Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus

Jan Krajíček*

Mathematical Institute, Oxford**

Abstract. We prove lower bounds for a proof system having exponential speed-up over both polynomial calculus and constant-depth Frege systems in DeMorgan language.

Introduction

An interesting open problem is to prove a lower bound for constant-depth subsystems of $F(MOD_p)$ (cf. [5, Definition 12.6.1] or [3]), a system that combines boolean reasoning (DeMorgan language) with algebraic reasoning (counting modulo p). In this note we show that the lower bound for the degree of Nullstellensatz proofs for the onto pigeonhole principle PHP_n^{n+m} from [2], as well as the bound for the polynomial calculus proofs of the counting principles $Count_q^n$ from [8], imply lower bounds for a weak subsystem of $F(MOD_p)$ that has nevertheless an exponential speed-up over constant-depth Frege systems in DeMorgan language and over polynomial calculus.

Namely, the proofs in the system, call it $F_d^c(MOD_p)$ here, are $F(MOD_p)$ - proofs that may use only formulas that can be obtained by substituting DeMorgan formulas of depth at most d into formulas in the language

$$\{0, 1, \neg, \vee, \wedge, MOD_{p,0}, \ldots, MOD_{p,p-1}\}$$

$\vee$ and $\wedge$ binary and $MOD_{p,i}$ of arbitrary arity, of *logical depth* at most c, where d and c are independent constants.

The speed-ups are witnessed by $Count_p^n$ (see [5, Thms. 12.5.4 and 12.6.2]) and $PHP_n^{n^2}$ (see [13, Thm 3.1] and [5, Thm. 12.1.2]) respectively, and they are achieved already by tree-like $F_d^c(MOD_p)$-proofs.

This note complements my lecture at this meeting. Most of the material covered there can be found in literature (a good starting point is either [5], or one of [6, 7, 11, 12], or introductions to [1, 3, 13]) except the theorem and its proof given here.

* Partially supported by cooperative research grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic) and by the grant #A1019602 of the Academy of Sciences of the Czech Republic.

** On leave from the Mathematical Institute of the Academy of Sciences at Prague.

The paper is self-contained in giving all details but presupposes familiarity with the forcing method in propositional proof complexity as formalized by the notion of k-evaluations, in particular with the material covered in [2] or [5, Secs.12.4-7.]. Using these known results and terminology the proof is rather concise.

1 The lower bound

The formulas PHP_n^{n+m} and $Count_q^n$ are defined in [5, Def. 12.5.1]. In particular, PHP_n^{n+m} is the onto-version

$$\bigvee_i \bigwedge_j \neg x_{ij} \ \vee \ \bigvee_j \bigwedge_i \neg x_{ij} \ \vee$$

$$\bigvee_{i_1 \neq i_2} \bigvee_j (x_{i_1 j} \wedge x_{i_2 j}) \ \vee \ \bigvee_i \bigvee_{j_1 \neq j_2} (x_{ij_1} \wedge x_{ij_2})$$

with i, i_1, i_2 ranging over $n+m$ and j, j_1, j_2 ranging over n.

Theorem 1. *Let c, d and a prime p be fixed, and let q be a number not divisible by p. Then*

1. *There is $\delta > 0$ such that for all n large enough it holds: There is $m \leq n$ such that in every tree - like $F_d^c(MOD_p)$ - proof of PHP_n^{n+m} at least $\exp(n^\delta)$ different formulas must occur.*
2. *For every k the following holds: For all n large enough and not divisible by q, in every $F_d^c(MOD_p)$ - proof of $Count_q^n$ at least n^k different formulas must occur.*

Proof. We shall use without further explanation the notation and the results about k-evaluations as given in [5, Secs. 12.4.-12.7] (they are presented uniformly for PHP and $Count_q$) and in [2]. In particular, matching decision trees of height at most k of [2, 10] are particular k-complete systems of [9, 5], and sets denoted S_ω, H_ω in [5] are $Br(T_\omega)$, $Br_1(T_\omega)$ of [2, Defs. 3.1 and 4.1].

We prove the first statement only. The proof of the second statement is completely analogous replacing Nullstellensatz provability from $\neg PHP_{n'}^{n'+m}$ by provability in polynomial calculus from the (N, q)-system (see [1, 3]) and the bound from [2, Thm. 12] with [8, Cor. 3.3]. Assume for the simplicity that modus ponens is the only inference rule of the proof system. We consider Nullstellensatz proofs over $\mathbf{F}_p$.

Let $\pi = \sigma_1, \ldots, \sigma_\ell$ be a tree-like $F_d^c(MOD_p)$ - proof of PHP_n^{n+m}, where n is large enough and $m = p^\ell$ for suitable ℓ (to be chosen later). We are going to show that if the number of different formulas in π is less than 2^{n^δ}, $\delta > 0$ a rational depending only on d, then for some n' there is Nullstellensatz refutation of

$\neg PHP_{n'}^{n'+m}$ of degree less than $2^\ell - 1$. By $\neg PHP_{n'}^{n'+m}$ we denote the polynomial system denoted $onto - \mathcal{PHP}_{n'}^{n'+m}$ in [2], i.e.,

$$1 - \sum_j x_{ij} = 0 \quad \text{for each } i \tag{1}$$

$$1 - \sum_i x_{ij} = 0 \quad \text{for each } j \tag{2}$$

$$x_{i_1 j} x_{i_2 j} = 0 \quad \text{for each } i_1 \neq i_2, j \tag{3}$$

$$x_{i j_2} x_{i j_2} = 0 \quad \text{for each } i, j_1 \neq j_2 \tag{4}$$

with i, i_1, i_2 ranging over $n'+m$ and j, j_1, j_2 ranging over n'. That will contradict the bound [2, Thm. 12].

Note that it is more convenient to work over the ring $R_{n'} := \mathbf{F}_p[\overline{x}]/I_{n'}$, where $I_{n'}$ is the ideal generated by left-hand sides of equations (3) and (4) together with all $x_{ij}^2 - x_{ij}$. The degree of Nullstellensatz refutation of $\neg PHP_{n'}^{n'+m}$ in $\mathbf{F}_p[\overline{x}]$ is the same as of refutations of equations (1) and (2) over $R_{n'}$ (cf. [3, L. 3.1] holding identically for PHP). Monomials in $R_{n'}$ can be naturally identified with partial one-to-one maps from $n' + m$ to n'.

Pick $\frac{1}{5} > \epsilon > 0$ and $\epsilon^{d+1} \frac{\log_p 2}{2} > \delta > 0$ small enough that the hypotheses of [2, L. 6] (corresponds to [5, Thm. 12.4.3]) are fulfilled for $n_i := n^{\epsilon^i}$, $\ell := \lfloor \epsilon^{d+1} \log_p(n) \rfloor$ and $m := p^\ell$. By that lemma there is a k - evaluation of the set of all DeMorgan formulas in π, with $k = O(n^\delta)$, restricted by a partial one-to-one map ρ of size $n - n'$, for $n' = \Omega(n^{\epsilon^d})$.

Assume that $\sigma_i = \phi_i(\psi_{i,1}, \ldots, \psi_{i,j_i})$ where $\psi_{i,j}$ are DeMorgan of depth at most d and ϕ_i are of logical depth at most c.

We give first an intuitive argument motivating the proof ($m = 1$ here). Let n be a non - standard number in some countable model M of true arithmetic. By [5, L. 12.7.3] for any generic set G, (I, f_G) satisfies $\psi_{i,j}^\rho$ iff it satisfies the disjunction $\bigvee H_{i,j}$, where $H_{i,j}$ is the set assigned to $\psi_{i,j}^\rho$ by the k - evaluation. As all partial maps in $H_{i,j}$ are incompatible, the disjunction holds in (I, f_G) iff the equality $h_{i,j} = 1$ holds there, where $h_{i,j} := \sum H_{i,j}$, the sum of monomials corresponding to maps in $H_{i,j}$. Hence, in (I, f_G), $(\phi_i(\overline{\psi}))^\rho$ holds iff $g_i = 1$ where $g_i := \phi_i^*(h_{i,1}, \ldots, h_{i,j_i})$. Here ϕ_i^* is a polynomial of degree at most $(\max(2, p-1))^c \le p^c$ straightforwardly translating the formula ϕ_i into a polynomial: $0^* := 0$, $1^* := 1$, $(f \wedge g)^* := f^* \cdot g^*$, $(\neg f)^* := 1 - f^*$, $(f \vee g)^* := f + g - fg$ and $(MOD_{p,i}(f_1, \ldots, f_k))^* := (\sum_{i \le k} f_i)^{p-1}$. As both k -evaluation and the $*$ - translation are sound w.r.t generic extension (i.e., modulo provability from $\neg PHP_{n'}^{n'+1}$) the sequence $g_1, \ldots, g_\ell$ acts as a tree-like semantic refutation of $\neg PHP_{n'}^{n'+1}$ as $g_\ell = 0$ by [5, L. 12.5.2]. This is then turned into a low degree Nullstellensatz refutation using [3, Thms. 2.6 and 5.4].

The proof shall follow these lines replacing validity in generic extensions by provability, and the statements about $PHP_{n'}^{n'+1}$ from [5] by corresponding statements from [2] about $PHP_{n'}^{n'+m}$.

Claim 1. *Every $1 - g_i$ has a Nullstellensatz proof from $\neg PHP_{n'}^{n'+m}$ of degree at most $O(p^c k^2)$.*

Note that as $O(p^c k^2) << 2^\ell - 1$ we get the required contradiction.

We need to show that any axiom translates into a polynomial g such that $1 - g$ has a Nullstellensatz proof and that modus ponens can be simulated by Nullstellensatz such that the degrees of these simulations are small, i.e. proportional to the degrees of polynomials involved. Then we get tree-like polynomial calculus refutation of $\neg PHP_{n'}^{n'+m}$ of size at most 2^k and degree $O(p^c k)$ and applying [3, Thm. 5.4] yields the required Nullstellensatz refutation.

If only the translation $*$ were involved then this is trivial, see also [3]. A problem can arise when the $*$ translation is combined with the translation via k-evaluations. The following claim clarifies this situation. Note that it also explains why it is irrelevant how exactly are σ_i represented in the form $\phi_i(\psi_{i,1}, \dots, \psi_{i,j_i})$, provided that the total degree is small.

Claim 2. *Let $\alpha = \beta(\gamma_1, \dots, \gamma_t)$ be a DeMorgan formula and let $h_\alpha := \sum H_\alpha$, $h_{\gamma_i} := \sum H_{\gamma_i}$ be the polynomials assigned to α, γ_i via the k-evaluation. Then $h_\alpha - \beta^*(h_{\gamma_1}, \dots, h_{\gamma_t})$ has a Nullstellensatz proof from $\neg PHP_{n'}^{n'+m}$ of degree at most $O(k)$.*

Let h_ω denotes $\sum H_\omega$, whenever defined by the k-evaluation. By [2, L. 11] $1 - \sum S_\omega$ has a Nullstellensatz proof from $\neg PHP_{n'}^{n'+m}$ of degree bounded by the height of S_ω, i.e. by $\max(deg(h_\omega, deg(h_{\neg\omega}))$ (in case of $Count_p$ this is replaced by [1, L. 4.3] or [5, L. 12.6.3]). By [2, Def. 4.1] (or [5, Def.12.4.1]) $h_\omega + h_{\neg\omega} = \sum S_\omega$. Thus $h_{\neg\omega} - (1 - h_\omega)$ has degree $\max(deg(h_\omega), deg(h_{\neg\omega}))$ Nullstellensatz proof. As $1 - h_\omega$ is by definition also $(\neg h_\omega)^*$ this shows that the translations behave equally w.r.t. the negation.

It remains to show the same for the disjunction (the conjunction is in both translations defined by DeMorgan rules from the negation and the disjunction). Let $\eta = \omega_1 \vee \omega_2$ We want to show that $h_\eta - (h_{\omega_1} \vee h_{\omega_2})^*$, i.e.

$$h_\eta - (h_{\omega_1} + h_{\omega_2} - h_{\omega_1} h_{\omega_2}) \tag{5}$$

has Nullstellensatz proof of degree at most $O(k)$. Note that monomials in $h_{\omega_1} h_{\omega_2}$ that do not cancel by $I_{n'}$ have degree at most the height of S_η, i.e., $O(k)$. This is because such monomials are of the form $\mu_1 \cup \mu_2$, $\mu_i \in H_{\omega_i}$ compatible, and thus contained in some $\xi \in S_\eta$.

To prove this we need to exploit the definition of k-evaluations. Recall that we identify monomials with partial one-to-one maps.

Claim 3. *Let μ be a monomial and let S be a k-complete system such that for all $\xi \in S$, $\xi \supseteq \mu$ or $\xi \perp \mu$. Then*

$$\mu - \sum_{\xi \in S, \xi \supseteq \mu} \xi$$

has a Nullstellensatz proof of degree bounded by the height of S, i.e., by $O(k)$.

To prove Claim 3 note that $S^\mu = \{\xi \setminus \mu \mid \xi \in S \wedge \xi \supseteq \mu\}$. By [2, L. 1] (or [5, L. 12.3.9]) S^μ is k-complete too (on the universe without the elements of μ) and thus by [2, L. 11] $1 - \sum_{\xi\setminus\mu\in S^\mu} \xi \setminus \mu$ has a Nullstellensatz proof of degree less then the height of S^μ (in case of $Count_p$ one uses here [1, L. 4.3]). Multiplying the proof by monomial μ gives a proof required in Claim 3.

Let us return to (5). Take $H_{\omega_1} \cup H_{\omega_2}$, monomials occurring in one of h_{ω_1},h_{ω_2}. By the definition of k-evaluation ([5, Def. 12.4.1]), S_η refines $H_{\omega_1} \cup H_{\omega_2}$ and hence any $\xi \in S_\eta$ either contains some $\mu \in H_{\omega_1} \cup H_{\omega_2}$ or is incompatible to all such μ. If it contains some $\mu_i \in H_{\omega_i}$ $(i = 1, 2)$ it contains no other $\mu \in H_{\omega_i}$ (as $\mu, \mu_i \in S_{\omega_i}$ and thus are incompatible). Thus for any $\xi \in H_\eta$ one of the two cases occurs:

1. ξ contains one $\mu_i \in H_{\omega_i}$ and no $\mu \in H_{\omega_{2-i}}$, some $i = 1, 2$
2. ξ contains one $\mu_i \in H_{\omega_i}$ for both $i = 1, 2$

In the former case ξ contains no monomial of $h_{\omega_1}h_{\omega_2}$ (as it would also contain a monomial from $H_{\omega_{2-i}}$). In the later case ξ contains exactly one monomial of $h_{\omega_1}h_{\omega_2}$, namely $\mu_1 \cup \mu_2$. Hence applying Claim 3 for S_η and each monomial in h_{ω_1}, h_{ω_2} and $h_{\omega_1}h_{\omega_2}$ yields the Nullstellensatz proof required for (5).

This completes the proof of Claim 2 and of the theorem.

□

Note that exponential lower bounds for sequence-like $F_d^c(MOD_p)$ - proofs of either formula would follow from $n^{\Omega(1)}$ lower bounds for the degree of polynomial calculus refutations of the onto pigeonhole principle and of the counting principles. Unfortunately, neither [8] nor [13] seem to yield such bounds ([13] gives $\frac{n}{2}$ lower bound for the pigeonhole principle but not for the onto-version needed for the transformation from k - evaluations to Nullstellensatz provability as above).

Acknowledgements: It is stated in [4, Sec.8] and again in [13, Sec.1] that T.Pitassi suggested that a lower bound for polynomial calculus proofs of the pigeonhole principle or counting principles would yield a lower bound for constant - depth proofs operating with formulas that are DeMorgan except the top connective that might be the parity. That remark inspired somewhat stronger Theorem 1.

References

1. Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., Pudlák, P.: Lower bounds on Hilbert's Nullstellensatz and propositional proofs. Proceedings of the London Mathematical Society **73(3)** (1996) 1–26
2. Beame, P., Riis, S.: More on the relative strength of counting principles. (submitted)
3. Buss, S., Impagliazzo, R., Krajíček, J., Pudlák, P., Razborov, A. A., Sgall, J.: Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. Computational Complexity (to appear)

4. Clegg, M, Edmonds, J., Impagliazzo, R.: Using the Groebner basis algorithm to find proofs of unsatisfiability. In: *Proceedings of the 28th ACM Symposium on Theory of Computing*, ACM (1996) 174–183
5. Krajíček, J.: *Bounded arithmetic, propositional logic, and complexity theory.* Encyclopedia of Mathematics and Its Applications, Vol. **60** Cambridge University Press (1995)
6. Krajíček, J.: A fundamental problem of mathematical logic. Annals of the Kurt Gödel Society, Springer-Verlag, Collegium Logicum, **2** (1995) 56–64
7. Krajíček, J.: On methods for proving lower bounds in propositional logic. In: *Logic and Scientific Methods* Eds. M. L. Dalla Chiara et al., (Vol. 1 of Proc. of the Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence (August 19-25, 1995)), Synthese Library, **259** Kluwer Academic Publ., Dordrecht (1997) 69–83
8. Krajíček, J.: On the degree of ideal membership proofs from uniform families of polynomials over a finite field. (in preparation)
9. Krajíček, J.,Pudlák, P., Woods, A.: Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. Random Structures and Algorithms **7(1)** (1995) 15–39
10. Pitassi, T., Beame, P., and Impagliazzo, R.: Exponential lower bounds for the pigeonhole principle. Computational Complexity **3(2)** (1993) 97–140
11. Pudlák, P.: The lengths of proofs. In: *Handbook of Proof Theory*, Ed. S. Buss, (to appear)
12. Razborov, A. A.: Lower bounds for propositional proofs and independence results in bounded arithmetic. In: *Proc. of the 23rd ICALP*, F.Meyer auf der Heide and B. Monien eds., LN in Computer Science, **1099**, Springer-Verlag, (1996) 48–62
13. Razborov, A. A.: Lower bounds for the polynomial calculus. (submitted)

Current address:

Mathematical Institute
University of Oxford
24-29 St.Giles'
Oxford, OX1 3LB, U.K.
E.mail: `krajicek@maths.ox.ac.uk`