Proof complexity and arithmetic (lecture notes)

Jan Krajíček
Mathematical Institute
Academy of Sciences of the Czech Republic
Praha

These are rough notes for my course *Proof complexity and arithmetic* at the Charles University in Fall'03. They are formed to a large extent by parts of Chapters 9 and 14 in [5]. Some background material given in the course is in the notes [8] (relating to a course I had in Spring'03).

These two sets of lecture notes will eventually form a part of bigger lecture notes on *Proof complexity.* In particular, the bibliographical information given here is rather rudimentary and often refers just to [5]; full details will appear in the eventual lecture notes.

Contents

1 Background review

Here I list background notions and facts the reader is assumed to be familiar with; see [8] or [5].

Definition of Frege systems F, general definition of a propositional proof system (shortly "proof system", from now on) in the sense of Cook-Reckhow [4].

p-bounded proof systems. Their existence and the NP/coNP problem. The notions of *simulation* and *p-simulation*.

Reckhow's theorem: Any two Frege systems p-simulate each other. Proof of the theorem in the case the two systems have the same language (and for EF). Tree-like Frege systems F^*, their p-equivalence with F.

Extended Frege system EF, extension rule. Proportional relation between the minimal number of steps in F-proofs and in EF-proofs. Polynomial relation between the minimal number of steps and the size in EF-proofs.

Substitution Frege system SF, p-simulation of EF by SF (the opposite will be in here - Lemma 6.12). Circuit Frege CF from alla Jeřábek, and its p-equivalence with EF.

Quantified propositional calculus G and a p-simulation of SF by G.

2 Language L and bounded formulas

L is a two-sorted first order language. One sort $x, y, i, j, \ldots$ are numbers. There are constants 0, 1, and functions $+$ and $\cdot$ with their usual arithmetical meaning, and relation $<$. (Equality $=$ is always included for all sorts.)

The other sort ranges over bounded sets of numbers. The variables are written $\alpha^{t(x)}$, where $t(x)$ is a number-term in number-variables $x = (x_1, \ldots, x_n)$. The meaning of the term is that (as will be forced by axioms of the theories we will consider) $\alpha^t \subseteq [t] := \{0, \ldots, t-1\}$. We will often skip the superscript t, if there is no danger of a confusion.

Bounded formulas are those with all number-quantifiers bounded, i.e. of the form: $\exists y < t$ or $\forall y < t$. The class of all bounded formulas without the set-quantifiers is denoted $\Sigma_0^{1,b}$.

Define simulatenously two bigger classes of bounded formulas, $\Sigma_1^{1,b}$ and $\Pi_1^{1,b}$: These are the smallest classes of bounded formulas such that it holds:

- $\Sigma_0^{1,b} \subseteq \Sigma_1^{1,b} \cap \Pi_1^{1,b}$.
- Both $\Sigma_1^{1,b}$ and $\Pi_1^{1,b}$ are closed under $\vee$ and $\wedge$.
- Both $\Sigma_1^{1,b}$ and $\Pi_1^{1,b}$ are closed under bounded number-quantifiers.
- If $A \in \Sigma_1^{1,b}$ then $\neg A \in \Pi_1^{1,b}$, and vice versa.

Theorem 2.1 (Fagin) *A language $L \subseteq \{0,1\}^*$ is in the class NP iff it is $\Sigma_1^{1,b}$-definable, i.e. there is a $\Sigma_1^{1,b}$-formula $A(\alpha^x)$ such that*

$$w \in L \quad \textit{iff} \quad A(w^n)$$

where words w of length n are identified with subsets of $[n]$.

Any language definable by a $\Sigma_0^{1,b}$-formula is p-time decidable but the converse is not true. However, we have at least the following.

Corollary 2.2 *A p-time decidable language is $\Sigma_1^{1,b}$-definable and also $\Pi_1^{1,b}$-definable.*

In particular, properties of strings (i.e. bounded sets) like being a proof, a formula, a satisfying assignment etc. are also definable by both $\Sigma_1^{1,b}$ and $\Pi_1^{1,b}$ formulas.

3 Propositional translation of bounded formulas

Definition 3.1 *Let $\theta(x_1, \dots, x_k, \alpha_1^{t_1(x)}, \dots, \alpha_\ell^{t_\ell(x)})$ be a $\Sigma_0^{1,b}$-formula. Let $n = (n_1, \dots, n_k)$. Let p_j^i be propositional atoms, one for each $i \leq \ell$ and $j < t_i(n) - 1$.*

Define the propositional formula $\langle\theta\rangle_{(n_1,\dots,n_k)}$ by induction on the logical depth of θ:

1. *if θ is the atomic formula $s(\overline{x}) = t(\overline{x})$ then:*

$$\langle\theta\rangle_{(\overline{n})} := \begin{cases} 1 & \textit{if } s(\overline{n}) = t(\overline{n}) \textit{ is true} \\ 0 & \textit{if } s(\overline{n}) = t(\overline{n}) \textit{ is false} \end{cases}$$

2. *if θ is the atomic formula $s(\overline{x}) \leq t(\overline{x})$ then:*

$$\langle\theta\rangle_{(\overline{n})} := \begin{cases} 1 & \text{if } s(\overline{n}) \leq t(\overline{n}) \text{ is true} \\ 0 & \text{if } s(\overline{n}) \leq t(\overline{n}) \text{ is false} \end{cases}$$

3. $\langle\alpha^{s(x)} = \beta^{t(x)}\rangle_n := \bigwedge_{i\leq s(n)}(p_i \equiv q_i) \wedge \bigwedge_{s(n)<i\leq t(n)} \neg q_i$ *where $s(n) \leq t(n)$ and atoms p_i resp. q_i correspond to α and β resp.. The case $s(n) > t(n)$ is defined analogously.*

4. $$\langle s(x) \in \beta^{t(x)}\rangle_n := \begin{cases} q_u & \text{if } u = s(n) \leq t(n) \\ 0 & \text{otherwise} \end{cases}$$

5. *if $\theta = \neg\xi$ then:*
$$\langle\theta\rangle_{(\overline{n})} := \neg\langle\xi\rangle_{(\overline{n})}$$

6. *if $\theta = \nu \circ \xi$, $\circ = \vee, \wedge$ then:*
$$\langle\theta\rangle_{(\overline{n})} := \langle\nu\rangle_{(\overline{n})} \circ \langle\xi\rangle_{(\overline{n})}$$

7. *if $\theta = \exists y \leq s(\overline{x})\ \nu(\overline{x}, y)$ and $s(\overline{n}) = u$ then:*
$$\langle\theta\rangle_{(\overline{n})} := \bigvee_{m\leq u} \langle\nu\rangle_{(\overline{n},m)}$$

8. *if $\theta = \forall y \leq s(\overline{x})\ \nu(\overline{x}, y)$ and $s(\overline{n}) = u$ then:*
$$\langle\theta\rangle_{(\overline{n})} := \bigwedge_{m\leq u} \langle\nu\rangle_{(\overline{n},m)}$$

In the last two clauses the disjunction (resp. the conjunction) is formed from the binary connectives with the brackets associated, for example, to the left.

Next lemma is proved by induction on the complexity of θ.

Lemma 3.2 *Let $\theta(\overline{x})$ be a $\Sigma_0^{1,b}$-formula. Then there are d and ℓ such that for every $\overline{n}$:*

1. $dp(\langle\theta\rangle_{(\overline{n})}) \leq d$

2. $|\langle\theta\rangle_{(\overline{n})}| \leq max(\overline{n})^\ell$

The *depth* of θ is the maximal number of alternations of $\bigvee$ and $\bigwedge$ in the formula.

4 Theories V_1^1 and V_1^0

V_1^1 is a theory in the language L with the following axioms:

- A finite set of axioms codifying the basic arithmetical properties of the addition and the multiplication. E.g. finite theory PA^- (the theory of non-negative parts of ordered commutative rings) will work fine.
- Extensionality: $(\forall x < t + s; x \in \alpha^t \equiv x \in \beta^s) \to \alpha^t = \beta^s$.
- Boundedness of sets: $y \in \alpha^t \to y < t$.
- Comprehension axiom CA:

  $$\exists \alpha^t \forall y < t; A(y) \equiv y \in \alpha^t$$

  where A is any $\Sigma_0^{1,b}$-formula.
- Induction axioms IND:

  $$A(0) \vee (\exists y < x; A(y) \wedge \neg A(y + 1)) \vee A(x)$$

  where A is any $\Sigma_1^{1,b}$-formula.

Formulas A may have other free parameters, and all free variables are assumed to be universally quantified.

The theory V_1^0 is defined exactly like the theory V_1^1 except that the axiom scheme IND is accepted for all $\Sigma_0^{1,b}$-formulas only.

5 Propositional simulation of arithmetical proofs

Theorem 5.1 *Let $\theta(x)$ be a $\Sigma_0^{1,b}$-formula and assume:*

$$V_1^0 \vdash \forall x \theta(x).$$

Then there are d and ℓ such that every propositional formula $\langle \theta \rangle_{(n)}$ has a depth d F-proof of size at most n^ℓ.

Moreover, there is a polynomial time algorithm producing on input $1 \dots 1(n$ *- times) a depth d F-proof of $\langle \theta \rangle_{(n)}$.*

Proof

We shall describe the construction of a depth d size n^ℓ LK - proof of the sequent

$$\longrightarrow \langle\theta\rangle_{(n)} \ ,$$

and it will be obvious that the required algorithm exists. This is equivalent to the required task by the mutual p-simulation of Frege systems and sequent calculus LK that preserves the depth (cf.[8]).

By cut - elimination theorem (straightforwardly modified for V^0_1) there is an LKB - proof π using the $\Sigma^{1,b}_0$ - IND rule (see the end of the proof for the defintion of the rule) of the sequent:

$$\longrightarrow \theta(a) \ .$$

A sequent in the proof π has the form:

$$\phi_1(\overline{b}), \ldots \phi_r(\overline{b}) \longrightarrow \psi_1(\overline{b}), \ldots \psi_s(\overline{b})$$

where all ϕ_i, ψ_j are $\Sigma^{1,b}_0$. By induction on the number of inferences above the sequent in π prove that there is d and ℓ such that for any tuple $\overline{n}$ the sequent:

$$\langle\phi_1\rangle_{(\overline{n})}, \ldots, \langle\phi_r\rangle_{(\overline{n})} \longrightarrow \langle\psi_1\rangle_{(\overline{n})}, \ldots, \langle\psi_s\rangle_{(\overline{n})}$$

has a depth d size $max(\overline{n})^\ell$ LK - proof.

All initial sequents have the form $A \longrightarrow A$, A atomic, or $\longrightarrow A$, A an axiom of PA^-. In the former case the propositional translation is either $0 \longrightarrow 0, 1 \longrightarrow 1$ or $p^i_j \longrightarrow p^i_j$. In the latter case the translation is of the form $\longrightarrow \tau$, where τ is true boolean sentence (i.e. without atoms). Moreover, the depth of τ is constant (= the maximal logical depth of a PA^- - axiom). Any such sentence has a $dp(\tau)$ LK - proof of size $O(|\tau|)$.

The case when the sequent was obtained by structural or propositional rules or by the cut - rule is obvious : the same rules of propositional logic should be applied to the propositional translations of the upper sequents.

For the closed terms $t \leq s(\overline{n})$ is a formula of the form $\langle\eta(t)\rangle_{(\overline{n})}$ one of the disjuncts of $\langle\exists x \leq s, \eta(x)\rangle_{(\overline{n})}$; thus $\exists \leq$: *right* rule is simulated by repeated (polynomially many times) $\bigvee$: *right* rule of LK.

For the $\forall \leq$: *right* inference:

$$\frac{a \leq t, \Gamma \longrightarrow \Delta, A(a)}{\Gamma \longrightarrow \Delta, \forall x \leq t \ A(x)}$$

assume that for each $a = 0, 1, \ldots, val(t)$ there is an LK -proof of the translation of the upper sequent with the required properties. Then all

$a \leq t$ translate to 1, and thus can be cut out with the initial sequent $\longrightarrow 1$, and the obtained sequents are joined by repeated applications of the $\bigwedge : right$ rule for $a = 0, 1, \ldots, val(t)$. Hence the size of this translation is $val(t)^{O(1)} = max(\overline{n})^{O(1)}$. The left quantifier rules are treated analogously.

Finally, the IND rule:

$$\frac{A(a), \Gamma \longrightarrow \Delta, A(a+1)}{A(0), \Gamma \longrightarrow \Delta, A(t)}$$

is simulated by applying the cut rule to the LK -proofs of the translations of the upper sequent for $a = 0, 1, \ldots, val(t) - 1$.

Q.E.D.

We shall extend the simulation to the theory V_1^1.

A sequence of formulas $\theta_1, \ldots, \theta_k$ is called an EF **- sequence** iff it satisfies the conditions to be an EF - proof with the condition that no extension atom appears in θ_k *dropped*.

Theorem 5.2 *Let $A(x)$ be a $\Sigma_0^{1,b}$-formula and assume that:*

$$V_1^1 \vdash \forall x A(x).$$

Then the formulas $\langle A(x) \rangle_n$ have polynomial size EF-proofs.

Proof

We shall consider V_1^1 formalized in the sequent calculus with $\Sigma_1^{1,b} - IND$ rule in place of $\Sigma_1^{1,b} - IND$ axioms and with the introduction rules for the second order quantifiers replacing $\Sigma_0^{1,b} - CA$.

Assume that π is a V_1^1-proof of the sequent $\rightarrow A(a)$; w.l.o.g. we may assume that all formulas in π are $strict\Sigma_1^{1,b}$. These are $\Sigma_1^{1,b}$-formulas in which all second order quantifier precede all first order quantifiers and all connectives.

By induction on the number of steps in π above a sequent show that if:

$$\exists \psi_1 B_1(\overline{x}, \overline{\alpha}, \psi_1), \ldots, \exists \psi_u B_u(\overline{x}, \overline{\alpha}, \psi_u) \rightarrow \exists \xi_1 C_1(\overline{x}, \overline{\alpha}, \xi_1), \ldots, \exists \xi_v C_v(\overline{x}, \overline{\alpha}, \xi_v)$$

is a sequent in π then there is a constant k such that for all $\overline{m}$ there is an EF-sequence of size at most $(\max(\overline{m}))^k$ ending with the sequent:

$$\langle B_1 \rangle_{\overline{m}}(\overline{p}^{\alpha}, \overline{p}^{\psi_1}), \ldots, \langle B_u \rangle_{\overline{m}}(\overline{p}^{\alpha}, \overline{p}^{\psi_u}) \longrightarrow \langle C_1 \rangle_{\overline{m}}(\overline{p}^{\alpha}, \overline{p}^{\xi_1}), \ldots, \langle C_v \rangle_{\overline{m}}(\overline{p}^{\alpha}, \overline{p}^{\xi_v}) \ ,$$

and such that in this EF-sequence none of the atoms p^{α}_t or $p^{\psi_i}_t$ corresponding to a free second order variable α_i resp. to a second order variable ψ_j from an antecedent is an extension atom.

The construction follows the proof of the earlier theorem and we only need to treat two new rules : the introduction of the second order $\exists$ to the succedent and $\Sigma^{1,b}_1$-IND (the introduction of the second order $\exists$ to the antecedent does not change the translation).

Assume that in the former case the minor formula of the inference is

$$C(\overline{x}, \overline{\alpha}, \frac{t \in \xi}{E(\overline{x}, t, \overline{\alpha})})$$

with both $C, E \in \Sigma^{1,b}_0$, and that the principal formula is $\exists \xi C(\overline{x}, \overline{\alpha}, \xi)$. Introduce a new atom $p^{\xi}_t \equiv \langle E \rangle_{\overline{m},t}(\overline{p}^{\alpha})$. Then the equivalence :

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

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.

Now consider a $\Sigma^{1,b}_1$-IND inference:

$$\frac{\exists \xi_b C(b, \xi_b) \rightarrow \exists \xi_{b+1} C(b+1, \xi_{b+1})}{\exists \xi_0 C(0, \xi_0) \rightarrow \exists \xi_n C(n, \xi_n)}$$

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

$$\langle C \rangle_{\overline{m},u}(\overline{p}^{\xi_u}) \rightarrow \langle C \rangle_{\overline{m},u+1}(\overline{p}^{\xi_{u+1}})$$

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

$$\langle C \rangle_{\overline{m},0}(\overline{p}^{\xi_0}) \rightarrow \langle C \rangle_{\overline{m},n}(\overline{p}^{\xi_n}),$$

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

As the formula A is $\Sigma^{1,b}_0$, atoms in $\langle A \rangle_{(n)}$ correspond to free second order variables in A and hence cannot be the extension atoms. Thus the final EF -sequence is, in fact, an EF - proof.

Q.E.D.

6 Reflection principles and polynomial simulations

In this section we show that the provability of the reflection principles for propositional proof systems in bounded arithmetic implies polynomial simulation. As an illustration of this idea assume that we can verify in V_1^1 the soundness of a proof system P. Then the simulation of V_1^1 by EF allows to "prove" the soundness of P in EF, and then to use this proof to simulate P -proofs by EF - proofs. This idea is due to Cook (1975).

Recall that a sequence of sets can be coded by a set by:

$$j \in (\alpha)_i \equiv \langle j, i \rangle \in \alpha \ ,$$

and again such coding exists using CA applied to the definition of the sequence; this will always be $\Sigma_0^{1,b}$ or $\Delta_1^{1,b}$. Thus we can carry in V_1^0 some usual set - theoretic coding of propositional formulas, say as finite binary trees with inner nodes labelled by the connectives and leaves labelled by atoms or constants. Proofs are then particular sequences of formulas, and for systems F or EF the definitions of F- proofs resp. of EF - proofs are obviously also $\Sigma_0^{1,b}$. A truth evaluation of a formula will be coded a $0,1$-labelling of the nodes of the formula computed according to truth tables of the connectives. Moreover, these definitions allow to prove in V_1^0 the elementary syntactic properties like " a formula has unique immediate subformulas " etc. . We leave to the reader to design her/his own definitions and to carry with them the arguments below. We just stipulate a certain notation.

Definition 6.1 *1. $Fla(\alpha)$ is a $\Sigma_0^{1,b}$-definition of " α is a propositional formula "*

2. *For $P = F, EF$, $Prf_P(\pi, \alpha)$ is a $\Sigma_0^{1,b}$-definition of " π is a P - proof of α "*

3. *$Assign(\eta, \alpha)$ is a $\Sigma_0^{1,b}$-definition of " η is a truth assignment to the atoms of the formula α ", and $Assign(\eta, \alpha)$ implies in V_1^0 $Fla(\alpha)$*

4. *$Eval(\eta, \alpha, \gamma)$ is a $\Sigma_0^{1,b}$-definition of " γ is the evaluation of the formula α over the truth assignment η to its atoms " , and $Eval(\eta, \alpha, \gamma)$ implies in V_1^0 the conjunction $Fla(\alpha) \wedge Assign(\eta, \alpha)$*

5. *$\eta \models \alpha$ is a $\Delta_1^{1,b}$-definition in V_1^1 of " η is a satisfying truth assignment to the atoms of the formula α " , and it is in V_1^0-defined by:*

$$\exists \gamma, Eval(\eta, \alpha, \gamma) \wedge \text{"}\gamma \textit{ evaluates to } 1 \text{ "} \ .$$

6. $TAUT(\alpha)$ *is a* $\Pi_1^{1,b}$ *formula defined in* V_1^0 *as:*

$$\forall \eta, Assign(\eta, \alpha) \to \eta \models \alpha \ .$$

Formula $\eta \models \alpha$ is $\Delta_1^{1,b}$ in V_1^1 as even V_1^0 can prove the implication:

$$Eval(\eta, \alpha, \gamma_1) \wedge Eval(\eta, \alpha, \gamma_2) \to \gamma_1 = \gamma_2$$

(by induction on the size of γ_1, γ_2), and by the following lemma which is *not* obvious.

Lemma 6.2 *The theory* V_1^1 *proves that every propositional formula can be evaluated over any truth assignment to its atoms:*

$$\forall \eta, \alpha \exists \gamma, Assign(\eta, \alpha) \to Eval(\eta, \alpha, \gamma) \ .$$

Definition 6.3 *Let* P *be a proof system.* $Ref_P(x)$ *is (the universal closure of) the following* $\Sigma_0^{1,b}$*-formula:*

$$Prf_P(\pi^x, \alpha^x) \to \eta^x \models \alpha^x$$

Theorem 6.4 *The theory* V_1^1 *proves that* EF *is a sound proof system:*

$$\forall \alpha, \pi; Prf_{EF}(\pi, \alpha) \to TAUT(\alpha) \ .$$

Proof

Argue in V_1^1. Let π be an EF - proof of α with steps $(\pi)_1, \ldots, (\pi)_k = \alpha$, where $(\pi)_1, \ldots, (\pi)_m$ are the extension atoms used in π, $m < k$.

Let $Assign(\eta, \alpha)$ holds and w.l.o.g. assume that in π occur only the atoms from α or the extension atoms. Take the formula $A(u)$:

$$A(u) := \exists \xi \text{ "}\xi \text{ is a truth assignment to the extension atoms in } \pi\text{"} \wedge$$

$$\wedge \ \eta \cup \xi \models (\pi)_u \ .$$

This is a $\Sigma_1^{1,b}$ - formula clearly satisfying $A(1)$ and $A(u) \to A(u+1)$, giving to the extension atoms truth values computed from η by their definitions, for $u = 1, \ldots, m$. Hence $\Sigma_1^{1,b} - IND$ implies $A(k)$, and $\eta \models \alpha$ follows.

Q.E.D.

There is no $\Sigma_0^{1,b}$-definition of the relation $\eta \models \alpha$. This is because such definition would allow to express every boolean formula by a constant depth circuit $\langle \eta \models \alpha \rangle_n$ of size polynomial in $n = |\alpha|$, which is impossible (e.g. the parity function $\oplus(x_1, \ldots, x_n)$ has a formula of size n^2 but it has no polynomial size constant depth circuits. Thus we cannot translate the previous arguments into V_1^0. The theory V_1^0 does not even prove that every formula can be evaluated:

$$\forall \eta, \alpha; Assign(\eta, \alpha) \rightarrow \exists \gamma, Eval(\eta, \alpha, \gamma) \ .$$

There is, however, a $\Sigma_0^{1,b}$-definition of $\eta \models \alpha$ *assuming* that the depth of α is bounded by a *standard* constant.

Lemma 6.5 *Let d be a constant and let $Fla_d(\alpha)$ be a $\Sigma_0^{1,b}$ - definition of " α is a depth $\leq d$ formula " . Then:*

$$V_1^0 \vdash \forall \eta, \alpha; Fla_d(\alpha) \wedge Assign(\eta, \alpha) \rightarrow \exists \gamma, Eval(\eta, \alpha, \gamma) \ .$$

Proof

Prove the statement by induction on d showing that the evaluation γ is actually (for fixed d) $\Sigma_0^{1,b}$ - definable from η and α (the implication then follows by $\Sigma_0^{1,b} - CA$). This is because V_1^0 can prove that a depth d formula with the outmost connective $\wedge$ is a conjunction of (arbitrarily bracketed) depth $d-1$ formulas, i.e. it is true iff "all these subformulas of depth $d-1$ are true ". Assuming that a truth definition for $d-1$ formulas is already formed, this allows to define the truth for depth d formulas with a help of a $\forall \leq$ quantifier. Similarly when the outmost connective is $\vee$. If it is $\neg$ then first apply de Morgan rules to rewrite α such that all negations apply only to the atomic subformulas.

Q.E.D.

Theorem 6.6 *Let $d > 0$ be a constant. Then the theory V_1^0 proves that any Frege proof of depth $\leq d$ is sound:*

$$\forall \pi, \alpha; Prf_F(\pi, \alpha) \wedge \text{"}dp(\pi) \leq d\text{"} \rightarrow TAUT(\alpha) \ .$$

Proof

The proof goes by induction on the number of steps in π as before, using the $\Sigma_0^{1,b}$ - definition of the satisfaction relation for depth $\leq d$ formulas provided by the previous lemma.

Q.E.D.

Now we will formulate in model theoretic terms a sufficient condition for a demonstration of superpolynomial lower bounds.

Lemma 6.7 *Assume that A is a $\Sigma_0^{1,b}$ - formula. Then V_1^0 proves the equivalence:*

$$A(\alpha^x) \equiv (\tilde{\alpha} \models \langle A \rangle_x(\overline{p}))$$

where is a truth assignment, $\tilde{\alpha}$ is a $\Sigma_0^{1,b}$ -definable in V_1^0, assigning to p_i the value 1 iff $i \in \alpha^x$.

Proof

This is readily established by induction on the logical complexity of A.

Q.E.D.

Define $n^\omega := \bigcup_{k<\omega} n^k$ for n an element of a non-standard model of arithmetic.

Theorem 6.8 *Let $A(a, \alpha)$ be a $\Sigma_0^{1,b}$-formula with a and α the only free variables. Let M be a non-standard model of the true arithmetic $Th(\omega)$ and let $n \in M \setminus \omega$ be its non-standard element.*

Assume that for every bounded set $\pi \subseteq n^\omega$ coded in M there is a family $\mathcal{X} \subseteq exp(n^\omega)$ of bounded subsets of n^ω and $\alpha \in \mathcal{X}$ such that:

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

(ii) $(n^\omega, \mathcal{X}) \models V_1^0$

(iii) $(n^\omega, \mathcal{X}) \models \neg A(n, \alpha)$.

Then the formulas $\langle A(a) \rangle_m$, $m < \omega$, do not have polynomial size constant - depth F-proofs.

If $(n^\omega, \mathcal{X}) \models V_1^1$ then the formulas $\langle A(a) \rangle_m$ do not have polynomial size EF - proofs.

Proof

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

Take $\mathcal{X}$ and $\alpha \in \mathcal{X}$ satisfying the conditions (i)-(iii). Then $(n^\omega, \mathcal{X})$ is a model of V_1^0 in which the propositional formula $\langle A(a)\rangle_n$ has a depth d F - proof, some $d \in \omega$. By the soundness of depth d F in V_1^0 the formula $\langle A(a)\rangle_n$ must be a tautology. However, $\neg A(n, \alpha)$ is true, hence the assignment $\tilde{\alpha}$ defined in Lemma 6.7 does not satisfy $\langle A(a)\rangle_n$, by that lemma. This is a contradiction.

The case of V_1^1 follows analogously, using the provability of Ref_{EF} in V_1^1.

Q.E.D.

The following lemma is a formalized version of $\Sigma_1^{1,b}$-completeness.

Lemma 6.9 *Assume that* $A(\alpha^x) \in \Sigma_0^{1,b}$. *Then:*

$$V_1^1 \vdash A(\alpha^x) \to (\ EF \vdash \langle A\rangle_x(\overline{p}/\tilde{a})\ )\ .$$

where $\tilde{\alpha}$ *is as in Lemma 6.7.*

Lemma 6.10 *Let* $A(\alpha^x)$ *be a* $\Sigma_0^{1,b}$*-formula. Let* P *be a proof system. Then* V_1^1 *proves the implication:*

$$(\ Ref_P \wedge (P \vdash \langle A\rangle_x) \to \forall \alpha^x, A(\alpha^x)\ )\ .$$

Proof

The lemma follows from (essentially) Lemma 6.7.

Q.E.D.

Corollary 6.11 *Let* P *be a propositional proof system. Assume:*

$$V_1^1 \vdash Ref_P\ .$$

Then EF *p-simulates* P *and, in fact:*

$$V_1^1 \vdash EF \geq_p P\ .$$

The following corollary states a p-simulation result that is hard to prove directly.

Corollary 6.12 *EF p-simulates SF.*

Proof

By the previous corollary it is enough to prove Ref_{SF} in V_1^1, which is straightforward : by induction on the number of steps in an SF-proof show that every formula in the proof is a tautology. This needs IND for $\Pi_1^{1,b}$-formulas which is, however, available in V_1^1.

Q.E.D.

7 Model-theoretic constructions

In this section we give model - theoretic proofs for Theorems 5.1 and 5.2. I believe that this side of the simulation results is important for understanding of the interplay between arithmetic and propositional logic, and the fundamental problem of lower bounds for proof systems.

Theorem 7.1 *Let M be a countable model of the true arithmetic $Th(\omega)$ and let $n, t \in M \setminus \omega$ be its two non-standard elements. Let $\theta(a)$ be a $\Sigma_0^{1,b}$-formula with a the only free number-variable and R^a the only set-variable.*

Assume that in M there is no Frege proof of $\langle\theta\rangle_{(n)}$ of depth $\leq t$ and size $\leq n^t$ (i.e. no element $\leq 2^{n^t}$ codes such a proof).

Then it is possible to define $R \subseteq M \times M$ such that:

$$(n^\omega, R^n) \models V_1^0$$

and

$$(n^\omega, R^n) \models \neg\theta(n) \ .$$

Before we give the proof we should understand that this theorem implies Theorem 5.1. Assume that the formulas $\langle\theta\rangle_{(m)}$, $m < \omega$, do not have polynomial size constant depth Frege proofs. This means that for any $k < \omega$ and any $d < \omega$ there are $m < \omega$ such that $\langle\theta\rangle_{(m)}$ does not have a depth d size $\leq m^k$ F-proof. By the compactness there is a model of $Th(\omega)$ and non-standard $d, k \in M$ such that for some $m \in M$, M thinks that there is no depth d F-proof of $\langle\theta\rangle_{(m)}$ of size $\leq m^k$. Take $t := min(d, k)$. By this theorem then there is a model of V_1^0 in which $\forall x\theta(x)$ fails, i.e. $\forall x\theta(x)$ is not provable in V_1^0.

Proof

Let M, θ, n and t satisfy the hypothesis of the theorem. Assume that the only set-variable in θ is R^a (we will skip the superscript). We will add an interpretation of R to n^ω, and we will consider all other sets in the eventual model of V_1^0 as being the sets $\Sigma_0^{1,b}$-definable from R. Denote by $\Delta_0(R)$ the subclass of $\Sigma_0^{1,b}$-formulas where the only set-variable is R.

Let Fle denotes the set of propositional formulas coded in M, having a *standard* depth, build from the atoms p_i (corresponding to R), and of size $\leq n^\omega$. We shall form a set $T \subseteq Fle$ satisfying :

1. $\neg\langle\theta\rangle_{(n)} \in T$

2. for any $\psi \in Fle$: $\psi \in T$ or $\neg\psi \in T$, but not both

3. if $\psi \in Fle$ has the form $\bigwedge_i \phi_i$ then: $\psi \in T$ iff $\phi_i \in T$ all i

4. if $\psi \in Fle$ has the form $\bigvee_i \phi_i$ then: $\psi \in T$ iff $\phi_i \in T$ some i

5. for all $\eta(x) \in \Delta_0(R)$ with parameters from n^ω and x the only free variable, either $\neg\langle\eta\rangle_{(0)} \in T$ or $\langle\eta\rangle_{(u)} \in T$ for all $u \in n^\omega$ or $\langle\eta\rangle_{(u)} \wedge \neg\langle\eta\rangle_{(u+1)} \in T$ for some $u \in n^\omega$

having such set T define a set $R \subseteq [n]$ by:

$$i \in R \ \text{ iff } \ p_i \in T \ .$$

Claim 1 *For any $\Delta_0(R)$-sentence ξ with parameters from n^ω :*

$$(n^\omega, R) \models \xi \quad \textit{iff} \quad \langle\xi\rangle \in T \ .$$

The claim follows by conditions 2.-4. posed on T.

Claim 2 $(n^\omega, R) \models V^0_1 + \neg\theta(n)$.

This follows from conditions 1. and 5.

It remains to construct the set T having the required properties. This can be done by a completeness type argument but we shall cast it as a forcing type argument.

Let $\mathcal{P}$ denotes the class of subsets $S \subseteq Fle$ satisfying the conditions:

(i) $\neg\langle\theta\rangle_{(n)} \in S$

(ii) for any $k < \omega$ there is no depth k size $\leq n^k$ F - proof of contradiction $(= 0)$ from formulas in S

(iii) S is definable (and hence coded) in M.

Note that for $S \in \mathcal{P}$ there is $s > \omega$ such that there is no F -proof of 0 from S of depth $\leq s$ and size $\leq n^s$; this follows by induction as it is true for all standard s.

The next claim is obvious.

Claim 3 *Let $S \in \mathcal{P}$ and $\psi \in Fle$.*
Then either $S \cup \{\psi\} \in \mathcal{P}$ or $S \cup \{\neg\psi\} \in \mathcal{P}$.

Claim 4 *Let $S \in \mathcal{P}$ and $\psi \in S$, and assume that ψ has the form $\psi := \bigvee_{j \leq r} \phi_j$. Then for some $j_0 \leq r$, $S \cup \{\phi_{j_0}\} \in \mathcal{P}$.*

Assume otherwise, i.e. for every $j \leq r$ there is a depth k_j size $\leq n^{k_j}$ F-proof of 0 from $S \cup \{\phi_j\}$, and hence depth ℓ_j size $\leq n^{\ell_j}$ F-proof π_j of $\neg\phi_j$ from S, $k_j, \ell_j < \omega$. As $\psi \in Fle$, $r \leq |\psi| \leq n^\ell$, some $\ell \in \omega$.

Take $s > \omega$ such that there is no depth s size $\leq n^s$ F - proof of 0 from S. Each proof π_j has depth $<<$ s and size $<<$ $\frac{n^s}{n^\ell}$, so joining these $\leq n^\ell$ proofs gets a depth $< s$ size $< n^s$ proof of 0 from S, a contradiction.

Claim 5 *Let $S \in \mathcal{P}$ and $\psi \in S$, and let ψ has the form $\bigwedge_i \phi_i$.*
Then $S \cup \{\phi_i \mid \text{all } i\} \in \mathcal{P}$.

This is seen analogously as Claim 4.

Claim 6 *Let $S \in \mathcal{P}$ and let $\eta(x)$ be a $\Delta_0(R)$ formula with the parameters from n^ω and with x the only free variable.*

Then one of the following sets is in $\mathcal{P}$ too:

(a) $S \cup \{\neg\langle\eta\rangle_{(0)}\}$

(b) $S \cup \{\langle\eta\rangle_{(u)} \mid u \in n^\omega\}$

(c) $S \cup \{\langle\eta\rangle_{(u)}\} \cup \{\neg\langle\eta\rangle_{(u+1)}\}$ *some* $u \in n^\omega$.

To prove Claim 6 assume otherwise, so there is a depth k_0 size $\leq n^{k_0}$ proof π_{-1} of $\langle\eta\rangle_{(0)}$ from S, a depth k_u size $\leq n^{k_u}$ proof π_u of

$$\langle\eta\rangle_{(u)} \rightarrow \langle\eta\rangle_{(u+1)}$$

from S for all $u \in n^\omega$, and there is a depth k size $\leq n^k$ proof from S of the disjunction

$$\bigvee_{u \in X} \neg\langle\eta\rangle_{(u)} ,$$

for some $X \subseteq n^\omega$ of size $\leq n^k$.

For any non-standard s, joining proofs $\pi_{-1}, \pi_0, \ldots, \pi_v$ for $v = max(X)$ by cuts entails all $\langle\eta\rangle_{(u)}$, $u \in X$ by a depth s size $\leq n^s$ proofs, obtaining thus a depth s size $\leq n^s$ proof of 0 from S, contradicting $S \in \mathcal{P}$.

Now we are ready to construct the set T. Let $\psi_1, \psi_2, \ldots$ enumerate the set Fle and $\eta_1(x), \eta_2(x), \ldots$ enumerate all $\Delta_0(R)$ formulas with parameters from n^ω and with one free variable x.

Construct a sequence $S_0, S_1, \ldots \in \mathcal{P}$ such that:

(i) $S_0 := \{\neg\langle\theta\rangle_{(n)}\}$

(ii) $S_i \subseteq S_{i+1}$

(iii) $\psi_i \in S_i$ or $\neg\psi_i \in S_i$

(iv) if $\psi_i \in S_i$ and $\psi_i = \bigvee_{j \leq r} \phi_j$ then $\phi_{j_0} \in S_i$, some $j_0 \leq r$

(v) if $\psi_i \in S_i$ and $\psi_i = \bigwedge_{j \leq r} \phi_j$ then all $\phi_j \in S_i$

(vi) either $\neg\langle\eta_i\rangle_{(0)} \in S_i$ or $\langle\eta_i\rangle_{(u)} \wedge \neg\langle\eta_i\rangle_{(u+1)} \in S_i$ for some $u < n^\omega$, or $\langle\eta_i\rangle_{(u)} \in S_i$ all $u \in n^\omega$.

Having S_i satisfying the conditions, S_{i+1} exists by Claims 3.- 6.. Put

$$T := \bigcup_i S_i \ .$$

The set T fulfils the requirements 1. - 5. above.

Q.E.D.

The reason for the particular forcing type formulation of the argument is its similarity with the following, more involved, construction which is conveniently expressed using forcing.

Theorem 7.2 *Let $(M, \mathcal{X})$ be a model of V_1^1 and let $\tilde{\tau}(p_1, \ldots, p_n) \in \mathcal{X}$ be a propositional formula in $(M, \mathcal{X})$.*

Then the following two conditions are equivalent:

1. *In $(M, \mathcal{X})$ there is no EF-proof of $\tilde{\tau}$.*
2. *There is a $\Sigma_0^{1,b}$-elementary extension $(M', \mathcal{X}')$ of $(M, \mathcal{X})$ in which $\neg\tilde{\tau}$ is satisfiable.*

Proof

Assume that 1. fails, and let $\pi \in \mathcal{X}$ be an EF-proof of $\tilde{\tau}$ in $(M, \mathcal{X})$. As $(M', \mathcal{X}')$ is a $\Sigma_0^{1,b}$-elementary extension, π is an EF-proof of $\tilde{\tau}$ in $(M', \mathcal{X}')$ as well. But Ref_{EF} is provable in V_1^1, so $\tilde{\tau}$ must be tautologically true in $(M', \mathcal{X}')$, hence 2. fails.

Assume now that 1. holds and assume also that $(M, \mathcal{X})$ is countable. Construct $(M', \mathcal{X}')$ as follows.

By the compactness there is a countable elementary extension $(M_0, \mathcal{X}_0)$ of $(M, \mathcal{X})$ satisfying V_1^1 such that:

(i) there is $t \in M_0$ such that for all $v \in M$, $v < t$

(ii) in $(M_0, \mathcal{X}_0)$ there is no EF-proof of $\tilde{\tau}$.

Let $(M^*, \mathcal{X}^*)$ be a substructure of $(M_0, \mathcal{X}_0)$ defined by:

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

(ii) $\mathcal{X}^* = \{\tilde{\beta} \in X_0 \mid \tilde{\beta} \subseteq M^*\}$.

We define in $(M_0, \mathcal{X}_0)$ several families. Let $\{\overline{p}\}$ be the atoms of $\tilde{\tau}$ and let $Fle(\overline{p}) \subseteq X_0$ be the formulas with the atoms among $\{\overline{p}\}$. Further let A be the smallest set of the atoms containing $\{\overline{p}\}$ plus new atoms of the form q_ψ, one for each ψ built from atoms in A, and let $Fle \subseteq X_0$ be the set of the formulas with atoms among A.

Let $C \subseteq X_0$ be the family of tuples of elements of $A \cup \{0, 1\}$. Let

$$C^* := \{\beta \in C \mid |\beta| \in M^*\}$$

where $|(q_{\psi_1}, \ldots, q_{\psi_m})| = m$, and let

$$Fle^* := \{\phi \in Fle \mid |\phi| \in M^*\} \ .$$

The size means here the number of occurence of atoms. We will consider $\tilde{\beta} \in \mathcal{X}_0$ simultaneously also as an element of C: the tuple of bits of the characteristic function of $\tilde{\beta}$ (so for such $\tilde{\beta}$: $\tilde{\beta} \in C^* \equiv \beta \in \mathcal{X}^*$).

The following claim is established by induction on the logical complexity of B.

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

$$(M^*, X^*) \models B(\tilde{\beta}) \rightarrow \exists \pi Prf_F(\pi, \langle B \rangle(\overline{q}/\tilde{\beta})) \ ,$$

where $\overline{q}$ are atoms corresponding to β.

This is analogous to Lemma 6.7.

We will construct a 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 $\pi \in \mathcal{X}_0$ is an EF-proof of ψ from the assumptions $\psi_1, \ldots, \psi_r$, $|\pi| \in M^*$ and all $\psi_i \in G$, then also $\psi \in G$,

(4) if $\psi \in G$, $\psi \in Fle^*$ 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 $H(\phi, x)$ with the parameters from C^* and any $v \in M^*$ one of the following three conditions hold:

   (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

$$\langle H(\phi, v')\rangle_v(\tilde{\delta}) \in G \text{ and } \neg\langle H(\phi, v'+1)\rangle_v(\tilde{\epsilon}) \in G$$

   for some $\tilde{\delta} \in C^*$ of length $\leq t(v)$ and for all $\tilde{\epsilon} \in C^*$ of length $\leq t(v)$.

The term $t(v)$ bounds implicitly the size of the interval whose subsets can be substituted for ϕ in H for $x \leq v$.

Assume for a moment that we have such set G. Define a structure $(M^*[G], \mathcal{X}^*[G])$ by:

$$M^*[G] := M^* \text{ and } \mathcal{X}^*[G] := C^*/\sim\ ,$$

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 $(M^*[G], \mathcal{X}^*[G])$ is an extension of $(M^*, \mathcal{X}^*)$ and hence of $(M, \mathcal{X})$ 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 sufficiently large u:*

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

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

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

Claim 3 *Structure $(M^*[G], \mathcal{X}^*[G])$ is a model of V_1^1.*

Condition (5) posed on G guarantees that the induction for every $\Sigma_1^{1,b}$-formula $\exists\phi H(\phi, x)$ holds up to every $v \in M^*[G]$. The other axioms hold in $(M^*[G], \mathcal{X}^*[G])$ obviously. In particular, the $\Sigma_0^{1,b} - CA$ is guaranteed by *Claim 2.*

Claim 4 *There is $\tilde{\alpha} \in \mathcal{X}^*[G]$ such that*

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

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

$$\tilde{\alpha} := \overline{p}^{\alpha} / \sim \ .$$

It remains to construct the set G satisfying the above five requirements. We shall use two simple technical properties of system EF.

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

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

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

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

A set of formulas $S \subseteq Fle$ is said to *ℓ-entail* formula ψ iff there is an F-proof of size at most ℓ of ψ with the axioms from $S \cup T$ (the *size* means here the number of occurences of atoms). A 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 in $(M_0, \mathcal{X}_0)$, and assume that ψ has an EF-proof from S of size ℓ in $(M_0, \mathcal{X}_0)$.*

Then S also $O(\ell)^2$-entails ψ in $(M_0, \mathcal{X}_0)$.

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

Claim 6 *Let $S \subseteq Fle$ be a $\Delta_1^{1,b}$- definable in $(M_0, \mathcal{X}_0)$ and assume that S is ℓ-consistent in $(M_0, \mathcal{X}_0)$, where ℓ is non-standard.*

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

Also, for every disjunction $\bigvee_{i \leq r} \psi_i \in Fle$ of size at most $\ell^{3^{-1}}$ 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 $\ell^{3^{-1}}$-consistent.

The first part is obvious. For the second part; assuming that all $r + 2$ sets above are $\ell^{3^{-1}}$-inconsistent would allow us to construct in an obvious way a proof of 0 from S of size at most

$$(r + 2)\ell^{3-1} + O(|\bigvee_{i \leq r} \psi_i|^2) \leq \ell \ .$$

This is a contradiction.

Claim 7 *Let $S \subseteq Fle$ be a $\Delta_1^{1,b}$- definable family of formulas in $(M_0, \mathcal{X}_0)$, and assume that S is ℓ-consistent in $(M_0, \mathcal{X}_0)$, where ℓ is non-standard.*

Let $H(\phi, x)$ be a $\Sigma_0^{1,b}$-formula with parameters from C^* and M^*. Let $v \in M^*$, and assume that a term $t(v)$ bounds the size of the interval whose subsets can be substituted for ϕ in H for all $x < v$.

Then one of the following sets is $\ell^{3^{-1}}$-consistent:

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

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

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

To prove *Claim 7* take a formula $D(u)$:

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

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

As $(M_0, \mathcal{X}_0) \models V_1^1$ one of the two cases must occur:

(a) $D(v)$ holds in $(M_0, \mathcal{X}_0)$

(b) there exists minimal $u \leq v$ for which $D(u)$ fails in $(M_0, \mathcal{X}_0)$.

In case (a) define

$$S' := S \cup \{\langle H(\phi, v)\rangle(\overline{r}_v)\}\ ,$$

where $\overline{r}_v$ is a witness to the existential quantifier of $D(v)$. The set S' is $\ell/2$-consistent as otherwise one could $\ell/2 + \ell^{3^{-1}} \leq \ell$-entail 0 from S, which would be a contradiction.

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

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

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

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

for $u = 0$.

We claim that S' is $\ell^{3^{-1}}$-consistent. Assume otherwise and w.l.o.g. let $u \geq 1$. The set $S + \langle H(\phi, u-1)\rangle(\overline{r}_{u-1})$ then $O(\ell^{2/3})$-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 also $O(\ell^{2/3})$-entailed from $S + \langle H(\phi, u-1)\rangle(\overline{r}_{u-1})$, where $\overline{r}$ is a new tuple defined by extension atoms using a case distinction considering which disjunct in the disjunction is true (cf. Claim 5). Note that $|\overline{r}| \leq t(v)$. This contradicts the assumption that $D(u)$ fails, hence S' is $\ell^{3^{-1}}$-consistent.

Define now the family $\mathcal{P}$ of all $H \subseteq \mathit{Fle}$ which are $\Delta_1^{1,b}$-definable in $(M_0, \mathcal{X}_0)$ and which are ℓ-consistent for some $\ell \in (M_0 \setminus M^*)$; such ℓ exists by our assumption about $(M_0, \mathcal{X}_0)$. Note that $\{\neg\tilde{\tau}\} \in \mathcal{P}$.

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:

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

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 a generic class and assume that $\{\neg\tilde{\tau}\} \in \mathcal{G}$. Put*

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

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

As model $(M_0, \mathcal{X}_0)$ is countable there are only countably many dense definable subclasses of $\mathcal{P}$, hence by the standard argument a generic class $\mathcal{G}$ exists. By *Claims 5,6,7* the classes of those $K \in \mathcal{P}$ which fullfil condition (2) for $\psi \in \mathit{Fle}^*$, i.e.:

$$\psi \in K \ \mathit{or}\ \neg\psi \in K,$$

are clearly definable and dense, as well as are the classes of $K \in \mathcal{P}$ which fullfil condition (4) for $\psi = \bigvee_{i \leq r} \psi_i \in Fle^*$, i.e.:

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

and the classes of $K \in \mathcal{P}$ which fullfil condition (5) for $K(\phi, x)$ and $v \in M^*$, i.e.:

$\{\neg\langle K(\phi, 0)\rangle_v(\tilde{\delta}) \mid \tilde{\delta} \in C,\ |\tilde{\delta}| \leq t(v)\} \subseteq K$, or:

$\{\langle K(\phi, v)\rangle_v(\tilde{\delta})\} \subseteq K$, some $\tilde{\delta} \in C$ of length $\leq t(v)$, or:

$\{\langle K(\phi, v')_v(\tilde{\delta})\} \cup \{\neg\langle K(\phi, v'+1)_v(\tilde{\rho}) \mid \tilde{\rho} \in C,\ |\tilde{\rho}| \leq t(v)\} \subseteq K$, some $\tilde{\delta} \in C$ of length $\leq t(v)$ and $v' < v$.

Hence any G defined from a generic $\mathcal{G}$ satisfies conditions (1) - (5).

This concludes the description of the forcing construction of the model

$$(M', \mathcal{X}') = (M^*[G], X^*[G]) \ .$$

Q.E.D.

We leave it as an exercise for the reader to give proofs for the preceeding two theorems modifying the proofs of Theorems 5.1 and 5.2 and by working with V_1^0 (resp. V_1^1) plus the $\Sigma_0^{1,b}$ - diagram of the original model.

8 Finitistic consistency statements and optimal proof systems

Definition 8.1 *(a) Let P be a propositional proof system. Function $c_P(\tau) : TAUT \rightarrow \mathbf{N}$ is defined by:*

$$c_P(\tau) := min\{|\pi| \mid \pi \textit{ is an } P\textit{-proof of } \tau\} \ .$$

(b) Let P, Q be two propositional proof systems. Then system P is better than *Q, $P \geq Q$ in symbols, iff there is a polynomial $p(x)$ such that:*

$$\forall \tau \in TAUT,\ c_P(\tau) \leq p(c_Q(\tau)) \ .$$

(c) Propositional proof system P is optimal *iff it is the greatest element of the quasi order $\geq$.*

Observe that P is better than Q iff Q has a polynomial speed-up over P, and that $P \geq_p Q$ implies $P \geq Q$ but not necessarily vice versa.

Problem *Does there exist an optimal propositional proof system ?*

Any proof system P which proves all tautologies in polynomial size is optimal; thus $NP = coNP$ implies the affirmative answer to the problem. It is unknown however, whether the converse implication is also true.

A non-trivial information about the problem is provided by Corollary 6.11: *relative* to V_1^1 EF is an optimal proof system, i.e. it is a $\geq$-greatest proof system among those whose soundness is provable in the theory. We use the idea of the proof of these results to obtain a particular representation of a general proof system.

Denote by $\langle Ref_P \rangle$ teh sets of all formulas $\langle Ref_P \rangle_n$, $n < \omega$.

Theorem 8.2 *Let P be a propositional proof system. Let*

$$EF + \langle Ref_P \rangle$$

be the proof system obtained from EF by adding tautologies from $\langle Ref_P \rangle$ as extra axioms.

Then:

$$EF + \langle Ref_P \rangle \geq_p P \ .$$

In particular:

$$EF + \langle Ref_P \rangle \geq P \ .$$

Proof

Let π be a P - proof of τ. By Lemmas 6.9 and 6.10 there is a polynomial size EF-proof η_1 of:

$$\langle Prf \rangle_m(\tilde{\pi}, \tilde{\tau}) \wedge \langle Fla(v) \rangle_m(\tilde{\tau})$$

where $m = max(|\pi|, |\tau|)$. From this formula (and η_1) and the new axiom

$$\langle Ref_P \rangle_m$$

we get by the substitution a polynomial size $(EF + \langle Ref_P \rangle)$- proof η_2 of:

$$\langle TAUT(v) \rangle_m(\tilde{\tau}) \ .$$

There is polynomial size EF- proof η_3 of the implication (analogously to Lemma 6.7):

$$\langle TAUT(v) \rangle_m(\tilde{\tau}) \rightarrow \tau \ .$$

From η_2 and η_3 one obtains by modus ponens a polynomial size $(EF + \langle Ref_P\rangle)$ - proof η_4 of τ.

Note that η_1 and η_3 are actually constructible by a polynomial time algorithm and so this gives a p-simulation of P by $(EF + \langle Ref_P\rangle)$.

Q.E.D.

Note that a *natural* P (like the systems SF or G, and other) is, in fact, p-equivalent to $EF + \langle Ref_P\rangle$. This is because such P admits a polynomial time construction of proofs of the formulas $\langle Ref_P\rangle_n$.

Now we link the problem of the existence of an optimal proof system to a question from logic. The question deals with the lengths of first order proofs of the so called *finitistic consistency statements.* Let T be a consistent theory extending V_1^1 and with a polynomial time set of axioms. Then there is a $\Delta_1^{1,b}$ - formula $Prf_T(\pi, \alpha)$ expressing that "π is a T-proof of formula α". Consider a formula $Con_T(x)$ naturally expressing that no T-proof of length $\leq x$ is a proof of $0 = 1$:

$$\forall \pi^x \neg Prf_P(\pi^x, \ulcorner 0 = 1 \urcorner) \ .$$

It is a fundamental problem to estimate the length of the shortest proof of the sentence $Con_T(\tilde{n})$ in a theory S. The term $\tilde{n}$ is the dyiadic numeral for n defined inductively by: $\tilde{0} := 0$, $\tilde{1} := 1$, $\tilde{2} := (1+1)$, $\widetilde{2k} := \tilde{2} \cdot \tilde{k}$, and $\widetilde{2k+1} := \widetilde{2k} + 1$. The length of the numeral $\tilde{n}$ is $O(\log n)$ hence the only apriori lower bound to such proofs is the length of the formula, i.e. $\Omega(\log n)$. The next theorem estimates sharply the length of the shortest S - proofs in the case when $S = T$.

Theorem 8.3 (H. Friedman, P. Pudlák) *Let $T \supseteq V_1^1$ be a consistent theory with a polynomial time set of axioms and let $Con_T(x)$ be the formula defined above.*

Then there are constants $\epsilon > 0$ and $c \geq 1$ such that for all n the minimal size m_n of a T-proof of the sentence $Con_T(\tilde{n})$ satisfies:

$$n^\epsilon \leq m_n \leq n^c \ .$$

Note that $|Con_T(\tilde{n})| << n^\epsilon$ and hence the lower bound is non-trivial. The upper bound is also non-trivial. To see this take, for example, $S = V_1^1$ and $T = ZFC$. There does not seem to be other way how to prove $Con_T(\tilde{n})$ in S then to list (in S) all T-proofs of length $\leq n$ and check that none of them is a proof of $0 = 1$. This gives however, only the estimate $2^{O(n)}$.

The question whether there is S admitting size $n^{O(1)}$ proofs of $Con_T(\tilde{n})$ for all T can be linked to the problem posed above.

Theorem 8.4 *The following two propositions are equivalent:*

1. *there exists an optimal propositional proof system*
2. *there exists a consistent theory $S \supseteq S^1_2$ with a polynomial-time set of axioms such that for every consistent theory $T \supseteq S^1_2$ with a polynomial-time set of axioms there is polynomial $p(x)$ such that for each n the sentence $Con_T(\tilde{n})$ has S-proof of size $\leq p(n)$.*

Proof
Assume that P is an optimal proof system. Define the theory S_P by:

$$S_P := S^1_2 + Ref_P \ .$$

Now let $T \supseteq V^1_1$ be a consistent theory with a polynomial-time set of axioms. Define the formula $A(\beta^x)$:

$$A(\beta^x) := Con_T(x) \ .$$

Then A is a $\Pi^{1,b}_1$ - formula. Consider a proof system Q:

$$Q := P + \{\langle A\rangle_m \mid m < \omega\} \ .$$

The formulas $\langle A\rangle_m$ are tautologies as T is consistent,a nd form a p-time set, so Q is indeed a proof system.

Since P is optimal, there is a polynomial $q(x)$ such that each $\langle A\rangle_m$ has P-proof of size $\leq q(m)$. Hence the theory S_P admits proofs of

$$TAUT(\langle A\rangle_m)$$

of size $m^{O(1)}$ and also size $m^{O(1)}$ proofs of

$$A(\tilde{m}) \ .$$

Consequently $Con_T(\tilde{m})$ has S_P - proof of size $m^{O(1)}$. This proves that the first statement implies the second.

Now let S be a theory satisfying the second statement. Define the propositional proof system P_S by:

$$\pi : P_S \vdash \tau) \text{ iff } \pi : S \vdash \lceil TAUT(\tilde{\tau})\rceil \ .$$

That is, a P_S-proof of a formula is an S-proof of the statement that the formula is a tautology.

Let Q be an arbitrary propositional proof system. We know by earlier theorems that Q is p-simulated by the system $EF + \langle Ref_Q \rangle$. As $S \supseteq V_1^1$, we also know that P_S p-simulates EF. It is thus sufficient to construct polynomial size P_S-proofs for the tautologies:

$$\langle Ref_Q \rangle_m \ .$$

Consider the theory T_Q:

$$T_Q := V_1^1 + Ref_Q \ .$$

By the hypothesis there are polynomial size S-proofs of:

$$Con_{T_Q}(\tilde{n}) \ .$$

Assume that π is the size $m = |\pi|$ Q-proof of τ. As $\neg Taut \in \Sigma_1^{1,b}$, there is $k < \omega$ such that the implication:

$$\neg TAUT(\tilde{\tau}) \to \exists \delta^{m^k} \wedge Prf_S(\delta, \ulcorner \neg TAUT(\tilde{\tau}) \urcorner)$$

is provable in V_1^1 and hence also in S (this is analogous to Lemma 6.7).

For the same reason there is a size $\leq m^k$ T_Q-proof of $Prf_Q(\tilde{\pi}, \tilde{\tau})$, and by the axioms Ref_Q T_Q also admits size $\leq m^k$ proofs of:

$$TAUT(\tilde{\tau})$$

and hence there are size $m^{O(1)}$ S-proofs of

$$\exists \delta^{m^{O(1)}}, Prf_{T_Q}(\delta, \ulcorner TAUT(\tilde{\tau}) \urcorner) \ .$$

This formula and the last but one entails that there is a size $m^{O(1)}$ S-proof of:

$$\neg TAUT(\tilde{\tau}) \to \neg Con_{T_Q}(\widetilde{m^d}) \ ,$$

some fixed $d < \omega$.

By the hypothesis there is a constant $t < \omega$ such that all $Con_{T_Q}(\tilde{n})$ have size $\leq n^t$ S-proofs, hence there are size $\leq m^{dt}$ S-proofs of $TAUT(\tilde{\tau})$.

By the definition of P_S this proof is also a P_S-proof of τ of size $\leq m^{dt}$.

Q.E.D.

One may speculate about a construction of a theory T for which given S does not admit size $n^{O(1)}$ proofs of $Con_T(\tilde{n})$. Possible candidates are $T := S + Con_S$ or a theory formed from S by adding to the language a truth predicate for formulas in the language of S , Tarski's conditions on this predicate and the statement (using the new predicate) that all axioms of S are true (such theory is called "jump" of S by Buss). However, if for S one can find T without short S-proofs of $Con_T(\tilde{n})$ it follows that S does not prove that $NP = coNP$. This is because the formula A considered in the proof above is $\Pi_1^{1,b}$ and $NP = coNP$ would allow to express it also as a $\Sigma_1^{1,b}$-formula and so its instances (and consequently the instances of $Con_T(x)$) would have polynomial size proofs by (an analogy of) Lemma 6.7.

The next theorem links the problem of the existence of an optimal proof system to a problem in structural complexity theory. We will not prove it.

Theorem 8.5 *The following two propositions are equivalent:*

1. *there exists an optimal propositional proof system*

2. *for every $coNP$ - set X there exists a non-deterministic Turing machine M accepting exactly X and such that for every polynomial-time, sparse $Y \subseteq X$ there is a polynomial $p(x)$ such that every $u \in Y$ is accepted by M in time $\leq p(|u|)$.*

9 Hard tautologies

The first definition formalizes a notion of hard tautologies.

Definition 9.1 *A sequence $\{\tau_n\}_{n<\omega}$ of tautologies is* hard *for a propositional proof system P iff the following three conditions are fullfiled:*

1. *there exists a polynomial time machine computing from $1^{(n)}$ the formula τ_n*

2. *$n \leq |\tau_n|$, for all n*

3. *there is no polynomial $p(x)$ for which*

$$c_P(\tau_n) \leq p(|\tau_n|)$$

would hold for all n

Note that $|\tau_n| = n^{O(1)}$. Conditions 1. and 2. imply that set $\{\tau_n \mid n < \omega\}$ is polynomial-time recognizable and so we may add it to P as extra axioms to form new proof system $Q := P + \{\tau_n \mid n < \omega\}$. Adding extra axioms to a general proof system precisely means that π is a Q-proof of τ iff it is a P-proof of $\sigma \to \tau$, where σ is a conjunction of *substitution instances* of new axioms. P is then not better than Q. Hence the task to construct a hard sequence $\{\tau_n\}_{n<\omega}$ for P is the same as the task to find proof system Q such that $P \not\geq Q$ and its *axiomatization* over P by a polynomial-time set of tautologies.

Assume $P \geq EF$. Having Q for which $P \not\geq Q$ we may take the proof system $Q' := EF + \langle Ref_Q \rangle$. Then $Q' \geq Q$, hence $P \not\geq Q'$ and the sequence $\langle Ref_Q \rangle_n\}_{n<\omega}$ is hard for P. This gives the following simple but useful statement.

Theorem 9.2 *Let P be a proof system and assume that $P \geq EF$. The following three statements are equivalent:*

1. *there exists a sequence of tautologies $\{\tau_n\}_{n<\omega}$ hard for P*
2. *there exists a proof system Q such that P is not better than Q : $P \not\geq Q$*
3. *there exists a proof system Q such that the sequence $\langle Ref_Q \rangle_n\}_{n<\omega}$ is hard for P*

The quasiordering of proof systems induces a reducibility among sequences $\{\tau_n\}_{n<\omega}$, $\{\sigma_n\}_{n<\omega}$ over a given system P:

$$\{\tau_n\}_{n<\omega} \geq_P \{\sigma_n\}_{n<\omega} \ \text{ iff } \quad P + \{\tau_n \mid n < \omega\} \geq_P P + \{\sigma_n \mid n < \omega\} \ ,$$

i.e. formulas σ_n can be deduced by polynomial size P - proofs from *substitution instances* of some τ_m 's.

10 Further topics

We have discussed a relations of cryptographic conjectures to feasible interpolation and to the automatizability of proof systems. See [7] and [11] (both available from my web page).

References

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

[2] Cook, S A. (1971) The complexity of theorem proving procedures, in: *Proc. 3rd Annual ACM Symp. on Theory of Computing*, pp. 151-158. ACM Press.

[3] —— (1975) Feasibly constructive proofs and the propositional calculus, in: *Proc. 7th Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.

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

[5] Krajíček, J. (1995) *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press.

[6] J. Krajíček, On Frege and Extended Frege Proof Systems. in: ”Feasible Mathematics II”, eds. P. Clote and J. Remmel, Birkhauser, (1995), pp. 284-319.

[7] Krajíček, J. (1997) Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. Symbolic Logic*, **62(2)**, pp. 457-486.

[8] Krajíček, J. (2003) *Propositional proof complexity I.*, lecture notes.

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

[10] Krajíček, J., and Pudlák, P. (1990a) Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**:29-46.

[11] Krajíček, J., and Pudlák, P.: Some consequences of cryptographical conjectures for S^1_2 and EF”, *Information and Computation*, Vol. **140 (1)**, (January 10, 1998), pp.82-94.

[12] Krajíček, J.,Pudlák, P. and Woods, A. (1991) Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, submitted.

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

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