositional translation of a false $\Sigma_0^{1,b}$-sentence $A(n)$ has an F-proof, contradicting Theorem 2.4.

The case of V_1^1 is entirely the same.

q.e.d.

We shall study in section 4 the question for what formulas A one should attempt to construct the extension.

3 Simulation of U_1^1 and V_1^1 by F and EF

In this section we obtain a form of converse statements to Theorems 2.4 and 2.5.

Theorem 3.1 *Let $A(x)$ be a $\Sigma_0^{1,b}$-formula and assume that V_1^1 proves $\forall x A(x)$. Then formulas $\langle A(x)\rangle_n$ have polynomial size EF-proofs.*

Proof :

Assume D is a V_1^1-proof of sequent $\rightarrow A(a)$; by free cut elimination we may assume that all formulas in D have the form $\exists\varphi C(\overline{x},\overline{\alpha},\varphi)$ with C in $\Sigma_0^{1,b}$, cf. [7, 32]. By induction on the number of steps in D show that if:

$$\exists\psi_1 B_1(\overline{x},\overline{\alpha},\psi_1),\ldots,\exists\psi_u B_u(\overline{x},\overline{\alpha},\psi_u) \rightarrow \exists\varphi_1 C_1(\overline{x},\overline{\alpha},\varphi_1),\ldots,\exists\varphi_v C_v(\overline{x},\overline{\alpha},\varphi_v)$$

is a sequent in D then there is constant k such that for all $\overline{m}$ there is an EF-sequence (not necessarily a proof) of size at most $(\max(\overline{m}))^k$ ending with formula:

$$\bigwedge_{i\leq u} \langle B_i\rangle_{\overline{m}}(\overline{p}^\alpha, \overline{p}^{\psi_i}) \to \bigvee_{j\leq v} \langle C_j\rangle_{\overline{m}}(\overline{p}^\alpha, \overline{p}^{\varphi_j})$$

(recall that $\overline{p}^\alpha = (p_0^\alpha, p_1^\alpha, \ldots))$. Moreover, in this EF-sequence none of the atoms p_t^α or $p_t^{\psi_i}$ corresponding to a free second order variable resp. to a second order variable from an antecedent is an extension atom.

The only nontrivial rules to treat are the introduction of second order $\exists$ to the succedent and $\Sigma_1^{1,b}$-IND.

Assume that in the former case the minor formula of the inference is $C(\overline{x}, \overline{\alpha}, \frac{t\in\varphi}{E(\overline{x},t,\overline{\alpha})})$ with both $C, E \in \Sigma_0^{1,b}$, and the principal formula is $\exists\varphi C(\overline{x}, \overline{\alpha}, \varphi)$. Introduce new atom $p_t^\varphi \equiv \langle E\rangle_{\overline{m},t}(\overline{p}^\alpha)$. Then equivalence

$$\langle C\rangle_{\overline{m}}(\overline{p}^\alpha, \frac{p_t^\varphi}{\langle E\rangle_{\overline{m},t}}) \equiv \langle C\rangle_{\overline{m}}(\overline{p}^\alpha, \overline{p}^\varphi)$$

can be derived from the new extension axioms by an F-derivation of size

$$O((|\langle C\rangle_{\overline{m}}| + |\langle E\rangle_{\overline{m},t}|)^2) = (\max(\overline{m}))^{O(1)},$$

as t is implicitly bounded in E by a power of $\max(\overline{m})$. This concludes the first case.

In the case of a $\Sigma_1^{1,b}$-IND inference

$$\frac{\exists\varphi_b C(b, \varphi_b) \to \exists\varphi_{b+1} C(b+1, \varphi_{b+1})}{\exists\varphi_0 C(0, \varphi_0) \to \exists\varphi_n C(n, \varphi_n)}$$

(where for simplicity we omitted other free variables and side formulas) by the induction hypothesis we have polynomial size EF-sequences ending with formulas:

$$\langle C\rangle_{\overline{m},u}(\overline{p}^{\varphi_u}) \to \langle C\rangle_{\overline{m},u+1}(\overline{p}^{\varphi_{u+1}})$$

for $u = 0, 1, \ldots, n-1$. Joining these implications by $n-1$ cuts gives an EF-sequence ending with implication:

$$\langle C\rangle_{\overline{m},0}(\overline{p}^{\varphi_0}) \to \langle C\rangle_{\overline{m},n}(\overline{p}^{\varphi_n}),$$

of total size polynomial in $\max(\overline{m}, n)$.

q.e.d.

The preceding proof can be modified a bit to yield the following statement.

Theorem 3.2 *Let $A(x)$ be a $\Sigma_0^{1,b}$-formula and assume that U_1^1 proves $\forall x A(x)$. Then formulas $\langle A(x)\rangle_n$ have F-proofs of size $n^{(\log n)^{O(1)}}$.*

Proof :

By Theorem 3.1 there is an EF-proof of $\langle A(x)\rangle_n$ of size $n^{O(1)}$. Moreover, by the proof of that theorem in these EF -proofs there will be only $(\log n)^{O(1)}$ extension atoms since the starting arithmetic proof D uses $\Sigma_1^{1,b}$-LIND instead of $\Sigma_1^{1,b}$-IND. There will be at most $O(\log^k n)$ extension atoms if there are k $\Sigma_1^{1,b}$-LIND inferences in D.

Take such an EF-proof and replace in it the last introduced extension atom by its definition: this yields a new EF-proof of size $n^{O(1)} \cdot n^{O(1)}$ with one less application of the extension rule. Repeating this procedure until all extension axioms are eliminated produces an F-proof of size $n^{(\log n)^{O(1)}}$.

q.e.d.

In a search for some theory corresponding to polynomial size Frege proofs one should look for an extension of $I\Sigma_0^{1,b}$ with a clear combinatorial meaning and not just for any extension.[4] For example, an extension of $I\Sigma_0^{1,b}$ by a $\Pi_1^{1,b}$-sentence saying that F is sound (any evaluation of any F-provable formula over any evaluation of its atoms outputs the truth-value 1) has the property that if it proves a $\Sigma_0^{1,b}$-formula $A(x)$ then all $\langle A\rangle_n$ have polynomial size F-proofs (this follows by arguments analogous to those in proofs of 3.4 and 3.5, employing [9] in an essential way). Such a theory however, does not increase our understanding of F [5] and so we shall not treat the details. Instead consider a theory $\left(I\Sigma_0^{1,b}\right)^{count}$ which is an extension of $I\Sigma_0^{1,b}$ by the axiom

$$\forall\alpha\exists f, u; Enum(f, u, \alpha).$$

By Lemma 2.1, this theory is a subtheory of U_1^1.

The following appears to be an interesting open question.

Problem 1

Does $\left(I\Sigma_0^{1,b}\right)^{count}$ *prove the soundness of* F*? Does it prove that every formula can be evaluated over any evaluation of its atoms?*

In [27] we proved that F polynomially simulates proofs in this theory.

It is straightforward to define an extension of F by new connectives allowing counting such that *constant-depth,* polynomial size proofs in this system correspond to $\left(I\Sigma_0^{1,b}\right)^{count}$. For instance, let FC (for F with *counting*) be a system

[4] [3] defined a theory corresponding to polynomial-size F.

[5] This theory also does not prove that every formula can be evaluated over any evaluation of its atoms. This is because the witnessing of such a proof would allow to express size n formulas by size $n^{O(1)}$ constant-depth circuits (cf. Corollary 3.3) which is impossible by [1, 20].

extending F by new (infinitely many) connectives $C_{n,k}(\phi_1, \ldots, \phi_n)$, for $1 \leq n$ and $k \leq n$, with intended meaning that $C_{n,k}(\phi_1, \ldots, \phi_n)$ is true iff the number of true ϕ_i's is k, and by adding new axioms:

1. $A \equiv C_{1,1}(A)$
2. $C_{n,0}(A_1, \ldots, A_n) \equiv (\neg A_1 \wedge \ldots \wedge \neg A_n)$
3. $C_{n+1,k+1}(A_1, \ldots, A_{n+1}) \equiv$

   $$\equiv [\ (C_{n,k}(A_1, \ldots, A_n) \wedge A_{n+1})\ \vee\ (C_{n,k+1}(A_1, \ldots, A_n) \wedge \neg A_{n+1})\ ]$$

   if $k < n$
4. $C_{n+1,n+1}(A_1, \ldots, A_{n+1}) \equiv [\ (C_{n,n}(A_1, \ldots, A_n) \wedge A_{n+1})\ ]$.

For every fixed d, the depth d FC-proofs are provably sound in $\left(I\Sigma_0^{1,b}\right)^{count}$ and, on the other side, tautologies $\langle A \rangle_n$ derived from a $\Sigma_0^{1,b}$-consequence of $\left(I\Sigma_0^{1,b}\right)^{count}$ have polynomial size, constant-depth FC-proofs.

Constant-depth FC-proofs p-simulate the *cutting planes proof system,* a system working with linear inequalities with integer coefficients (expressing that a linear combination of truth values of some literals have at least a particular integer value) with several natural rules, see [18]. This system contains the resolution system and it is open whether cutting planes p-simulate constant-depth F-proofs. Goerdt [21] showed, building on [8], that F p-simulates the cutting planes.

Hence an interesting open problem, clearly related to the one above, is the following:

Problem 2
Does constant-depth FC system p-simulate F?[6]

Next we consider three corollaries to Theorems 3.1 and 3.2. The first one is known and we offer a new proof.

Corollary 3.3 ([37]) *Let $A(x)$ be $\Sigma_0^{1,b}$ and assume that $I\Sigma_0^{1,b}$ proves $\forall x A(x)$. Then formulas $\langle A(x) \rangle_n$ have F-proofs of polynomial size and constant depth (the depth measured by the number of alterations of connectives).*

[6] This appears to be linked also to an open question whether there is d and k such that every boolean formula of size n is equivalent to a threshold circuit od depth d and size at most n^k. A negative answer to this implies a negative answer to the problem above, as an FC-proof witnessing that in $(I\Sigma_0^{1,b})^{count}$ every formula of size n can be evaluated on every input would provide an equivalent polynomial size, constant depth threshold circuit.

Proof :

By the free cut elimination we may assume that in the proof of $A(a)$ occur only $\Sigma_0^{1,b}$-formulas. In the EF-proof of $\langle A(x)\rangle_n$ constructed in Theorem 3.1 there will be then no extension axioms, and all formulas are translations of $\Sigma_0^{1,b}$-formulas and hence of bounded depth. After the elimination of the axioms in the proof of Theorem 3.2, the new F-proofs will have size $n^{O(1)}$ and constant depth.

q.e.d.

The next corollary is a weaker form of a statement implicitly contained in [39] and explicitly proved in [27]; namely, one can even guarantee the existence of a proof of size $n^{O(1)}$ with formulas of logical depth $O(log\ n) + \ell dp(\varphi)$. We present the weaker form as it admits a simple proof using the relations between U_1^1 and F.

Corollary 3.4 *Assume φ has an F-proof of size n. Then there is an F-proof of φ of size $n^{(\log n)^{O(1)}}$ in which all formulas have the logical depth*

$$\log^{O(1)} n + \ell dp(\varphi)\ .$$

Proof :

By Theorem 2.4 theory U_1^1 proves

$$Prf_F(\pi, \varphi) \to Tr(\varphi, \alpha),$$

and so also

$$Prf_F(\pi, \varphi) \wedge Eval(\eta, \varphi, \alpha) \to \text{“}\eta_0 = 1\text{”},$$

where we may assume that η_0 is the label the evaluation η assigns to φ, i.e. the value of φ over evaluation α of its atoms.

By Theorem 3.2 there are F-proofs π_1 of size $n^{(\log n)^{O(1)}}$ of:

$$\langle Prf\rangle_n(\overline{p}^\pi, \overline{p}^\varphi) \wedge \langle Eval\rangle_n(\overline{p}^\eta, \overline{p}^\varphi, \overline{p}^\alpha) \to p_0^\eta$$

in which all formulas have the logical depth at most $\log^{O(1)} n$ (because the depth increases by at most $O(\log n)$ for every eliminated extension atom).

Construct two F-proofs π_2 and π_3, both of size $n^{O(1)}$ and the logical depth $O(\log n)$. Proof π_2 is a proof of:

$$\langle Prf\rangle_n(\tilde{\pi}, \tilde{\varphi}),$$

where $(\tilde{\pi}, \tilde{\varphi})$ are truth evaluations of $\overline{p}^\pi$ and $\overline{p}^\varphi$ corresponding to $0-1$ sequences coding an actual F-proof π of size $\leq n$ of an actual formula φ. This is simple as the formula is a true (as we assume that π is an F-proof of φ) boolean sentence and its proof consists just of its evaluation.

The second proof π_3 is a proof of:

$$\langle Eval\rangle_n(\frac{p_i^\eta}{\varphi_i}, \tilde{\varphi}, \overline{p}^\alpha)$$

where φ_i is a subformula of φ corresponding to node i with atoms $\overline{p}^\alpha$. This proof π_3 exists since the evaluation of φ by (values of) subformulas φ_i clearly fulfills the local truth table conditions.

Now replace in π_1 every atom p_i^η by φ_i and join the resulting proof by cuts with π_2 and π_3; this yields an F-proof of φ_0, i.e. of φ.

q.e.d.

Corollary 3.5 *Assume that V_1^1 is conservative over U_1^1 w.r.t. $\Sigma_0^{1,b}$-formulas. Then EF has at most $n^{(\log n)^{O(1)}}$ speed-up over F. In particular, every formula provable in F in k proof steps has then also an F-proof of size $k^{(\log k)^{O(1)}}$.*

Proof :

By the assumption and Theorem 2.5 U_1^1 proves:

$$Prf_{EF}(\pi, \varphi) \wedge Eval(\eta, \varphi, \alpha) \rightarrow \text{“}\eta_0 = 1\text{”}.$$

Hence there are F-proofs of translations of this formula of the size $n^{(\log n)^{O(1)}}$, and this is used for a construction of an F-proof of φ from any EF-proof π of φ in the same way as in the proof of Corollary 3.4.

The second part of the corollary follows from the first part using also Theorem 1.2.

q.e.d.

4 Hard tautologies

The following definition is a formalization of the informal notion of hard tautology.

Definition 4.1 *(a) Sequence $\{\tau_n\}$ of tautologies is* hard *for proof system P iff the following three conditions are satisfied:*

(i) there exists a polynomial time algorithm producing τ_n from string $1\ldots1$ (n-times)

(ii) $|\tau_n| \geq n$, all n

(iii) for every polynomial $q(x)$ there is n such that:

$$s_P^0(\tau_n) \geq q(|\tau_n|)\ .$$

A sequence of tautologies satisfying (i) and (ii) will be called a p-time sequence of tautologies*.*

(b) Let $\{\tau_n\}$ be a p-time sequence of tautologies and P be a proof system. String π is a proof of σ in the proof system:

$$P + \{\tau_n\}$$

iff π is a P-proof of an implication of the form:

$$(\phi_1 \wedge \ldots \wedge \phi_k) \rightarrow \sigma$$

where each ϕ_i is a substitution instance of some τ_{n_i}.

(c) Let $\{\tau_n\}$ and $\{\sigma_n\}$ be two p-time sequences of tautologies and let P be a proof system. We say that $\{\tau_n\}$ is reducible over P to $\{\sigma_n\}$*, denoted $\{\tau_n\} \leq_P \{\sigma_n\}$, iff $s^0_Q(\tau_n) = |\tau_n|^{O(1)}$ for $Q := P + \{\sigma_n\}$.*

We say that $\{\sigma_n\}$ is harder than $\{\tau_n\}$ over P *iff $\{\tau_n\}$ reduces over P to $\{\sigma_n\}$ but not vice versa.*

■

The following theorem restates some results from [28] and we shall not reprove it here.

Theorem 4.2 *Let P be a proof system p-simulating EF. Then the following two propositions hold :*

(a) There is a p-time sequence of tautologies $\{\tau_n\}$ such that for proof system $Q := EF + \{\tau_n\}$ it holds:

$$s_Q(n)^{\Omega(1)} = s_P(n) = s_Q(n)^{O(1)} \ .$$

(b) The following two conditions are equivalent:

(i) there is a sequence of tautologies hard for P

(ii) system P is not optimal (i.e. there is Q such that no power of $s_Q(n)$) majorizes $s_P(n)$).

■

Tautologies $\{\tau_n\}$ axiomatizing P over EF obtained from [28] express the soundness of P. It is an interesting question whether one can find such τ_n of the form $\langle A \rangle_n$, A a $\Sigma^{1,b}_0$-formula expressing a natural finite combinatorial principle. No such principle is known which would make a plausible candidate for tautologies hard for F or EF.

A weaker construction is based on NP-completeness results. Any $coNP$-property of finite structures can be expressed by a $\Pi^{1,b}_1$-formula. As a specific example consider the set of *non-3-colorable* graphs. For fixed n take $\binom{n}{2}$ atoms p_{ij} (for possible edges in a graph with n vertices $i, j, \ldots$) and another $3n$ atoms a_i, b_i, c_i (for coding a 3-coloring of the vertices), and consider the formula

$$C_n := \bigwedge_i (a_i \vee b_i \vee c_i) \ \wedge \ \bigwedge_i [(\neg a_i \wedge \neg b_i) \vee (\neg a_i \wedge \neg c_i) \vee (\neg b_i \wedge \neg c_i)]$$

expressing that a, b, c define a coloring, and take formula

$$A_n := C_n \to \bigvee_{ij} (p_{ij} \wedge [(a_i \wedge a_j) \vee (b_i \wedge b_j) \vee (c_i \wedge c_j)]) \ .$$

Any particular graph G with n nodes defines an instance $A_G(a, b, c)$ of $A_n(a, b, c, p)$ by evaluating atoms p_{ij} as follows:

$$p_{ij} := \begin{cases} 1 & \text{if } \{i, j\} \text{ is an edge in } G \\ 0 & \text{otherwise} \end{cases}$$

Hence A_G is a tautology iff G is not 3-colorable.

Theorem 4.3 *Assume that $s_{EF}(n)$ is not polynomially bounded. Then there is a sequence of graphs $\{G_n\}$ satisfying:*

1. *each G_n is a non-3-colorable graph with n vertices*
2. *there is no polynomial $q(x)$ such that:*

$$s^0_{EF}(A_{G_n}) \leq q(|A_{G_n}|)$$

   would hold for all n.

■

The idea of the proof is that V^1_1 proves the NP-completeness of 3-colorability and hence the set of all tautologies can be reduced, via a $\Delta^{1,b}_1$-definable map, to the set of non-3-colorable graphs, and that V^1_1 proves also that G is non-3-colorable iff A_{G_n} is a tautology. By methods of section 3 these proofs can be simulated by system EF.

Note that we do not claim that sequence $\{A_{G_n}\}$ is hard for EF as we do not have a polynomial time algorithm which would construct graphs G_n. To get such a sequence one would have to strengthen the assumption to the hypothesis that EF is not optimal, which appears to be stronger than the hypothesis of the theorem, cf. [28].

Theorem 4.3 implies that a type of extension of models of V^1_1 whose construction would yield a superpolynomial lower bound to $s_{EF}(n)$ is the following: the extension M' of M contains a 3-colorable graph $G \in X_M$ which is not 3-colorable in M.

5 A Forcing Construction

In this section we consider extensions of models of V_1^1. In the next section we shall present a framework for lower bound proofs for EF, and generally for any extension of EF by extra axioms. The motivation for it comes from a particular model-theoretic proof of Theorem 5.1 below which is a subject of this section.

The following theorem is a consequence of Theorems 2.5 and 3.1.[7]

Theorem 5.1 *Let M be a model of V_1^1 and $\tilde{\tau}(p_1, \ldots, p_n) \in X_M$ a propositional formula in M. Then the following two conditions are equivalent:*

(a) In M there is no EF-proof of $\tilde{\tau}$.

(b) There is a $\Sigma_0^{1,b}$-elementary extension of M in which $\tilde{\neg\tau}$ is satisfiable.

Proof :
Assume first that (b) holds while (a) fails, and that $\tilde{\pi} \in X_M$ is an EF-proof in M of $\tilde{\tau}(\overline{p})$. As M' extends M, $\tilde{\pi} \in X_{M'}$, and as the extension is $\Sigma_0^{1,b}$-elementary, $\tilde{\pi}$ is an EF-proof in M' too. M' is a model of V_1^1 hence by Theorem 2.5 $\tilde{\pi}$ is a proof of a tautology, i.e. $\tilde{\tau}$ is satisfied in M' by all evaluations. But this contradicts (b).

Assume now that (b) fails which means that the theory in the language with names for all elements of $N_M \cup X_M$ and new constants $\underline{\alpha}, \underline{\eta}$ and consisting of axioms:

(i) V_1^1,

(ii) a $\Sigma_0^{1,b}$-formula $B(\underline{\alpha}, \tilde{\neg\tau}, \underline{\eta})$, saying:

$$Eval(\underline{\eta}, \tilde{\neg\tau}, \underline{\alpha}) \textit{ and } ``\underline{\eta} \textit{ gives } \tilde{\neg\tau} \textit{ value } 1"$$

(cf. Section 2),

(iii) all $\Sigma_0^{1,b}$-sentences true in M,

is inconsistent.

By compactness V_1^1 proves an implication of the form

$$C \to \neg B(\underline{\alpha}, \tilde{\neg\tau}, \underline{\eta}) \ ,$$

where C is a conjunction of some formulas from (iii). By Theorem 3.1, formula

$$\langle C \rangle_u \to \langle \neg B(\underline{\alpha}, \tilde{\neg\tau}, \underline{\eta}) \rangle_{n,m}$$

is, for suitably large $u \in N_M$, EF-provable in M. As C is true in M, $\langle C \rangle_u$ has an EF-proof in M too, and hence has also $\langle \neg B \rangle_{n,m}(\overline{p}, \tilde{\neg\tau}, \overline{q})$ for suitable $\overline{p}$ and $\overline{q}$. The latter formula implies however, in EF, formula $\tilde{\tau}$ itself (cf. [28]). This shows that (a) fails.

[7] See [30] for analogous argument in the context of theory S_2^1.

q.e.d.

This theorem is relevant to the extensions considered at the end of the previous section: take $G \in X_M$ a non-3-colorable graph and

$$\tilde{\tau} := A_G \ .$$

We are interested in a model-theoretic construction of model M' from model M assuming condition (a).[8] The ultimate goal is to learn how to construct some extensions for suitable G *without* assuming condition (a).

Assume that M is countable, and that M and $\tilde{\tau} \in X_M$ satisfy (a). We will construct M' as follows. By compactness there is a countable elementary extension M_0 of M (satisfying therefore V_1^1) such that:

(i) there is $t \in N_{M_0}$ such that for all $v \in N_M$, $v < t$,

(ii) in M_0 there is no EF-proof of $\tilde{\tau}$.

Let M^* be a substructure of M_0 defined by:

(i) $N_{M^*} = \{v \in N_{M_0} | \exists w \in N_M, v \leq w\}$

(ii) $X_{M^*} = \{\tilde{\beta} \in X_{M_0} | \tilde{\beta} \subseteq N_{M^*}\}$.

Let $\overline{p}$ be the atoms of $\tilde{\tau}$ and let $Fle(\overline{p}) \subseteq X_{M_0}$ be the collection of boolean formulas with atoms among $\overline{p}$. Further let A be the set of atoms $\overline{p}$ plus new atoms of the form q_ψ, one for each $\psi \in Fle(\overline{p})$, and let $Fle \subseteq X_{M_0}$ be the set of formulas with atoms among A.

Let $C \subseteq X_{M_0}$ be the family of all tuples of propositional atoms from $A \cup \{0, 1\}$:

$$C = \{\beta = (\beta_1, \ldots, \beta_m) \in X_{M_0} \mid \forall i \leq m, \beta_i \in A \cup \{0, 1\}\}$$

and for $\beta = (\beta_1, \ldots, \beta_m) \in C$ define the length $|\beta|$ to be m.

Let $C^* = \{\beta \in C \mid |\beta| \in N_{M^*}\}$ and $Fle^* = \{\phi \in Fle \mid |\phi| \in N_{M^*}\}$. We will consider $\tilde{\beta} \in X_{M_0}$ simultaneously also as an element of C: the tuple of bits of the characteristic function of $\tilde{\beta}$; note that for such $\tilde{\beta}$: $\tilde{\beta} \in C^* \equiv \beta \in X_{M^*}$. The following claim is established by induction on the logical complexity of B. Note that the formula $B(\beta)$ contains implicitly a number parameter in the term bounding the size of intervals whose subsets may be substituted for β (see the beginning of section 2).

[8] In 1987 at the meeting *Logic, Methodology and Philosophy of Science* in Moscow, A. Wilkie (unpublished) sketched a model-theoretic argument proving that if S_2^1 proves that $NP = coNP$ then tautologies have polynomial size proofs in EF (this result follows from earlier [16] proving the same statement for the theory PV and from the $\forall\Sigma_1^b$-conservativity of S_2^1 over PV established in [7]). The construction below generalizes his completeness-type argument to an argument which is more amenable to a finitisation.

Claim 1: *Let $B(\beta)$ be a $\Sigma_0^{1,b}$-formula and $\tilde{\beta} \in X_{M^*}$. Then*

$$M^* \models B(\tilde{\beta}) \to \exists \pi Prf_{EF}(\pi, \langle B \rangle_{|\tilde{\beta}|}(\overline{p}^\beta/\tilde{\beta}))$$

.

We will construct set $G \subseteq Fle$ satisfying the following conditions:

1. $\neg \tilde{\tau} \in G$
2. for all $\psi \in Fle^*$ exactly one of ψ, $\neg\psi$ is in G
3. whenever $\pi \in X_{M_0}$ is an EF-proof of ψ from assumptions $\psi_1, \ldots, \psi_r$, $|\pi| \in N_{M^*}$ and all $\psi_i \in G$, then also $\psi \in G$
4. if $\psi \in G \cap Fle^*$ and $\psi = \bigvee_{1 \leq i \leq r} \psi_i$ then $\psi_j \in G$ for some $1 \leq j \leq r$
5. for any $\Sigma_0^{1,b}$-formula $H(\phi, x)$ and for any term $t(x)$ with parameters from C^* and any $v \in N_{M^*}$ at least one of the following three conditions holds:
   (a) $\neg\langle H(\phi, 0)\rangle_v(\tilde{\delta}) \in G$, all $\tilde{\delta} \in C^*$ of length $\leq t(v)$
   (b) $\langle H(\phi, v)\rangle_v(\tilde{\delta}) \in G$, for some $\tilde{\delta} \in C^*$ of length $\leq t(v)$
   (c) there is $v' < v$ such that $\langle H(\phi, v')\rangle_v(\tilde{\delta}) \in G$ for some $\tilde{\delta} \in C^*$ of length $\leq t(v)$, but $\neg\langle H(\phi, v'+1)\rangle_v(\tilde{\epsilon}) \in G$ for all $\tilde{\epsilon} \in C^*$ of length $\leq t(v)$

(Term $t(v)$ bounds implicitly the interval whose subsets are substitutable for ϕ in H for $x \leq v$.)

Assume for a moment that we have such a set G. Define structure $M^*[G]$ by:

$$N_{M^*[G]} = N_{M^*} \text{ and } X_{M^*[G]} = C^*/\sim\ ,$$

where $\sim$ is an equivalence relation defined by:

$$\tilde{\beta}_1 \sim \tilde{\beta}_2 \text{ iff } \langle \beta_1 = \beta_2 \rangle_u(\tilde{\beta}_1, \tilde{\beta}_2) \in G$$

(u the maximum of the lengths of $\tilde{\beta}_1, \tilde{\beta}_2$). Note that $M^*[G]$ is an extension of M^* and hence of M too.

Claim 2: *Let $B(\beta)$ be any $\Sigma_0^{1,b}$-formula with parameters from C^* and $\tilde{\beta} \in C^*$. Then we have for all u sufficiently large:*

$$M^*[G] \models B(\tilde{\beta}/\sim) \textit{ iff } \langle B \rangle_u(\tilde{\beta}) \in G.$$

In particular, $M^*[G]$ is a $\Sigma_0^{1,b}$-elementary extension of M.

The claim follows from conditions (2)-(4) posed on G. For example, that all $\Sigma_0^{1,b}$-sentences true in M hold also in $M^*[G]$ follows from condition (3) and *Claim 1* .

Claim 3: *Structure $M^*[G]$ is a model of V_1^1.*

Condition (5) posed on G guarantees that induction for every $\Sigma_1^{1,b}$-formula $\exists\phi H(\phi, x)$ holds up to every $v \in N_{M^*[G]}$. The other axioms hold in $M^*[G]$ obviously. In particular, $\Sigma_0^{1,b}$-comprehension holds since in C we have explicit names for the sets defined by $\Sigma_0^{1,b}$-formulas. The tuple $(q_{\psi_0}, \ldots, q_{\psi_m})$ where:

$$\psi_i := \langle B\rangle_i(\beta)$$

represents the set $\{i \leq m \mid B(\beta, i)\}$.

Claim 4: *There is a truth evaluation $\tilde{\alpha} \in X_{M^*[G]}$ of atoms of $\tilde{\tau}$ such that*

$$M^*[G] \models Tr(\tilde{\neg\tau}, \tilde{\alpha}) \ .$$

By condition (1) posed on G and *Claim 2* , $\tilde{\alpha}$ is a satisfying assignment for $\neg\tilde{\tau}$ in $M^*[G]$, where $\tilde{\alpha} = \overline{p}^{\alpha}/\sim$.

It remains to construct the set G satisfying the above five requirements. First we will state two simple technical properties of the system EF.

Form a set $T \subseteq Fle$ consisting of formulas:

(i) $q_{p_i} \equiv p_i$, whenever $p_i \in \{\overline{p}\}$

(ii) $q_{\neg\psi} \equiv (\neg q_\psi)$, whenever $\psi \in Fle(\overline{p})$

(iii) $q_{\psi_1\circ\psi_2} \equiv (q_{\psi_1} \circ q_{\psi_2})$, whenever $\psi_1,\ \psi_2 \in Fle(\overline{p})$ and $\circ \in \{\vee, \wedge\}$

A set of formulas $S \subseteq Fle$ is said to ℓ-*entail* formula ψ iff there is an F-proof of ψ of size at most ℓ with axioms from $S \cup T$. Set S is called ℓ-*consistent* iff S does not ℓ-entail 0.

Claim 5: *Let $S \subseteq Fle$ be a $\Delta_1^{1,b}$-definable family in M_0, and assume that ψ has an EF-proof from S of size ℓ in M_0. Then S $O(\ell^2)$-entails ψ in M_0 too.*

This follows as every extension axiom of size t in the EF-proof can be proved (after suitably renaming extension axioms) from T by an F-proof of size $O(t^2)$.

Claim 6: *Let $S \subseteq Fle$ be a $\Delta_1^{1,b}$- definable family in M_0, and assume that S is ℓ-consistent in M_0, where ℓ is non-standard.*

Then for every formula ψ of size at most $\ell^{1/2}$ one of sets $S\cup\{\psi\}$ or $S\cup\{\neg\psi\}$ is $\ell^{1/2}$-consistent.

Also, for every disjunction $\bigvee_{i\leq r}\psi_i \in Fle$ of size at most $\ell^{1/3}$ one of sets $S \cup \{\bigwedge_{i\leq r}\neg\psi_i\}$ or $S \cup \{\bigvee_{i\leq r}\psi_i\} \cup \{\psi_j\}$, some $j \leq r$, is $\ell^{1/3}$-consistent.

First part is obvious. For the second part: assuming that all $r+2$ sets above are $\ell^{1/3}$-inconsistent would allow us to construct in an obvious way a proof of 0 from S of size at most $(r+2)\ell^{1/3} + O(|\bigvee_{i\leq r} \psi_i|^2) \leq \ell$: a contradiction. Note that the claim is valid also for system F.

Claim 7: *Let $S \subseteq Fle$ be a $\Delta_1^{1,b}$- definable family of formulas in M_0, and assume that S is ℓ-consistent in M_0, where $\ell \in (N_{M_0} \setminus N_{M^*})$.*

Let $H(\phi, x)$ be a $\Sigma_0^{1,b}$-formula with parameters from C^* and N_{M^*}. Let $v \in N_{M^*}$, and assume that $t(v)$ bounds the interval whose subsets are substitutable for ϕ in H for all $x < v$. Then one of the following sets is $\ell^{1/3}$-consistent:

(i) $S \cup \{\neg\langle H(\phi,0)\rangle_v(\tilde{\delta}) |\ \tilde{\delta} \in C^*,\ |\tilde{\delta}| \leq t(v)\}$,

(ii) $S \cup \{\langle H(\phi,v)\rangle_v(\tilde{\delta})\}$, *some* $\tilde{\delta} \in C^*$ *of length* $\leq t(v)$,

(iii) $S \cup \{\langle H(\phi,v')\rangle_v(\tilde{\delta})\} \cup \{\neg\langle H(\phi,v'+1)\rangle_v(\tilde{\rho}) | \tilde{\rho} \in C^*,\ |\tilde{\rho}| \leq t(v)\}$, *some* $\tilde{\delta} \in C^*$ *of length* $\leq t(v)$ *and* $v' < v$.

To prove the claim define formula $D(u)$ saying:

$$\forall w \leq u \exists \overline{r}_w \in C;\ |\overline{r}_w| \leq t(v) \wedge [\ S\ \ell^{1/3} - entails\ formula\ \langle H(\phi,w)\rangle(\overline{r}_w)\ ]\ .$$

Note that $D(u)$ is a $\Sigma_1^{1,b}$-formula and that witnesses $\overline{r}_w$ are actually from C^* due to the bound $t(v)$.

As M_0 is a model of V_1^1 one of two cases must occur:

(a) $D(u)$ holds for $u = v$,

(b) there exists minimal $u \leq v$ for which $D(u)$ fails.

In case (a) define $S' := S \cup \{\langle H(\phi,v)\rangle(\overline{r}_v)\}$, where $\overline{r}_v$ is a witness to validity of $D(v)$. Set S' is $\ell/2$-consistent as otherwise one could $\ell/2 + \ell^{1/3} \leq \ell$-entail 0 from S, which is a contradiction.

In case (b) let $u \leq v$ be the first u such that $D(u)$ fails. Take set

$$S' := S \cup \{\langle H(\phi,u-1)\rangle(\overline{r}_{u-1})\} \cup \{\neg\langle H(\phi,u)\rangle(\overline{q}) |\ \overline{q} \in C,\ |\overline{q}| \leq t(v)\}$$

for $u \geq 1$ (and again $\overline{r}_{u-1}$ the relevant witness) or

$$S' := S \cup \{\neg\langle H(\phi,0)\rangle(\overline{q}) |\ \overline{q} \in C,\ |\overline{q}| \leq t(v)\}$$

for $u = 0$.

We claim that S' is $\ell^{1/3}$-consistent. Assume otherwise and w.l.o.g. $u \geq 1$. Then $S + \langle H(\phi,u-1)\rangle(\overline{r}_{u-1})$ $O(\ell^{2/3})$-entails some disjunction of the form $\bigvee_{\overline{q}\in I}\langle H(\phi,u)\rangle(\overline{q})$, where $I \subseteq C^*$. But then $\langle H(\phi,u)\rangle(\overline{r})$ can be $O(\ell^{2/3})$-entailed from $S + \langle H(\phi,u-1)\rangle(\overline{r}_{u-1})$ too, where $\overline{r}$ is a new tuple defined by extension atoms using a case distinction considering which disjunct $\langle H(\phi, u)\rangle(\overline{q})$ in the disjuction is true (cf. Claim 6).

Note that automatically $|\overline{r}| \leq t(v)$ as $|\overline{q}| \leq t(v)$ holds for all $\overline{q} \in I$. This contradicts the assumption that $D(u)$ fails, hence S' is $\ell^{1/3}$-consistent.

Define now the family $\mathcal{P}$ be the family of all $H \subseteq Fle$ which are $\Delta_1^{1,b}$-definable in M_0 and which are ℓ-consistent for some $\ell \in (N_{M_0} \setminus N_{M^*})$; note that such ℓ exists by our assumption on M_0, and that set $\{\neg\tilde{\tau}\} \in \mathcal{P}$.

Family $\mathcal{P}$ is partially ordered by the inclusion relation $\subseteq$. Class $\mathcal{Q} \subseteq \mathcal{P}$ is *dense* if

$$\forall H \in \mathcal{P} \exists H' \in \mathcal{Q};\ H \subseteq H'.$$

Class $\mathcal{Q}$ is *definable* if there is a formula $\Psi(X)$ in the language of V_1^1 augmented by new metavariable X such that:

$$\mathcal{Q} = \{H \in \mathcal{P} |\ (M, H) \models \Psi(H)\}.$$

Finally, class $\mathcal{G} \subseteq \mathcal{P}$ is *generic* if it satisfies the following conditions:

(i) if $H \in \mathcal{G}$ and $H' \subseteq H$ then $H' \in \mathcal{G}$,

(ii) $\mathcal{G}$ intersects every dense, definable subclass of $\mathcal{P}$.

Claim 8: *Let $\mathcal{G} \subseteq \mathcal{P}$ be generic and assume that $\{\neg\tilde{\tau}\} \in \mathcal{G}$. Put*

$$G := \bigcup \mathcal{G}\ .$$

Then G satisfies conditions 1. - 5. above and hence $M^*[G]$ is a model of V_1^1 in which $\neg\tilde{\tau}$ is satisfiable.

As model M_0 is countable there is only countably many dense definable subclasses of $\mathcal{P}$, hence by standard argument a generic class $\mathcal{G}$ exists. By *Claims 5, 6, 7* the classes

1. of those $H \in \mathcal{P}$ which fulfill condition 2. for $\psi \in Fle^*$,i.e.:

$$\psi \in H \text{ or } \neg\psi \in H\ ,$$

2. of those $H \in \mathcal{P}$ which fulfill condition 4. for $\psi = \bigvee_{i \leq r} \psi_i \in Fle^*$, i.e.:

$$\bigwedge_{i \leq r} \neg\psi_i \in H \text{ or } \{\psi, \psi_j\} \subseteq H, \text{ some } j \leq r,$$

3. of those $H \in \mathcal{P}$ which fulfill condition 5. for $H(\phi, x)$ and $v \in N_{M^*}$, i.e.:

   $\{\neg\langle H(\phi,0)\rangle_v(\tilde{\delta})|\ \tilde{\delta} \in C,\ |\tilde{\delta}| \leq t(v)\} \subseteq H$, **or**
   $\{\langle H(\phi,v)\rangle_v(\tilde{\delta})\} \subseteq H$, some $\tilde{\delta} \in C$ of length $\leq t(v)$, **or**
   $\{\langle H(\phi,v')\rangle_v(\tilde{\delta})\} \cup \{\neg\langle H(\phi,v'+1)\rangle_v(\tilde{\rho})|\tilde{\rho} \in C,\ |\tilde{\rho}| \leq t(v)\} \subseteq H$, some $\tilde{\delta} \in C$ of size $\leq t(v)$ and $v' < v$

are all dense and clearly definable. Hence any G defined from a generic $\mathcal{G}$ satisfies conditions 1 - 5.

This concludes the description of a forcing construction of model

$$M' = M^*[G] .$$

In a natural way one can define a *forcing relation* between elements of $\mathcal{P}$ and formulas from Fle^*, namely:

$$H \text{ forces } \psi \text{ iff } H\ \ell - entails\ \psi, \text{ for some } \ell \in N_{M^*} .$$

This relation satisfies the usual properties of a forcing relation. In particular, one can shift to a *boolean valuation* of formulas by taking the boolean algebra $\mathcal{B}$ of regular open subsets of $\mathcal{P}$ (thinking of $\mathcal{P}$ as augmented with the order topology defined by $\subseteq$). We refer reader to [42] for general information on forcing and boolean-valued models.

Generic family $\mathcal{G}$ defines naturally an ultrafilter $\mathcal{F}$ on $\mathcal{B}$ by:

$$\mathcal{F} := \{b \in \mathcal{B}|\ b \cap \mathcal{G} \neq \emptyset\}.$$

In particular, an ultrafilter $\mathcal{F}$ defines a $0-1$-valuation of Fle^* by:

$$\psi \text{ gets value } 1 \textbf{ iff } \nu(\psi) \in \mathcal{F}.$$

Important thing to notice is that the boolean values are assigned only to formulas from Fle^* and not to all formulas from Fle. In fact, there is no apparent way how to extend consistently the valuation ν to Fle.

6 Finite Boolean Valuations

In this section we define the notion of *boolean valuations* of finite sets of formulas and we show in Theorem 6.5 that in principle it can be used to prove lower bounds to $s_{EF}(n)$ (equivalently to $k_F(n)$ or to $\ell_F(n)$).

Definition 6.1 *(a) A* partial boolean algebra $\mathcal{B}(0, 1, \wedge, \vee, \neg)$ *is a set* $\mathcal{B}$ *with at least two distinct elements* 0 *and* 1*, with partial binary operations* $\wedge, \vee$ *and with a partial unary operation* $\neg$ *satisfying the following conditions:*

whenever both sides of an identity below are defined then they are equal in $\mathcal{B}$*:*

(i) $\neg 0 = 1 \;\; \neg 1 = 0, \;\; 0 \vee a = a$ *and* $1 \wedge a = a$,

(ii) $a \vee \neg a = 1, \; a \wedge \neg a = 0$,

(iii) $a \vee b = b \vee a, \; a \wedge b = b \wedge a$,

(iv) $a \vee (b \vee c) = (a \vee b) \vee c, \; a \wedge (b \wedge c) = (a \wedge b) \wedge c$,

(v) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \; a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,

(b) A homomorphism $h : \mathcal{B}_1 \to \mathcal{B}_2$ *of a partial boolean algebra* $\mathcal{B}_1$ *into* $\mathcal{B}_2$ *is a map h of the universe of* $\mathcal{B}_1$ *into the universe of* $\mathcal{B}_2$ *such that* $h(0_{\mathcal{B}_1}) = 0_{\mathcal{B}_2}$, $h(1_{\mathcal{B}_1}) = 1_{\mathcal{B}_2}$*, and:*

(i) $\neg h(u)$ *is defined and equal to* $h(\neg u)$*, whenever* $\neg u$ *is defined in* $\mathcal{B}_1$,

(ii) $h(u) \circ h(v)$ *is defined and equal to* $h(u \circ v)$ *, whenever* $u \circ v$ *is defined in* $\mathcal{B}_1$ $(\circ = \wedge, \vee)$.

(c) A congruence relation *on a partial boolean algebra* $\mathcal{B}$ *is a partition* $\cong$ *of the universe of* $\mathcal{B}$ *such that:*

(i) $u \cong v$ *implies* $(\neg u) \cong (\neg v)$*, provided both* $\neg u, \neg v$ *are defined in* $\mathcal{B}$,

(ii) $u \cong v$ *and* $u' \cong v'$ *implies* $(u \circ u') \cong (v \circ v')$*, provided both* $u \circ u'$ *and* $v \circ v'$ *are defined in* $\mathcal{B}$ $(\circ = \wedge, \vee)$.

Simple examples of partial boolean algebras are obtained by restricting a (total) boolean algebra to a subset of its universe. However, the partial boolean algebras arising in Theorem 6.5 are *never* of this form.

Definition 6.2 *Let* Γ *be a set of formulas. A* boolean evaluation *of* Γ *is a map*

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

of formulas from Γ *into a partial boolean algebra* $\mathcal{B}(0, 1, \wedge, \vee, \neg)$ *satisfying the following conditions:*

(i) $\nu(0) = 0_{\mathcal{B}}$ *and* $\nu(1) = 1_{\mathcal{B}}$,

(ii) $\neg \nu(\psi)$ *is defined and* $\nu(\neg \psi) = \neg \nu(\psi)$*, whenever* $\psi, \; \neg \psi \in \Gamma$,

(iii) $\nu(\psi) \circ \nu(\phi)$ *is defined and* $\nu(\psi \circ \phi) = \nu(\psi) \circ \nu(\phi)$*, whenever* $\psi, \phi, \psi \circ \phi \in \Gamma$*, for* $\circ = \vee, \; \wedge, \; \to$.

For convenience we will always assume that Γ is closed under subformulas. We use the same symbols for logical connectives and operations in the algebra as there is no danger of confusion. Operation $\rightarrow$ in $\mathcal{B}$ is defined as usual: $(a \rightarrow b) := (\neg a) \vee b$ and may be only partial.

Let Γ be a set of formulas. We shall say that an F-proof of τ is *within* Γ, $\vdash_\Gamma$ in symbols, if every formula occurring as a subformula in the proof is from Γ.

Lemma 6.3 *Let Γ be a set of formulas closed under subformulas such that $\tau \in \Gamma$ and let π be an F-proof of τ within Γ.*

Then there is set $\Gamma^*_\pi \supseteq \Gamma$ of formulas such that whenever

$$\nu : \Gamma^*_\pi \rightarrow \mathcal{B}$$

is a boolean valuation of Γ^*_π then

$$\nu(\tau) = 1_{\mathcal{B}} \ .$$

Moreover:

$$|\Gamma^*_\pi| \leq c \cdot |\Gamma|$$

where c is a constant depending on F only.

Proof :

Define set Γ^*_π in two steps:

1. For every axiom scheme $\eta(A, B, C)$ of F let

   $$Z_\eta := \{t_1(A, B, C), \ldots, t_k(A, B, C)\}$$

   be all terms occurring as subterms in a fixed derivation of equality $\eta(A, B, C) = 1$ from identities defining boolean algebras (cf. Definition 6.1) in some equational derivation.

2. For Γ a set of formulas and π an F-proof within Γ let Γ^*_π be the smallest set of formulas containing Γ, closed under subformulas and satisfying the condition:

   whenever $\eta(\alpha, \beta, \gamma)$ is an axiom in π and $t(A, B, C) \in Z_\eta$ then formula:

   $$t(\alpha, \beta, \gamma)$$

   is in set Γ^*_π.

As ν behaves as a homomorphism on formulas from Γ^*_π, every F-axiom from π receives value $1_{\mathcal{B}}$ by ν (as its equational derivation is included in Γ^*_π). Value $1_{\mathcal{B}}$ is preserved by the modus ponens rule and hence $\nu(\tau) = 1_{\mathcal{B}}$.

q.e.d.

Next we prove a form of a converse to the preceeding lemma.

Lemma 6.4 *There is an assignment $\Gamma \mapsto \Gamma^+$ assigning to any finite set of formulas Γ set $\Gamma^+ \supseteq \Gamma$ having the following property:*

If Γ is a set of formulas closed under subformulas such that $\tau \in \Gamma$, and there is no F-proof of τ within Γ^+, then there is a boolean valuation

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

of Γ in which

$$\nu(\tau) \neq 1_{\mathcal{B}} \ .$$

Moreover:

$$|\Gamma^+| \leq |\Gamma|^c$$

where c is a constant depending on F only.

Proof :

We shall define set Γ^+ first and then verify its properties.

1. For t_1, t_2 terms in the language of boolean algebras we define formulas Π_{t_1,t_2} by the following process. First introduce new atoms A^i_s for every subterm s of t_i, $i = 1, 2$, and consider formulas:

   (a) for $s_1 \circ s_2$ a subterm of t_i and $\circ = \wedge, \vee$:

   $$A^i_{s_1 \circ s_2} \equiv A^i_{s_1} \circ A^i_{s_2}$$

   (b) for $\neg s$ a subterm of t_i:

   $$A^i_{\neg s} \equiv \neg A^i_s .$$

   Formula $Eq(t_1, t_2)$ is a formula of the form $C \to (A^1_{t_1} \equiv A^2_{t_2})$, where C is the conjuction of all formulas in (a) and (b). For $t_1 = t_2$ a valid identity of boolean algebras let π_{t_1,t_2} be a fixed F-proof of $Eq(t_1, t_2)$ and let Π_{t_1,t_2} be all subformulas occurring in it.

2. For Γ a set of formulas closed under subformulas let Γ^+ be the smallest set of formulas containing Γ, closed under subformulas and satisfying the conditions:

   (a) whenever (t_1, t_2) is one of the following pairs:

   $$(\neg a, \neg a), (a \wedge b, a \wedge b), (a \vee b, a \vee b)$$

or whenever $t_1 = t_2$ is an identity from Definition 6.1 then sets

$$\Pi_{t_1,t_2}(A^i_s/\phi^i_s),$$

are included in Γ^+, for all choices $\phi^i_s \in \Gamma$,

(b) for $\alpha, \beta, \gamma \in \Gamma$ formulas:

$$(\alpha \equiv \beta) \rightarrow (\beta \equiv \alpha) \ ,$$

$$(\alpha \equiv \beta) \rightarrow ((\beta \equiv \gamma) \rightarrow (\alpha \equiv \gamma)) \ ,$$

$$(0 \equiv 1) \rightarrow 0 \text{ and } (\alpha \equiv 1) \rightarrow \alpha$$

are included in Γ^+.

Define relation $\cong$ on Γ by:

$$\psi \cong \phi \ iff \ \vdash_{\Gamma^+} \psi \equiv \phi \ .$$

Relation $\cong$ is an equivalence relation on Γ because of condition (b) of part 2 of the definition of Γ^+, and it is in fact a congruence relation because of condition (a) of 2. By (b) of 2 it also follows that τ is not congruent to 1, as we assume that τ has no F-proof included in Γ^+.

Define a partial boolean algebra $\mathcal{B}$ as follows:

(i) elements of $\mathcal{B}$ are the congruence classes of $\Gamma/\cong$,

(ii) for $a, b \in \mathcal{B}$ and any $\alpha \in a$ and $\beta \in b$ such that $\alpha \wedge \beta \in \Gamma$ define $a \wedge b$ to be the congruence class of $\alpha \wedge \beta$, and analogously for other operations $\vee, \neg, 1, 0$.

That this is in fact a correct definition of operations and that these operations satisfy the requirements of Definition 6.1 follows from part (a) of 2 of the definition of Γ^+.

q.e.d.

We are ready now to formulate the theorem on *boolean valuations*.

Theorem 6.5 *Let τ be a tautology and let $\kappa(\tau)$ be the maximal number n such that for any set Γ closed under subformulas and satisfying:*

$$|\Gamma| \leq n \quad and \quad \tau \in \Gamma$$

($|\Gamma|$ is the cardinality of the set) there is a boolean valuation $\nu : \Gamma \rightarrow \mathcal{B}$ in which $\nu(\tau) \neq 1_{\mathcal{B}}$.

Then for every tautology τ it holds:

$$\kappa(\tau) = O(\ell_F^0(\tau)) \quad \textit{and} \quad \ell_F^0(\tau) = \kappa(\tau)^{O(1)} \ .$$

In particular,

$$s_{EF}^0(\tau) = \Omega(\kappa(\tau)) \ .$$

Proof :

Let π be an F-proof of τ with $\ell_F^0(\tau)$ distinct formulas and let Γ be the set of formulas occurring in π as subformulas. Then by Lemma 6.3 in any boolean valuation

$$\nu : \Gamma_\pi^* \to \mathcal{B}$$

it must hold that $\nu(\tau) = 1_{\mathcal{B}}$, but it also holds that

$$\kappa(\tau) \leq |\Gamma_\pi^*| = O(|\Gamma|) = O(\ell_F^0(\tau)) \ .$$

This proves the first inequality.

For the second inequality take some set Γ of size $\kappa(\tau) + 1$, closed under subformulas and containing τ, such that in any boolean valuation $\nu : \Gamma \to \mathcal{B}$ it holds that $\nu(\tau) = 1_{\mathcal{B}}$. By Lemma 6.4 τ must be F-provable within set Γ^+. Since

$$\ell_F^0(\tau) \leq |\Gamma^+| = |\Gamma|^{O(1)} = (\kappa(\tau))^{O(1)}$$

the second inequality follows.

By Theorem 1.2 and Lemma 1.4 it holds that

$$\ell_F^0(\tau) = O(s_{EF}^0(\tau)) \ ,$$

hence the last sentence of the theorem follows from the first inequality.

q.e.d.

For a lower bound $n \leq s_{EF}^0(\tau)$ we need to consider partial boolean algebras $\mathcal{B}$ of size $O(n)$. It would be interesting to know whether this is really necessary or whether one could have $\mathcal{B}$ of much smaller cardinality than $|\Gamma|$.

For an extension EF_A of the system EF by a set A of new axioms it is easy to modify the method so that a theorem analogous to the preceding one is valid. An A-*boolean valuation* of Γ is any boolean valuation $\nu : \Gamma \to \mathcal{B}$ in which every formula $\psi \in \Gamma$ which is a substitution instance of a formula from A receives value $\nu(\psi) = 1_{\mathcal{B}}$.

With this notion a theorem completely analogous to Theorem 6.5 is valid for system EF_A. By Theorem 4.2, every propositional system in the sense of [17] can be polynomially simulated by some system EF_A, where A is a suitable polynomial time set of tautologies, cf. [28]. Hence in this sense the upper bound from the theorem transfers to any propositional proof system.

Also, for that matter, some earlier lower bounds for subsystems of F can be formalized in this concept. The general method itself can be reformulated for the constant-depth systems, since the maximal depth of a formula in sets Γ^*_π and Γ^+ in Lemmas 6.3 and 6.4 is at most a constant more than the maximal depth of a formula in Γ. For example, the proofs from [31, 36] can be phrased in terms of an explicit construction of a suitable boolean valuation of any subexponential-size set of constant-depth formulas (built from atoms used in the pigeonhole formulas). This is presented in detail in [27].

7 Concluding Remarks

There is a relation between first and second order bounded arithmetic called the *RSUV isomorphism (see [41, 38]).* A basis for this relation is the fact that sets can be treated directly as second order objects or can be coded by first order objects (numbers). Hence sets and numbers correspond to numbers and the lengths of numbers respectively, second order bounded formulas to first order bounded formulas, and second order theories of bounded arithmetic to first order ones. This relation can be made quite formal [41] (see also [38, 25]) and, in particular, one can show that theories V_1^1 and U_1^1 correspond to theories S_2^1 and R_2^1 respectively, in the sense that second order bounded formula A is provable in V_1^1 resp. in U_1^1 iff the corresponding first order bounded formula A^* is provable in S_2^1 resp. R_2^1.

There is also another translation of first order bounded formulas into quantified propositional formulas: for $A(x)$ a first order bounded formula and m, $||A||^m$ is a formula with m free atoms $p_1, \ldots, p_m$ standing for unknown bits of x, $|x| < m$, in which a bounded quantifier bounding y translates as a block of similar boolean quantifiers bounding (polynomially many) bits of y. See [29] for details.

In this translation the theory S_2^1 corresponds to the proof system EF (see [16, 7, 28]), meaning that S_2^1 proves the soundness of EF while EF polynomially proves translations of $\forall\Pi_1^b$-consequences of S_2^1. This correspondence can be extended to all theories S_2^i and T_2^i and appropriate fragments of the quantified propositional calculus G, see [29]. For Frege proof system F, P. Clote [12, 13] constructed an equational theory ALV whose consequences have polynomial size F-proofs. See also [15] for a related first order theory.

From the relations between S_2^1 and EF one can obtain another proof of Theorem 3.1, although not straightforward as e.g. $\langle A \rangle_n$ and $||A^*||^{|n|}$ are not identical formulas. I know of no such derivation of the relations between U_1^1 and F. This would require a theory T satisfying the following three conditions:

1. proofs in T translate (via the translation $||A||^m$) into (quasi)polynomial-size F-proofs

2. T proves the soundness of F

3. T proves that every formula can be evaluated over any truth assignment.

For example, only condition 1 was established in [12] for $T = ALV$. Arai [3] defined a theory AID which satisfies all these conditions.

We shall conclude the paper by mentioning a communication complexity problem related to F-provability.

Let $\tau(p_1, \ldots, p_n)$ be a tautology with n atoms and assume $\pi = (\varphi_1, \ldots, \varphi_k)$ is its F-proof. Consider the following search problem. Two players I and II each receive an evaluation α resp. β of atoms $p_1, \ldots, p_n$: player I (resp. II) gets α (resp. β) but does not know β (resp. α). Their task is to either find out that $\alpha = \beta$ or to find a formula ψ occurring as a subformula in π (in one of its steps φ_i) which gets different truth values by α and β. Observe that if $\alpha \neq \beta$ such ψ exists as α, β give different values to some p_i and w.l.o.g. we may assume that all atoms $p_1, \ldots, p_n$ actually appear in τ.

Players exchange bits until they agree on an answer. The minimal number of bits they need to exchange, denoted $C(\pi, n)$, is the *communication complexity* of the search problem (see [33] for a survey of communication complexity).

Define function:

$$K(m) := \max\{CC(\pi, n) | \pi \text{ is an } F\text{-proof of } \tau_n \text{ and } |\pi| \leq m\}.$$

The function $K(m)$ satisfies inequalities $n + 1 \leq K(m) \leq n + \log(n)$. The first inequality follows as by [34] the trivial strategy (one player sends its evaluation to the other one which sends back the answer) is optimal for the problem to decide whether α equals to β, which information is trivially included in an answer to the search problem. The second inequality holds as player I can send α (n bits) to player II which sends back either information that $\alpha = \beta$ or the index i ($\log n$ bits) of an atom receiving different values by α, β.

The point is however, not to determine the value of $K(m)$ but to describe $K(m)$ as a function of m. The idea is that if τ expresses a complex combinatorial principle, its elementary proof (which an F-proof presumably is) must distinguish many cases, and if α, β belong to different cases there must be a place in the proof - a subformula - which distinguishes between α, β.

More precisely, assume that assignments from some subset A of all assignments are mapped onto the set of cases such that at most b assignments belong to the same case. If $a = |A|$, then $\log(m) \geq \log(\frac{a}{b})$. This is because player I needs $\log(m)$ bits to name a subformula associated to the case of α while again by [34] $\log(\frac{a}{b})$ is a lower bound to the communication complexity of the problem. For example, in [22, 11] the set A consists of all assignments determined by a partial $1-1$ map of size $\frac{n}{4}$ and the case of an assignment is the complex clause: a bound to m follows then from $\log(\frac{a}{b}) = \Omega(n)$).

This serves only as an illustration of an idea that a proof of a tautology might help players to find a non-trivial strategy for solving a communication complexity problem related to evaluations of the atoms. To find a type of such a communication complexity problem is actually also a part of the difficulty to make this idea work. Other problems than the one considered above might be more fruitful, e.g. a task akin to the task of determining whether $\alpha(p_i) = 1 = \beta(p_i)$, some p_i, since its communication complexity is robust also for random communication protocols. Another natural search problem associated with any tautology of the form $\tau_n = \bigvee_i \tau_i$ give to each player an evaluation on complementary halves of atoms and ask them to identify a true disjunct τ_i.

Acknowledgement

I am indebted to P.Pudlák for discussions about communication complexity problems related to propositional logic. I profited from lectures by M.Karchmer and A.A. Razborov given during the meeting *Feasible Mathematics II* at Cornell University in May 1992, and from subsequent conversations with them.

I reported on a part of this paper during that meeting and on topics of *Section 6* during the Annual ASL meeting in San Antonio in January 1993.

I thank S. Buss, P. Clote, S. Cook, P. Pudlák, A.A.Razborov and G. Takeuti for comments on the preliminary version of this paper, which was finished during my stay at the *Department of Computer Science* of the *University of Toronto* in Spring 1993.

References

[1] M. Ajtai: "Σ^1_1-formulae in finite structures", Annals of Pure and Applied Logic, 24, (1983), pp.1-48.

[2] —— "The complexity of the pigeonhole principle", in: Proc. IEEE 29$^{\text{th}}$ Annual Symp. on Foundation of Computer Science, (1988), pp. 346-355.

[3] T. Arai: "Frege system, $ALOGTIME$ and bounded arithmetic", unpublished manuscript, (1993).

[4] J.A. Bondy: "Induced subsets", J.Combinatorial Theory (B), 12,(1972), pp.201-202.

[5] M. L. Bonet: "Number of symbols in Frege proofs with and without the deduction rule", in: Arithmetic, Proof Theory and Computational Complexity, eds.P. Clote and J. Krajíček, Oxford Press, (1993), pp.61-95.

[6] M.L.Bonet, S.R.Buss and T.Pitassi: "Are there hard examples for Frege systems?", this volume.

[7] S.R.Buss : **Bounded Arithmetic**, Bibliopolis, Naples,(1986).

[8] —— : "The propositional pigeonhole principle has polynomial size Frege proofs", J. Symbolic Logic 52, (1987), pp. 916-927.

[9] —— : "Propositional consistency proofs", Annals of Pure and Applied Logic, 52, (1991), pp.3-29.

[10] S.R. Buss, J. Krajíček and G. Takeuti: "On provably total functions in bounded arithmetic theories R^i_3, U^i_2 and V^i_2",in: Arithmetic, Proof Theory and Computational Complexity, eds.P. Clote and J. Krajíček, Oxford Press, (1993), pp.116-161.

[11] S.R. Buss and G. Turán: "Resolution proofs of generalized pigeonhole principle", *Theoretical Computer Science*, 62, (1988), pp.311-317.

[12] P. Clote: "ALOGTIME and a conjecture of S.A. Cook", Annals of Mathematics and Artificial Inteligence, 6, (1992), pp.57-106.

[13] P. Clote: " On polynomial size Frege proofs of certain combinatorial principles", in: Arithmetic, Proof Theory and Computational Complexity, eds.P. Clote and J. Krajíček, Oxford Press, (1993), pp.162-184.

[14] P. Clote and J. Krajíček: "Open problems", in: Arithmetic, Proof Theory and Computational Complexity, eds.P. Clote and J. Krajíček, Oxford Press, (1993), pp.1-19.

[15] P. Clote and G. Takeuti: "Bounded arithmetic for NC, $ALogTIME$, L and NL", Annals of Pure and Applied Logic 56, (1992), pp.73-117.

[16] S.A. Cook: "Feasibly constructive proofs and the propositional calculus", in: Proc. 7^{th} Annual ACM Symp. on Theory of Computing, (1975), pp. 83-97.

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

[18] W. Cook, C. R. Coullard and G. Turan: "On the complexity of cutting plane proofs", Discrete Applied Mathematics, 18, (1987). pp.25-38.

[19] M. Dowd: "Model-theoretic aspects of $P \neq NP$", unpublished manuscript, (1985).

[20] M. Furst, J.B.Saxe and M. Sipser: "Parity, circuits and the polynomial-time hierarchy", Math. Systems Theory, 17, (1984), pp.13-27.

[21] A. Goerdt : "Cutting plane versus Frege proof systems", in: *Computer Science Logic*, eds. E. Börger et. al., LN in Computer Science **533**, Springer Verlag, pp.174-194, (1991).

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

[23] J. Krajíček: “On the number of steps in proofs”, Annals of Pure and Applied Logic 41, (1989), pp. 153-178.

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

[25] —— : “Exponentiation and second-order bounded arithmetic”, Annals of Pure and Applied Logic 48, (1990), pp. 261-276

[26] —— : “Lower bounds to the size of constant-depth propositional proofs”, Journal of Symbolic Logic, 59(1), (1994), pp. 73-86.

[27] —— : **Bounded arithmetic, propositional logic and complexity theory**, a book prepared for the *Cambridge University Press*, (1993), 401 p.

[28] J. Krajíček and P. Pudlák: “Propositional proof systems, the consistency of first order theories and the complexity of computations”, J. Symbolic Logic 54(3), (1989), pp. 1063-1079

[29] —— : “Quantified propositional calculi and fragments of bounded arithmetic”, Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik 36, (1990), pp. 29-46.

[30] —— : “Propositional provability in models of weak arithmetic”, in:Computer Science Logic, eds.E.Boerger, H.Kleine-Bunning and M.M. Richter, Springer-Verlag, (1990), pp.193-210.

[31] J. Krajíček and P. Pudlák and A. Woods : “Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle”, submitted.

[32] J. Krajíček and G. Takeuti : “On bounded $\sum_1^1$-polynomial induction”, in: Feasible Mathematics, eds. S.R. Buss and P.J. Scott, Birkhauser, (1990), pp. 259-280.

[33] L. Lovász: “Communication complexity: a survey”, in: Paths, Flows and VLSI Layout, eds. Korte, Lovász, Promer, Schrijver, Springer-Verlag, (1990), pp.325-266.

[34] K. Mehlhorn and F. M. Schmidt : “Las Vegas is better than determinism in VLSI and distributed computing”, 14th Annual ACM Symp. on Th. of Computing, (1982), pp.330-337.

[35] R. Parikh: “Some results on the length of proofs”, Transactions of the A.M.S., 177, (1973), pp. 29-36.

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

[37] J. Paris and A. Wilkie: "Counting problems in bounded arithmetic", in: Methods in Mathematical Logic, LNM 1130, Springer (1985), pp. 317-340.

[38] A.A. Razborov : "An Equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic", in: Arithmetic,Proof Theory and Computational Complexity, eds. P. Clote and J. Krajíček, Oxford Univ. Press, (1993), pp.247-277.

[39] R.A.Reckhow: "On the lengths of proofs in the propositional calculus",PhD.Thesis, Dept. of CS, University of Toronto, (1976).

[40] P.M. Spira: "On time-hardware complexity of tradeoffs for Boolean functions", in: Proc. 4^{th} Hawaii Symp. System Sciences, Western Periodicals Co., North Hollywood (1971), pp. 525-527.

[41] G. Takeuti: "RSUV Isomorphism", in: Arithmetic, Proof Theory and Computational Complexity, eds. P. Clote and J. Krajíček, Oxford Univ. Press, (1993), pp.364-386.

[42] G. Takeuti and W.M. Zaring : **Axiomatic Set Theory**, Springer-Verlag, (1973), 238p.

[43] G. C. Tseitin: "On the complexity of derivations in propositional calculus", in: Studies in mathematics and mathematical logic, Part II, ed. A.O.Slisenko, (1968), pp.115-125.

[44] G.C. Tseitin and A.A. Choubarian: "On some bounds to the lengths of logical proofs in classical propositional calculus" (Russian), Trudy Vyčisl Centra AN Arm SSR i Erevanskovo Univ. 8, (1975), 57-64.

Jan Krajıček
Mathematical Institut
Academy of Sciences
Žitna 25
Praha 1, 115 67
The Czech Republic